DEDICATED TO

To my parents, teachers and all my seniors without their guidance and advice I would have been nowhere in life.

And

Especially to a person who has directed me towards the meaning of life.....
Acknowledgements

This book is not the end of anything; its just the beginning…. For you, for me and for all the friends and colleagues who have helped me shape and express the knowledge shared on these pages. They include, first and foremost, my family – my mother who has been from the day one my greatest source of inspiration; my father who taught me to be on the righteous path and who knew just when to kick the tar out of me to keep me in the line. I also wish to express my deep appreciation for someone who is far and away, the true intellectual powerhouse of the offspring for being there, through so many turning points.
Aims and Objectives
To provide:
- Essential body of IT knowledge relating to business systems
- IT security, control, and governance knowledge related to business systems
- Application of knowledge to manage and evaluate IT

Interactive Grid

<table>
<thead>
<tr>
<th>Syllabus Content Area</th>
<th>Weightage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. IT Strategy and Management</td>
<td>30</td>
</tr>
<tr>
<td>2. IT Security, Control and Management</td>
<td>40</td>
</tr>
<tr>
<td>3. Case Studies</td>
<td>30</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>100</strong></td>
</tr>
</tbody>
</table>

Syllabus

1. IT Strategy and Management

1.1 IT Strategy

Chapter 1 to 4

a. What is Strategy?
b. The Strategic Plan
c. The IT Strategic Plan
d. Considerations for IT Strategic Planning
e. Aligning the IT and Business Strategic Plans
f. Components of Long Range Plans
g. E-Business Models

1.2 Management of IT

Chapter 5

h. Management of computer operations
i. Management of inter-organisational computing
j. Management of end-user computing
k. Financial analysis and control
l. IT Control Objectives

1.3 Software

Chapter 6

a. Supply Chain Management (SCM)
b. Enterprise Resources Planning (ERP)
c. Customer Relationship Management (CRM)
d. Sales Force Automation (SFA)
e. E-Business Products

1.4 IFAC Guidelines/Discussion papers

Chapter 7

a. Managing Security of Information
b. Managing Information Technology Planning for Business Impact
c. Acquisition of Information Technology
d. Implementation of Information Technology Solutions
e. IT Service Delivery and Support
f. IT Executive Checklist
g. Other Papers and Guidelines
## 2. Information Technology Security, Control and Management

### 2.1 Introduction

### 2.2 Control frameworks

- a. Risks and exposures in computer-based information systems
- b. IT control frameworks

### 2.3 Control objectives

- a. Effectiveness, efficiency, economy of operations
- b. Reliability of financial reporting
- c. Effectiveness of design
- d. IT asset safeguarding
- e. Compliance with applicable laws and regulations
- f. System reliability
- g. Data integrity

### 2.4 Layer of control

- a. Societal
- b. Organisational environment
- c. Technology infrastructure
- d. Software
- e. Business process

### 2.5 Responsibility for control

- a. Role and responsibilities of key parties

### 2.6 Control environment

- a. External regulatory controls
- b. Board/audit committee governance
- c. Management philosophy and operating style
- d. Plans/structure of organisation
- e. Method to communicate the assignment of authority and responsibility
- f. Management control methods
- g. Human resource policies and practices
- h. Financial policies and practices

### 2.7 Risk assessment

- a. Risk categories
- b. Probability of loss
- c. Consequences

### 2.8 Control activities

- a. Control design
- b. Control procedures
- c. Control over data integrity, privacy and security
- d. Availability / continuity of processing, disaster recovery planning and control
- e. IS processing /operations

### 2.9 Monitoring of control compliance

- a. Roles of management, users, auditors
- b. Computer-assisted audit techniques
## Detailed Table of Contents

### 1. INFORMATION & INFORMATION SYSTEMS

1.1 INFORMATION REQUIREMENTS ................................................................................................................................. 19

1.1.1 Types of Information
1. Strategic information ................................................................. 20
2. Tactical information ............................................................... 20
3. Operational information ......................................................... 21

1.1.2 Improvements to information ........................................................................................................................................... 22

1.2 THE VALUE AND COST OF INFORMATION .................................................................................................................... 22

1.2.1 Assessing the value of information ......................................................... 23
1.2.2 Cost of information ......................................................................... 24
1.2.3 Traditional methods for assessing cost ........................................... 25
1.2.4 The benefits of a proposed information system .................................. 25

1.3 INFORMATION MANAGEMENT AND DECISION MAKING ............................................................................................... 26

1.3.1 Structured and unstructured decisions .......................................................................................................................... 26
1.3.2 Information systems to support decision making ................................ 27

1.4 TYPES OF INFORMATION SYSTEM ....................................................................................................................................... 28

1.4.1 Operational level information systems .............................................. 28
1.4.2 Tactical level information systems ..................................................... 28
1.4.3 Strategic level information systems .................................................. 28

1.4.4 Executive Support Systems (ESS) ..................................................... 30
1.4.5 Management Information Systems (MIS) ........................................ 30
1.4.6 Decision Support Systems (DSS) ...................................................... 31
1.4.7 Knowledge Work Systems (KWS) .................................................... 33
1.4.8 Office Automation Systems (OAS) .................................................... 34
1.4.9 Transaction Processing Systems (TPS) ............................................. 35

1.4.10 Batch Processing and On-line processing ........................................ 36

1.4.11 Expert Systems ................................................................................ 36

1.5 KNOWLEDGE MANAGEMENT ........................................................................................................................................... 37

1.5.1 What is knowledge? .......................................................................... 37
1. Knowledge and intellectual capital ............................................... 37
2. Knowledge processes........................................................................ 38

1.5.2 Knowledge management .................................................................. 38
1. Why knowledge management is important .................................... 38

1.5.3 Approaches to knowledge management ........................................... 39
1. Dealing with the human factor ....................................................... 39
2. Organisation structure ................................................................... 39
3. Top executive behaviour ............................................................. 40
4. The role of information and communication technologies (ICT) ...... 40
5. Organisation, People or ICT? ....................................................... 41
6. Defining a strategy ........................................................................... 41
7. What are organisations doing? ..................................................... 41
8. Measuring success in knowledge management ............................... 42

1.5.4 Conclusion .................................................................................... 42

### 2. STRATEGIC PLANNING OF INFORMATION SYSTEMS

2.1 STRATEGIC PLANNING .................................................................................................................................................. 48

2.1.1 Corporate strategy ........................................................................ 48
2.1.2 Business strategy ........................................................................ 48
2.1.3 Functional/operational strategic; information systems strategy ...... 49
2.2 FORMULATING STRATEGIES: THE RATIONAL MODEL .......................................................... 49
2.2.1 Strategic analysis.............................................................................................................. 49
2.2.2 Strategic choice................................................................................................................ 50
2.2.3 Strategy implementation ............................................................................................... 50
2.3 WHY HAVE AN IS/IT STRATEGY? ................................................................................ 50
2.3.1 Importance of information systems ................................................................................ 50
2.3.2 Strategic potential for IT ............................................................................................... 52
2.4 THE INFORMATION SYSTEMS STRATEGY ................................................................... 52
2.4.1 Purpose of an information systems strategy ................................................................. 52
2.4.2 Contents of IS strategy.................................................................................................. 53
2.5 DEVELOPING A STRATEGY FOR INFORMATION SYSTEMS AND INFORMATION TECHNOLOGY ........................................................................................................... 54
2.5.1 The Information Engineering ........................................................................................ 54
1. Initiating the ISP project..................................................................................................... 55
2. Clarifying the business strategy ........................................................................................ 55
3. Modelling the business ..................................................................................................... 55
4. Reviewing current information systems ......................................................................... 56
5. Building the information systems' architecture .............................................................. 56
6. Developing the strategic information systems plan (SISP) .............................................. 58
2.5.2 Parson Generic IS Strategies ......................................................................................... 58
1. Centrally planned ............................................................................................................. 58
2. Leading edge ................................................................................................................... 59
3. Free market ..................................................................................................................... 59
4. Monopoly ....................................................................................................................... 59
5. Scarce resource .............................................................................................................. 59
6. Necessary evil ................................................................................................................. 60
2.5.3 Generic framework for developing an IS strategy ...................................................... 60
1. ‘W3?’ Where We Were? .................................................................................................. 60
2. ‘W2R?’ Where We Are? ................................................................................................ 61
3. ‘W32B?’ Where We Want To Be? .................................................................................. 61
4. ‘(GT)2?’ Going To Get There? ...................................................................................... 63
5. ‘W4?’ Where We Went Wrong? ................................................................................... 64
6. Strategic Tools and Techniques ..................................................................................... 65
7. Conclusion ..................................................................................................................... 65
2.5.4 Earl three leg approach for IS Strategy development ................................................ 66
1. Infrastructure led - bottom up planning process ......................................................... 66
2. Business led - top down planning process .................................................................. 66
3. Eclectic (mixed) planning process ............................................................................... 66

3. STRATEGIC PLANNING OF INFORMATION SYSTEMS II 70
3.1 IS/IT STRATEGY ............................................................................................................ 70
3.2 ESTABLISHING ORGANISATIONAL INFORMATION REQUIREMENTS (REQUIREMENT ANALYSIS) ................................................................. 70
3.2.1 Enterprise analysis ..................................................................................................... 71
3.2.2 Critical success factors .............................................................................................. 71
1. Data sources for CSFs .................................................................................................. 72
3.2.3 CSF analysis ............................................................................................................. 73
3.2.4 Using Anthony’s levels of management .................................................................. 73
3.3 IT CURRENT SITUATION ANALYSIS ....................................................................... 74
3.3.1 Nolan’s stage Model ................................................................................................. 75
3.3.2 Earl’s Grid ............................................................................................................... 77
3.3.3 McFarlan IS Strategic Grid ...................................................................................... 77
3.3.4 The applications portfolio ...................................................................................... 79
3.4 IS/IT ENVIRONMENTAL ANALYSIS ......................................................................... 80
3.4.1 Opportunities And Threats ................................................................. 80
3.4.2 Pest Analysis .................................................................................. 81

3.5 SWOT ANALYSIS .............................................................................. 82
1. Economic/industry context .............................................................. 83
2. Stakeholders .................................................................................. 83
3. Technical issues ........................................................................... 84
4. The importance of management .................................................. 84

3.6 INFORMATION SYSTEMS AND COMPETITIVE ENVIRONMENT .......... 85
3.6.1 Changing the industry structure ................................................ 85
3.6.2 Creating new businesses and industries ..................................... 87
3.6.3 USING IS/IT FOR COMPETITIVE ADVANTAGE ...................... 87
   1. Generic strategies for competitive advantage ............................... 87
   2. Porter's value chain .................................................................. 88
   3. IS/IT and competitive advantage - other writers ....................... 90

3.7 INFORMATION SYSTEMS AND ITS ALIGNMENT WITH CORPORATE/BUSINESS STRATEGY .................. 91
3.7.1 Ward's Top down aligning of IS and business strategies .......... 91
3.7.2 Management and behavioural styles ......................................... 94
3.7.3 Business objectives and IS/IT resources .................................... 95
3.7.4 Components of Long Range plans ........................................... 95

4. INTERNET & E-COMMERCE .......................................................... 112
4.1 THE INTERNET- AN OVERVIEW .................................................. 112
   4.1.1 Problems with the Internet .................................................... 113
   4.1.2 INTERNET SECURITY ISSUES ............................................ 114
   4.1.3 Hacking ............................................................................. 115
   4.1.4 Viruses ............................................................................. 116
      1. Types of viruses ................................................................... 116

4.2 ENCRYPTION AND OTHER SAFETY MEASURES ......................... 118
   4.2.1 Encryption .......................................................................... 118
   4.2.2 Authentication ..................................................................... 118
   4.2.3 Firewalls ............................................................................ 118
   4.2.4 Dial-back security ............................................................... 118
   4.2.5 Cryptography, keys and signatures ...................................... 118

4.3 ELECTRONIC COMMERCE ............................................................ 119
4.3.1 Electronic Data Interchange (EDI) ............................................. 120
4.3.2 Opportunities over E-commerce and the web ......................... 120
   1. Distribution ........................................................................... 121
   2. Electronic marketing .............................................................. 121
   3. Collecting information about customers ................................... 122
   4. Clickstreams ......................................................................... 122
   5. Virtual companies and virtual supply chains (VSC) .................. 123

4.3.3 Impact of e-commerce and Internet on the traditional business .... 123
4.3.4 Disadvantages of e-commerce ................................................ 126
   1. Lack of trust .......................................................................... 127
   2. Confidentiality ....................................................................... 127
   3. Integrity ................................................................................ 127
   4. Availability ........................................................................... 127
   5. Authentication and non-repudiation ....................................... 127
   6. Power: .................................................................................. 127

4.4 E BUSINESS MODELS .................................................................... 128
   4.4.1 Types of E-business Models ................................................. 129
      1. Business to Consumer Models .............................................. 129
5. MANAGEMENT OF INFORMATION TECHNOLOGY

5.1 MANAGEMENT OF IT OPERATION ................................................................. 144

5.1.1 Computer operations ............................................................................. 145
  1. Operator Assisted Operations ................................................................. 145
  2. Lights Out Operations (Automated Unattended Operations) ............. 145

5.1.2 Input/Output Control Function ............................................................. 146
  1. Data Entry Personnel ........................................................................... 146

5.1.3 Management of IS Operations ............................................................ 147

5.1.4 Control Function .................................................................................. 147

5.1.5 Planning and Scheduling: Service Level ............................................ 147
  1. Service Level Agreements .................................................................... 148

5.1.6 Job Accounting .................................................................................... 149

5.1.7 Scheduling .......................................................................................... 149

5.1.8 Monitoring Use of Resources ............................................................ 149

5.1.9 Problem Management ........................................................................ 149

5.1.10 Program Change Control ................................................................. 151

5.1.11 Quality Assurance ............................................................................ 151

5.1.12 Support/Help Desk .......................................................................... 151

5.1.13 IS Operations Staffing ....................................................................... 152

5.1.14 Privacy ............................................................................................... 153

5.2 MANAGEMENT OF INTER-ORGANIZATIONAL COMPUTING ........... 154

5.2.1 Collaborative Computing .................................................................... 154
  1. Benefits and Costs involved in CSCW ................................................. 155

5.2.2 Distributed Systems ........................................................................... 156

5.2.3 EDI and Electronic Commerce ......................................................... 157

5.2.4 Outsourcing ......................................................................................... 157
  1. Different approaches to outsourcing .................................................... 158

5.2.5 Application Service Provider ............................................................. 159
  1. Defining an ASP ................................................................................... 160
  2. Defining an Internet ASP ...................................................................... 161
  3. Advantages of ASPs ............................................................................ 161
  4. Examples of ASPs ............................................................................... 162
  5. Things to Ask a Prospective ASP ......................................................... 163

5.3 MANAGEMENT OF END-USER COMPUTING ....................................... 164

5.3.1 Levels of End User Computing ......................................................... 164
6. E BUSINESS ENABLING SOFTWARE

6.1 CUSTOMER RELATIONSHIP MANAGEMENT

6.1.1 Definition

6.1.2 CRM Objectives

6.1.3 Impacts of CRM on Organizations

6.1.4 CRM Applications

6.1.5 The CRM Application Supplier

6.1.6 Selecting CRM Products

6.1.7 How to Succeed with CRM

6.1.8 Conclusion

6.2 SALES FORCE AUTOMATION (SFA)

6.3 SUPPLY CHAIN MANAGEMENT

6.3.1 Introduction

6.3.2 Supply Chain Management Software

6.3.3 Features of a SCM software

5.4 FINANCIAL ANALYSIS AND CONTROL

5.5 ACCOUNTING FOR IS COSTS

5.5.1 Costs incurred in delivering information system

5.5.2 Accounting for costs of an information system

5.5.3 Establishing information systems function as a separate entity
8.2.1 COBIT: Control Objectives for Information and related Technology
1. Definition: ................................................................. 248
2. IT Resources: ............................................................ 248
3. Requirements: .......................................................... 248
4. Process and Domains: ............................................... 248
5. Framework: ............................................................. 249

8.2.2 COSO Report .......................................................... 249

7.4 THE IMPLEMENTATION OF IT SOLUTIONS
7.4.1 Introduction ......................................................... 225
7.4.2 CORE PRINCIPLES .............................................. 226

7.5 IT SERVICE DELIVERY AND SUPPORT SUMMARY
7.5.1 Introduction ......................................................... 227
7.5.2 Core Principles .................................................... 227

7.6 IT MONITORING (EXPOSURE DRAFT)
7.6.1 Why monitor IT? .................................................. 228
7.6.2 What is IT monitoring? ......................................... 229
7.6.3 Key/Core Principles ............................................ 229
7.6.4 What tools are available?
1. Traffic light reports to follow up on projects and strategic initiatives ................................................. 229
2. Performance management through balanced scorecards (and dashboards) .......................................... 230
3. Benchmarking for decision making relative to IT investments for risk and control ................................ 230
4. Active monitoring of the IT infrastructure .............................................................................................. 230
5. Brainstorming for risk management and improvements ........................................................................ 231
6. Internal and external audit for independent assurance ............................................................................ 231
7. Management reporting for executive management review ........................................................................ 231
7.6.5 What is the best approach? ..................................... 231

7.7 PROJECT EXECUTIVE CHECKLIST
7.7.1 Introduction .......................................................... 232
1. The strategic dimension ............................................ 233
2. Checking the benefits ............................................... 233
3. Appraising the project ............................................... 234
4. Managing the change ............................................... 234
5. Managing the risk .................................................... 235
6. Legal compliance ..................................................... 235
7. Security issues .......................................................... 235

7.8 IFAC DISCUSSION PAPER - E BUSINESS AND THE ACCOUNTANT
7.8.1 Introduction .......................................................... 236
7.8.2 E-Business Risks and Opportunities
1. E-Business Opportunities ......................................... 236
2. E-Business IT Risks .................................................. 237
3. E-Business Legal Risks ............................................. 238
7.8.3 E-Business Systems and the Use of E-Business Systems in Enterprises .......................................... 238
7.8.4 E-Business Accounting Principles and Criteria
1. Principles for Reliable Accounting Information ........... 239
2. The Criteria for a Functioning Accounting System ... 240
3. Documentation ....................................................... 241
4. Retention Requirements for E-Business Transactions ... 242
7.8.5 Conclusion ........................................................... 242

8. IT CONTROL FRAMEWORKS ............................................. 246
8.1 INTERNAL CONTROLS FRAMEWORKS: COBIT® AND COSO ........................................................................ 246
8.2 SUMMARIES OF THE DOCUMENTS ........................................................................................................ 247

8.2.1 COBIT: Control Objectives for Information and related Technology
1. 248
2. Definition: ................................................................. 248
3. IT Resources: ............................................................ 248
4. Requirements: .......................................................... 248
5. Process and Domains: ............................................... 248
6. Framework: ............................................................. 249

8.2.2 COSO Report .......................................................... 249
1. Definition: .................................................................................................................................................... 249
2. Components: ................................................................................................................................................ 249
3. Control activities ........................................................................................................................................... 250
4. Other Concepts: .......................................................................................................................................... 250

8.2.3 Conclusion .................................................................................................................................................. 251

8.3 Statement on Auditing Standards (SAS) No. 70 .......................................................................................... 251

8.3.1 Service Auditor’s Reports .................................................................................................................. 252
8.3.2 Benefits to the Service Organization .................................................................................................. 252

8.4 COBIT .......................................................................................................................................................... 253

8.4.1 Components of COBIT Framework: .................................................................................................. 253
1. COBIT Framework ........................................................................................................................................ 253
2. COBIT Control Objectives ....................................................................................................................... 253
3. Audit Guideline ........................................................................................................................................... 253
4. Management Guidelines ............................................................................................................................. 253

8.4.2 Audience .................................................................................................................................................. 255
8.4.3 General Definitions ............................................................................................................................... 255

8.5 The COBIT Framework ............................................................................................................................. 256

8.6 Control Objectives ................................................................................................................................... 260

8.7 COBIT Management Guidelines ............................................................................................................. 261

8.7.1 Maturity Model ....................................................................................................................................... 261
8.7.2 Critical Success Factors ....................................................................................................................... 262
8.7.3 Key Goal Indicators .............................................................................................................................. 264
8.7.4 Key Performance Indicators .................................................................................................................. 265
8.7.5 Conclusion ................................................................................................................................................ 267

8.8 COBIT Audit Guidelines ............................................................................................................................ 267

8.8.1 Audit Process Requirements .................................................................................................................. 268

8.8.2 Generic Audit Guideline .......................................................................................................................... 270
1. Obtaining an Understanding ..................................................................................................................... 270
2. Evaluating the Controls .............................................................................................................................. 271
3. Assessing Compliance ............................................................................................................................... 271
4. Substantiating the Risk ............................................................................................................................... 271

8.8.3 Putting it All Together ............................................................................................................................. 271

8.8.4 Risk Analysis as an Alternative Assessment Approach ......................................................................... 272

8.9 WebTrust .................................................................................................................................................... 272

8.9.1 How WebTrust Works ........................................................................................................................... 273
1. Reduces Risk and Provides Assurance to Management and Boards .......................................................... 273
2. Builds Confidence and Trust for Customers and Visitors ....................................................................... 273
3. Who Provides WebTrust Services ........................................................................................................... 273
5. Site Re-examined Periodically - Customers Know Your Site is in Continuous Compliance .................. 274

8.9.2 Trust Services Principles and Criteria ..................................................................................................... 274
1. On-Line Privacy ......................................................................................................................................... 275
2. Confidentiality ........................................................................................................................................... 275
3. Security .................................................................................................................................................... 277
4. Business Practices/Transaction Integrity ................................................................................................. 277
5. Availability ............................................................................................................................................... 278

8.10 Control Objectives ................................................................................................................................... 278

8.10.1 Effectiveness efficiency, economy of operations ................................................................................. 279
1. IT strategy .................................................................................................................................................. 279
2. Reliance on individual ............................................................................................................................... 279
3. Budgeting .................................................................................................................................................. 279
4. Measures of effectiveness ......................................................................................................................... 280

8.10.2 Reliability of financial reporting ........................................................................................................ 281
TABLE OF CONTENTS

9. IS RISK MANAGEMENT ................................................................. 292

9.1 RISK ANALYSIS ................................................................................. 292

9.2 THREATS TO THE ORGANISATION .................................................. 293

9.2.1 Types of threat ............................................................................ 293

1. Physical damage to hardware or computer media ........................................ 293
2. Damage to data .................................................................................. 293
3. Damage to humans ........................................................................... 293
4. Operational Problems ........................................................................ 294
5. Industrial espionage/fraud .................................................................. 294

9.2.2 The underlying causes of problems ............................................. 294

9.3 SPECIFIC THREATS .......................................................................... 295

9.3.1 Physical threats ............................................................................ 295

1. Fire ................................................................................................. 297
2. Clamminess and bad weather ............................................................... 298
3. Natural disasters/terrorist attack ......................................................... 299
4. Uncontrolled physical environment .................................................... 299
5. Deliberate physical attack/fraud .......................................................... 299

9.3.2 Unauthorised access from inside ................................................... 301

9.3.3 Viruses ....................................................................................... 301

9.3.4 Unauthorised access from outside ................................................ 302

9.3.5 Natural disasters .......................................................................... 302

9.3.6 Technical errors ........................................................................... 304

9.3.7 Human error ............................................................................... 304

9.3.8 Industrial action ........................................................................... 306

9.4 CONSEQUENCES OF THE THREATS .............................................. 306

9.5 GENERAL PROTECTIVE MEASURES ............................................. 307

9.5.1 Physical security .......................................................................... 307

9.5.2 Protection against remote access .................................................. 307

9.5.3 Back up procedures .................................................................... 307

9.5.4 Strict operating procedures ........................................................ 307

9.5.5 Attention to health and safety ....................................................... 307

9.5.6 Encryption of data ....................................................................... 308

9.5.7 Vigilance ..................................................................................... 308

10. IS ORGANIZATIONAL ISSUES ......................................................... 312

10.1 ROLES AND RESPONSIBILITIES .................................................. 312

10.1.1 Information system department ................................................... 312

1. Information systems manager / director .............................................. 312
2. The role of the steering committee ...................................................... 313
3. Administration .................................................................................. 314
4. Database administrator ..................................................................... 314
5. User support Staff .......................................................................... 315
6. System development staff ................................................................. 316
7. Operational personnel ...................................................................... 317
8. Librarian ......................................................................................... 317
9. Security Administration .................................................................... 317
10. Quality Assurance .......................................................................... 318

10.1.2 IS Department and Responsibilities of User Departments ............. 318
10.2 STRUCTURE OF AN IS DEPARTMENT .......................................................... 319

10.2.1 Reasons for decentralising ................................................................. 319
10.2.2 Reasons for Centralisation ............................................................... 320

10.3 IS ENVIRONMENT ................................................................................. 320

10.3.1 Layers of Control ............................................................................. 320
1. Societal layer .......................................................................................... 321
2. Organizational environment layer ......................................................... 321
3. Technology infrastructure layer ............................................................ 321
4. Software layer ....................................................................................... 322
5. Business process layer .......................................................................... 322

10.3.2 Control Environment ........................................................................ 322
1. External regulatory controls ................................................................. 322
2. Board/audit committee governance ..................................................... 329
3. Management philosophy and operating style ....................................... 329
4. Plans/structure of organization ............................................................. 330
5. Method to communicate the assignment of authority and responsibility 330
6. Management control methods ............................................................... 330
7. Human resources policies and practices ............................................... 331
8. Financial policies and practices ............................................................. 334

11. CONTROL ACTIVITIES I ........................................................................ 341

11.1 CONTROL DESIGN ............................................................................... 341
11.1.1 Objectives, framework, environment, activities, monitoring ............. 341
1. Policies: ................................................................................................. 341
2. Procedures: ......................................................................................... 342
11.1.2 Legal, ethical, professional standards /requirements .......................... 342
11.1.3 Preventative/detective/corrective strategies ...................................... 342
11.1.4 Effective control environment (personnel management methods) .. 343
11.1.5 Contingency plans, insurance ........................................................ 343

11.2 CONTROL PROCEDURES ................................................................. 344
11.2.1 Boundary controls .......................................................................... 344
1. Physical access controls .................................................................... 344
2. Logical Access Controls .................................................................... 346
3. LOGICAL SECURITY, TOOLS AND PROCEDURES ......................... 353

12. CONTROL ACTIVITIES II ................................................................. 360

12.1 APPLICATION CONTROL PROCEDURES ........................................ 360
12.1.1 Input Controls ................................................................................ 360
1. Input Authorization ............................................................................ 361
2. Batch control and balancing ............................................................ 362
3. Error Reporting Handling ................................................................. 363
4. Data Validation and Editing ............................................................... 363
5. Source document design ................................................................... 365
6. Data entry screen design ................................................................... 365
7. Caption design .................................................................................. 366
8. Data entry Field design ..................................................................... 366
12.1.2 Processing Control Procedures ...................................................... 366
14.8.1 Suggested Solution .......................................................... 410
14.9 ARG ......................................................................................... 410
   14.9.1 Suggested Solution ............................................................ 412
14.10 TEP PLC .................................................................................. 413
   14.10.1 Suggested Solution ............................................................ 415
14.11 DS LTD’S .................................................................................. 416
   14.11.1 Suggested Solution ............................................................ 418
14.12 VEEMAX ................................................................................... 419
   14.12.1 Suggested Solution ............................................................ 420
14.13 PATAK’S FINE SILKS .............................................................. 421
   14.13.1 Suggested Solution ............................................................ 421
14.14 CONTROLS ............................................................................... 423
   14.14.1 Suggested Solution ............................................................ 424
   1. Potential Problem Areas ........................................................... 424
Information Technology Strategy and Management

1. Information & Information Systems
2. Strategic Planning of Information systems
3. Strategic Planning of Information Systems II
4. Internet & E-Commerce
5. Management of Information Technology
6. E business enabling software
7. IFAC Guidelines/Discussion Papers
Introduction

Welcome to Paper F21 Information Technology Management, Security and Control. This material has been specifically written for Paper F 21 of the Institute of Chartered Accountants of Pakistan (ICAP). As with all Module F papers, the examination for this paper will require you to apply knowledge, rather than simply testing your ability to recall information. So, when working through this Study Text, consider how the material could be applied or adapted for use in a range of business situations.

Study Guide

Although this chapter may not be directly examinable, but the scenario question of the examination provides the examiner with an ideal opportunity to test your understanding of the importance of an organisation utilising suitable systems to meet information requirements. It also revises the concepts relevant to this study text from the previous Module D paper, and thus forms a strong foundation for advanced study. Students should be able to understand and apply knowledge gained in this chapter to Scenario questions in the exams.
1. INFORMATION & INFORMATION SYSTEMS

1.1 INFORMATION REQUIREMENTS

KEY TERMS

Data is the raw material for data processing. Data consists of numbers, letters and symbols and relates to facts, events, and transactions. Information is data that has been processed in such a way as to be meaningful to the person who receives it. The Syllabus defines information as in organizational and management solution, based on information technology, to any challenge posed by the environment.

Information is a vital resource to all organisations. It is an important ingredient in its day-to-day operations, and it is also useful as a means of communicating with other organisations and individuals.

Historically the organisation’s information needs were categorised as follows:

(a) planning
(b) monitoring performance
(c) control
(d) decision making
(e) recording and processing transactions
(f) communication.

However, this list tends to treat information as something to help management in the organisation. The accounting system, for example, falls into this category. However, more and more organisations see information as a valuable strategic resource, which can help them gain competitive advantage rather than merely aid management. For example, credit card companies can analyse expenditure and use the results to specifically target mail-shots at likely customers. Hotel chains that record customer preferences increase customer loyalty.
1.1.1 Types of Information

1. Strategic information

Strategic management will be involved in making decisions about:

(a) the objectives of the organisation
(b) changes in these objectives
(c) the resources used to attain the objectives
(d) policies governing:
   (i) acquisition
   (ii) use
   (iii) disposition of these resources.

Strategic planning is usually, but not always, concerned with the long term. For example, a company specialising in production and sale of tobacco products may forecast a declining market for these products and may, therefore, decide to change its objectives to allow a progressive move into the leisure industry, which it considers to be expanding. Strategic decisions involve the formulation of the new objectives and deciding on the manner in which these new objectives will be achieved, ie, by acquisition of companies which are already established in the industry, or by starting new businesses itself (‘organic growth’).
Although strategic planning is concerned with long term goals, it often involves short term action. For example, the acquisition of a new company in the leisure industry is made in order to fulfil a long term objective but it requires short-term planning and control action, all of which is classified under the heading of strategic planning.

Strategic information is:
- Derived from both internal and external sources
- Summarized at a high level
- Relevant to the long term
- Concerned with the whole organization
- Often prepared on an 'ad hoc' basis
- Both quantitative and qualitative
- Uncertain, as the future cannot be accurately predicted

2. Tactical information
Tactical information is used to decide how the resources of the business should be employed, and to monitor how they are being and have been employed. Such information includes productivity measurements (output per hour) budgetary control or variance analysis reports, and cash flow forecasts, staffing levels and profit results within a particular department of the organisation, labour turnover statistics within a department and short-term purchasing requirements.

Tactical information is:
- Primarily generated internally (but may have a limited external component)
- Summarised at a lower level
- Relevant to the short and medium term
- Concerned with activities or departments
- Prepared routinely and regularly
- Based on quantitative measures

3. Operational information
Operational information is used to ensure that specific operational tasks are planned carried out as intended. In the payroll office, for example; operational information relating to day-rate labour will include the hours worked each week by each employee, the rate of pay per hour, details of deductions, and for the purpose of wages analysis, details of the time each employee spent on individual jobs during the week. In this example, the information is required, weekly, but more urgent operational information, such as the amount of raw materials being input to a production process, may be required daily, hourly, or in the case of automated production, second by second.

Operational information is:
- Derived from internal sources
- Detailed, being the processing of raw data
- Relevant to the immediate term
- Task-specific
- Prepared very frequently
- Largely quantitative
1.1.2 Improvements to information

The table on the following contains suggestions as to how poor information can be improved.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Example of possible improvements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accurate</td>
<td>Use computerised systems with automatic-input checks rather than manual systems. Allow sufficient time for collation and analysis of data if pinpoint accuracy is crucial. Incorporate elements of probability within projections so that the required response to different future scenarios can be assessed.</td>
</tr>
<tr>
<td>Complete</td>
<td>Include past data as a reference point for future projections. Include any planned developments, such as new products. Information about future demand would be more useful than information about past demand. Include external data.</td>
</tr>
<tr>
<td>Cost-beneficial</td>
<td>Always bear in mind whether the benefit of having the information is greater than the cost of obtaining it.</td>
</tr>
<tr>
<td>User-targeted</td>
<td>Information should be summarised and resent together with relevant ratios or percentages.</td>
</tr>
<tr>
<td>Relevant</td>
<td>The purpose of the report should be defined. It may be trying to fulfill too many purposes at once. Perhaps several shorter reports would be more effective. Information should include exception reporting, where only those items that are worthy of note - and the control actions taken by more junior managers to deal with them - are reported.</td>
</tr>
<tr>
<td>Authoritative</td>
<td>Use reliable sources and experienced personnel. If some figures are derived from other figures the method of derivation should be explained.</td>
</tr>
<tr>
<td>Timely</td>
<td>Information collection and analysis by production managers needs to be speeded up considerably, probably by the introduction of better information systems.</td>
</tr>
<tr>
<td>Easy to use</td>
<td>Graphical presentation, allowing trends to be quickly assimilated and relevant action decided upon. Alternative methods of presentation should be considered, such as graphs or charts, to make it easier to review the information at a glance. Numerical information is sometimes best summarised in narrative form or vice versa.</td>
</tr>
<tr>
<td></td>
<td>A ‘house style’ for reports should be devised and adhered to by all. This would cover such matters as number of decimal places to use, table headings and labels, paragraph numbering and so on.</td>
</tr>
</tbody>
</table>

1.2 The Value and Cost of Information

Information within an information system must be provided at an appropriate cost, or to put it another way, the information should have a value to the user over and above the cost of obtaining that information.

For information to have value, it must lead to a decision to take action that results in:

- Reducing unnecessary costs - an investigation into the causes of adverse cost variances may uncover inefficiencies and wastage, which can be eliminated in future.
- Eliminating losses.
- Adopting better marketing strategies - analysis of sales by product line from point-of-sale terminals may direct management’s attention to those products and locations, which show the highest profit potential. Market research studies enable managers to make decisions on the qualities of products which consumers value the most.
• Attaining a competitive advantage - there are many ways in which improved information flow can lead to a competitive advantage. Installing a direct computer link between a customer and your organisation makes it easier for that customer to deal with you and helps to safeguard sales.

• Better analysis of ‘cost drivers’ - detailed information about the causes of costs and the factors which ‘drive costs’ (Activity Based Costing) enables more realistic budgets to be set, which in turn should result in scarce resources being applied in the most profitable manner.

• Optimising techniques - information from operational research techniques such as linear programming, or critical path analysis, is worthwhile if it enables scarce resources to be applied more profitably.

• Increasing sales.
• Better use of resources.
• Prevention of fraud.
• Providing management with information about the consequences of alternative courses of action.

1.2.1 Assessing the value of information

Information has no value if it is not used. Neither has it any value if it is known already (no ‘surprise value’). In order to assess the value of information, the following questions can be asked:

• What information is provided?
• What is it used for?
• Who uses it?
• How often is it used?
• What is achieved by using it?
• Is it used as often as it is provided?
• What other relevant information is available which could be used instead?

The value of information must also relate to the frequency of its provision, and to the level in the management hierarchy where it is sent and used. Operational management needs more regular control information for decision-making, perhaps daily or weekly, whereas middle and senior management (tactical and strategic) might need information less frequently - monthly, quarterly or yearly.

Information may have value in a number of different ways. Decision theory identifies three situations under which decisions are made:

• Certainty
• Risk
• Uncertainty

Decision-making under conditions of certainty assumes that certain knowledge exists of the outcome of each of the various options available to the decision-taker. Decision-making under conditions of risk assumes that for each option available to the decision-taker, all possible outcomes are known and that probability of each outcome occurring is also known. Uncertain decision-making conditions are the same as risk but without the knowledge of probabilities. A monetary value of information can be calculated for decisions made under these conditions.
The value of information in decision-making situation is said to be the difference in the values of outcomes in a decision with and without the information minus the cost of obtaining the information. In other words, a manager will make a decision based upon the information currently known. If additional information is available, which makes the manager take different decision, then the value of that information is the savings or profits made as a result of taking the different decision. This is then adjusted for the cost of obtaining the information. The cost may be:

- Some monetary value arising from preparing the information internally
- The cost of purchasing the information from external sources
- The cost of the delay to the decision whilst the information is prepared

### 1.2.2 Cost of information

The cost of information can be classified under three general headings:

(a) The cost of **designing and setting up the system** that produces the information. This includes:
   (i) systems design
   (ii) testing
   (iii) capital costs of equipment
   (iv) installation
   (v) training.

(b) The **day-to-day running costs** of the system providing the information, including:
   (i) staff salaries
   (ii) supplies (paper, disks, etc)
   (iii) other expenses.

(c) **Storage** costs including:
   (i) hardware costs
   (ii) space costs
   (iii) retrieval costs.

### Question 1

The information is said to be valuable if its acquisition is followed by the course of action. What considerations you may have regarding the value of information?

### Answer

(a) What information is provided?
(b) What is it used?
(c) Who uses it?
(d) How often is it used?
(e) Does the frequency with it is used coincide with the frequency of provision?
(f) What is achieved by using?
(g) What other relevant information is available which could be used instead?

An assessment of the information can be derived in this way, and the cost of obtaining it should then be compared against in value. On the basis of this comparison, it can be decided whether certain items of information are worth having. It should be remembered that there may also be intangible benefits which may be harder to quantify.

### 1.2.3 Traditional methods for assessing cost

Traditional investment appraisal methods can be applied with varying degrees of success to problems of this kind. There principal methods of evaluating a capital project are: the payback method, the accounting rate of return and discounted cash flow methods such as net present value and internal rate of return. These methods should be familiar from your earlier studies.

**Question 2**

Draw up a table which identifies, for each of the four methods of evaluating a project (payback, APR, NPV, IRR), two advantages and two disadvantages.

**Answer**

<table>
<thead>
<tr>
<th>Method</th>
<th>Advantage</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Easy to calculate</td>
<td>Ignores cash flows after payback period</td>
</tr>
<tr>
<td></td>
<td>• Favours projects that offer quick returns</td>
<td>Only a crude measure of timing of a project’s cash flows.</td>
</tr>
<tr>
<td>ARR</td>
<td>• Easy to calculate</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Easy to understand</td>
<td>• Doesn’t allow for timing of inflows/outflows of cash</td>
</tr>
<tr>
<td>NPV</td>
<td>• Uses relevant cost approach by concentrating on cash flows</td>
<td>• Subject to accounting conventions.</td>
</tr>
<tr>
<td></td>
<td>• Represents increase to company’s wealth, expressed in present day terms</td>
<td>• Not easily understood by laymen.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cost of capital may be difficult to calculate.</td>
</tr>
<tr>
<td>IRR</td>
<td>• Uses opportunity cost approach</td>
<td>• Could get several IRRs or no IRRs</td>
</tr>
<tr>
<td></td>
<td>• Represents breakeven borrowing rate.</td>
<td>• Ignores scale of project whereas NPV takes this into account.</td>
</tr>
</tbody>
</table>

### 1.2.4 The benefits of a proposed information system

The benefits from a proposed information system should be evaluated against the costs. To quantify the benefits several factors need to be considered.

(a) **Savings** generated because the old system will no longer be operated. The savings may include **staff costs** and **other operating costs**.

Extra savings or revenue benefits because of the **improvements or enhancements** that the new system should bring:

(i) Possibly more **sales revenue** and so additional contribution.

(ii) Better **stock control** (with a new stock control system) and so fewer stock losses from obsolescence and deterioration.
(iii) **Savings in staff time**, resulting perhaps in reduced future staff growth. Some benefits might be **intangible**, or impossible to give a money value to. Even if they cannot be quantified, they must be identified and fully explained. It is arguable that the large proportion of all computerized information systems benefits is intangible.

(a) Greater **customer satisfaction**, arising from a more prompt service (e.g. because of a computerized sales and delivery services).

(b) Improved **staff morale** from working with a ‘better’ system.

(c) **Better decision making** is hard to quantify, but may result from a better MIS, DSS or ESS.

### 1.3 **Information Management and Decision Making**

Information must be managed just like any other organizational resource.

#### KEY TERM

**Information Management (IM) strategy** refers to the basic approach an organization has to the management of its information systems, including:

- Planning IS/IT developments
- Organisational environment of IS
- Control
- Technology

Information management entails the following **tasks**.

(a) Identifying current and future **information needs**.

(b) Identifying information **sources**.

(c) **Collecting** the information.

(d) **Storing** the information.

(e) Facilitating existing methods of using information and identifying new ways of using it.

(f) Ensuring that information is **communicated** to those who need it, and is not **communicated** to those who are not entitled to see it.

#### 1.3.1 **Structured and unstructured decisions**

Decisions can be broken down into two main types, those which can be made following a given set of rules (structured decisions), and those which can only be made subjectively (unstructured decisions).

(a) **Structured (or programmed) decisions**

This means that:

- decisions can be taken objectively;
- there is a clearly defined method of solving the problem;
- generally, there is a right answer.
There are a number of operational research techniques to help reach structured decisions. These include linear programming and network analysis.

An example of a structured decision would be deciding on the minimum price at which a product should be sold; the minimum price should equal the marginal cost of the product.

(b) **Unstructured decisions**

This sort of decision can only be reached subjectively. An example would be the hiring of a new employee - would they ‘fit in’ with the company ethos and existing practices? At what price should a product be sold - high price/low volume or low price/high volume?

Efforts are often made to turn unstructured decisions into structured ones by setting hard-and-fast criteria. This practice is gaining ground in such fields as recruitment and granting credit facilities.

In addition, you may also encounter **Semi-structured decisions**.

These lie between structured and unstructured decisions. Some parts of the decision-making process are programmable (structured), others not. For example, deciding how much stock to maintain for a product will involve an analysis of prior usage (programmable) but this may then have to be adjusted if a competitor has recently gone out of business and we expect additional, but unknown, demand.

Other terminology you should know:

**Analytical decisions**

An analytical decision is one that is based on an analysis of information that has been systematically acquired and evaluated. Much of the information will be quantitative.

**Heuristic decisions**

These solutions will usually depend on trial and error. Common sense, past experience and general guidelines may be used to help, but the decision maker is not applying any techniques that will guarantee the correct answer first time.

**1.3.2 Information systems to support decision making**

As has been discussed, the different decision levels within an organisation need different types of information. The information systems providing that information must therefore vary so that appropriate information is provided to each level of management. The information systems must vary accordingly. In general terms, there are three basic types of information system required to support the three levels of management already discussed. The diagram below re-iterates those management levels and indicates the general type of information system that will be provided for that management level.
Within this hierarchy, strategic planning will normally involve making unstructured decisions and operational planning will normally involve making structured decisions. Tactical planning is caught in the middle and will involve a mixture of both decision types.

1.4 TYPES OF INFORMATION SYSTEM

An introduction to the different types of information system is given below.

1. Operational level information systems

Operational decisions are programmable and require specific and detailed information. Many of the decisions taken are able to be programmed into the computer.

Most of the information used for operational decisions comes from the simplest form of information system, transaction processing systems. The outputs from these systems are simple reports and sorted lists of transactions.

Also used by operational managers are reports comparing their performance with target, and with other operational managers.

2. Tactical level information systems

Tactical information is also largely fed from transaction processing systems, although it may also come from external sources. Tactical managers must make use of a wider variety of data.

Many tactical MIS will be informal, and the tactical manager will be responsible for knitting together the different strands of information available. The formal MIS will concentrate on exception reporting as well as summaries of performance within the manager's sphere of influence. If an exception report triggers action by the manager, there is likely to be the ability to delve deeper into the detailed operational data.

3. Strategic level information systems

There is a much wider range of information needs at the strategic level, which are considerably more difficult to predict than at the other levels of management. This usually leads to a greater reliance on informal and ad hoc information systems.

The different information needs of the organisation have led to different types of system being developed - MIS, DSS (Decision Support Systems), EIS (Executive Information System) and Expert systems.
TYPES OF INFORMATION SYSTEM

These levels correspond roughly to the Strategic, tactical and operational level that have already been explained. The knowledge level of management has been introduced over the last few years to recognise the contribution of managers who use computerised systems to expand the knowledge base of an organisation. The summary of these systems can now be provided as follows:

- Operational level systems are provided to support operational managers by tracking the individual transactions that occur within an organisation. Detail such as individual sales invoices, cash receipts, specific goods sold to one customer etc. will be found within this system. All the data will be collected into the Transaction Processing System.

- At the knowledge level, systems are required to support the knowledge and data workers within an organisation. The aim of these systems is to help the organisation introduce new knowledge into the organisation as well as organise and provide access to existing knowledge. Information systems used by knowledge workers include the Office Automation System (OAS) and the Knowledge Work System (KWS). The OAS provides the basic electronic support in form of word processors, spreadsheets, diaries etc, on the computer systems. The KWS provides access to other computer applications such as Computer Assisted Design, Virtual Reality and advanced graphics packages to help knowledge workers express their work in different ways.

- The management level within an organisation is designed to assist with the monitoring and control of other systems. They will tend to provide reports on an exception basis to support the decision making of more senior managers. Decision Support Systems (DSS) are used to provide this summary information while Management Information Systems provide summaries of the transaction data from the TPS.

- Finally, the strategic level systems help managers address more longer term issues and problems such as the overall strategic direction of the organisation, where to invest in new factories and products, or the production of five year plans. The Executive Support Systems will provide management with the summarised strategic information needed to make these decisions.
### 1.4.2 Executive Support Systems (ESS)

**KEY TERM**

An executive support system is an interactive method of allowing executives and managers to access information for monitoring the operations of the organisation and scanning general business conditions.

An ESS should provide senior managers with easy access to key internal and external information. The system summarises tracks strategically critical information, possibly drawn from internal MIS and DSS, but also including data from external sources eg competitors, legislation, external databases such as Reuters.

An ESS is likely to have the following features.
- Flexibility
- Quick response time
- Sophisticated data analysis and modelling tools

### 1.4.3 Management Information Systems (MIS)

**KEY TERM**

MIS is an integrated, computer-based, user-machine system that provides information for supporting operations and decision-making functions.

Management Information Systems can be distinguished from other information systems within an organisation by reference to the specific features of that system.

- Provision of support for the structured decision making at all management levels
- Provision of on-line access to the TPS of the organisation, to give summary information on the performance of the organisation
- An internal rather than external focus, with detail being provided on the organisation itself rather than competitors or the overall economic environment
- Provision of more detailed information on the organisation’s operations, where required. This is the “drill down” facility so often associated with a MIS.
- Use of relatively simple programs to produce summaries and comparisons compared to more detailed mathematical models or statistical techniques found in a DSS, for example.

**Example**

Management Information Systems can be found in almost any organisation. A few examples are given below.

- In car manufacturing, systems to summarise sales of motor vehicles to assist in trend analysis and hiring of new workers
- In a firm of accountants, summarising work performed on different audit engagements to assist in fee negotiation.
- In a training company, provision of details of students booked onto different courses to indicate the size of lecture rooms required and number of lecturers for each subject.
In a manufacturing company, provision of stock ageing analysis to determine the amount of stock provision in the financial statements.

### 1.4.4 **Decision Support Systems (DSS)**

**KEY TERM**

Decision Support System (DSS) combine data and analytical models or data analysis tools to support semi-structured and unstructured decision making.

DSS are used by management to assist in making decisions on issues which are subject to high levels of uncertainty about the problem, the various *responses* which management could undertake or the likely *impact* of those actions.

Many decision support systems are based on spreadsheets. Normally the output from a spreadsheet is simply a columnar report, but they can also be used to produce graphs and charts.

More specialised decision support systems, such as treasury or marketing systems, can produce output in a variety of forms. The user can often specify output and design reports on the screen for a specific purpose, as individual decisions are often specialised and infrequent.
Case Example

CNN Interactive

This report comes from a decision support system used by marketing staff in planning corporate entertainment events. It shows a real-time weather forecast for the region in which the event is to be held. Note the use of text and graphics to convey clear messages.

Further characteristics of decision-support systems include:

- Broad-based approach to supporting decision-making - they help to identify important future trends, adapting the organisation to changing conditions.
- Decision-maker retains control over the decision-making process - VDU allows the capability to retrieve, manipulate, present, and store data.
- Utilisation of appropriate mathematical and statistical models - to assist the decision-maker in evaluating alternative solutions.
- Query capabilities to obtain information by request - the interactive mode of the system extends the individual’s reasoning process.
- Output directed to organisation personnel at all levels - it can also provide lower management and their operating personnel with the necessary output for supporting decisions or controlling current operations.
- Integrated sub-systems allow managers and personnel to retrieve and manipulate information to support decisions.
- Comprehensive database.
• Easy-to-use approach - the individual feels comfortable with the system rather than intimidated by it.
• Adaptive system - system changes may be effected within weeks or months.

1.4.5 Knowledge Work Systems (KWS)

KEY TERMS

Knowledge Work Systems (KWS) are information systems that facilitate the creation and integration of new knowledge into an organisation.

Knowledge Workers are people whose jobs consist of primarily creating new information and knowledge. They are often members of a profession such as doctors, engineers, lawyers and scientists.

Knowledge work means creating new knowledge or information by research, experimentation and investigation into existing trends and products. There are many different areas of knowledge work, and each one can be supported by its own collection of Knowledge Work Systems (KWS). Knowledge workers themselves perform many essential tasks within an organisation including:

• Keeping the organisation up-to-date with new knowledge as it develops outside the company, in areas such as technology, science and the humanities.
• Providing advice inside the organisation on the use of new knowledge, and
• Acting as change agents by actually recommending and implementing change within an organisation.

Examples of knowledge work systems

Knowledge Work Systems may include any of the following examples. Remember that the specific system will be tailored to the requirements of the individual knowledge worker.

(i) Virtual reality

Virtual Reality (VR) provides access to interactive graphics software and hardware. This is used to create computer-generated simulations in various areas including design of new buildings, testing new vehicles and even assisting in hospitals to provide simulations of operations for training purposes.

Use of VR normally means wearing specialist equipment such as visors and clothing to transmit movement back to the computer. With sufficient processing power, the VR world can appear to be “real” and the user may forget that the experience is really “virtual”!

(ii) Computer Aided Design

Computer Aided Design (CAD) is used to automate the creating and revision of drawings and designs. CAD means that items, ranging from vases to motor vehicles, can be designed and amended using the computer software with a physical item being produced only at the end of the design process. This approach saves the time and money normally spent in producing and refining many different physical designs.
(iii) **Virtual Reality Modelling Language**

VRML is an extension of VR, allowing simulations of real-world environments to be downloaded via the Internet. One specific application of the software is downloading training material to assist engineers install or operate large pieces of machinery.

(iv) **Investment workstation**

Investment workstations provide financial knowledge workers with all the information they require to make investment decisions. Previously, this information had to be obtained from a number of independent and incompatible systems. The investment workstation provides all the information within one computer system, giving considerable time and money saving for the organisation.

---

**KEY TERM**

Office Automation Systems (OAS) are computer systems designed to increase the productivity of data and information workers.

---

**1.4.6 Office Automation Systems (OAS)**

- OAS support the major activities performed in a typical office such as document management, facilitating communication and managing data.

**Examples of Office Automation applications**

Typical applications within an Office Automation System are explained below.

(i) **Word processing**

Word processing software allows users to create, edit, format, store and print text documents. They are probably the most commonly-used of all OAS applications because document production is carried out in every office; in fact many offices are designed simply to produce documents.

Word processed documents can be shared using Groupware so that more than one user can edit the document at once. This is particularly useful where some form of “brainstorming” of ideas is required. A document management system (such as Windows Explorer) will allow access to word-processed and other documents across networks to assist in the sharing of information.

(ii) **Desktop publishing**

This is an extension of word processing. Desktop publishing (or DTP), allows for the production of high quality documents and newspapers by allowing text, graphics and diagrams to be organised on-screen into a newspaper type format.

(iii) **Document imaging systems**

A document imaging system converts paper documents and images into electronic form so they can be stored and accessed on a computer system. When items of mail are received, they are scanned
into the computer and stored on high capacity storage media such as optical disk. The paper letters are thrown away. Data workers can access the stored information using keywords (such as the name of the person writing the letter) saving considerable time in finding the hardcopy letter within a paper filing system.

Within the system, optical disks are stored in a “jukebox”, which is simply a device for storing and retrieving large numbers of optical disks. The index to the documents, including the keywords for accessing those documents, is stored on an index server.

(iv) **Scheduling**

Scheduling software will include on-line diaries and calendars that can be accessed and updated by a large number of users. Write access to diaries will normally be limited, although general read access allows any worker to find the location of any other colleague. The diary feature in Lotus Notes or MS Outlook are examples of this type of system.

(v) **Communication**

Communication software will involve some form of e-mail application, although voice mail, intranets and video conferencing may all be included within this system. An Intranet involves the provision of information in Internet style format, with access being restricted to users within one organisation. Video-conferencing allows workers to communicate via video, with meetings being arranged worldwide, saving on travelling costs.

(vi) **Managing data**

Various data management systems will be available such as databases and spreadsheets as well as interfaces to large corporate data stores and data warehouses.

### 1.4.7 Transaction Processing Systems (TPS)

#### KEY TERM
A Transaction Processing System (TPS) performs and records routine transactions.

A Transaction Processing System (TPS) is the main system serving the operational level of the organisation. It records all of the daily routine transactions that take place within an organisation, and is used primarily by clerks and operations staffs that either input or maintain the data on the system.

TPS are used for routine tasks in which data items or transactions must be processed to that operations can continue. TPS support most business functions in most types of organizations. The following table shows a range of TPS applications.

<table>
<thead>
<tr>
<th>Major functions of system</th>
<th>Sales/ marketing systems</th>
<th>Manufacturing /production systems</th>
<th>Finance/ accounting systems</th>
<th>Human resources systems</th>
<th>Other types (e.g. university)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sales management</td>
<td>•</td>
<td>• Scheduling</td>
<td>• Budgeting</td>
<td>• Personnel records</td>
<td>• Admissions</td>
</tr>
<tr>
<td>Market research</td>
<td>•</td>
<td>• Purchasing Shipping/</td>
<td>• General Ledger</td>
<td>• Benefits</td>
<td>• Student academic</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Course records</td>
</tr>
</tbody>
</table>
1. **Batch Processing and On-line processing**

ATPS will process transactions using either batch processing or on-line processing. Batch processing involves transactions being **grouped** and **stored** before being processed at regular intervals, such as daily, weekly or monthly. Because data is not input as soon as it is received the system will not always be up-to-date. The lack of up-to-date information means batch processing is usually not suitable for systems involving customer contact. Batch processing is suitable for internal, regular tasks such as payroll. On-line processing involves transactions being input and processed immediately. An airline ticket sales and reservation system is an example. The workings of both processing methods are shown in the following diagram.

# Expert Systems

**KEY TERM**

An expert system is a computerised package designed to allow non-expert users to make expert decisions.

Expert systems are mentioned here because they provide useful information to management, even though they are not part of the hierarchy of information systems discussed previously.

The expert system stores the knowledge and experience of a number of experts in a structured database known as a ‘knowledge base. A ‘knowledge acquisition module gathers new and updated knowledge, often on-line or by frequent upgrades.

The user accesses the system through a user-friendly ‘graphical user interface (GUI) and asks questions of the system, or is prompted with questions by the system. The operating software or ‘inference engine’ then uses a mixture of rule-based logic and ‘fuzzy logic to infer a solution from the knowledge base.

**Examples of expert systems**

There are many examples of expert systems in such areas of business as credit control, engineering and recruitment. Even something as simple as the control panel of a photocopier can be considered an expert
system, as it allows the operator to diagnose the cause of a machine breakdown and to fix the machine. They are used widely in the following areas:

- law (e.g., conveyancing)
- taxation (e.g., personal tax)
- banking (e.g., granting credit)
- medicine (e.g., diagnosis of symptoms)
- defence (e.g., aircraft recognition).

Expert Systems can be used at a variety of different levels. At the simplest level they can give factual answers to technical questions. At a more complex level they can suggest how a decision should be made, recommending a course of action. In this respect, they go further than Decision Support Systems.

1.5 Knowledge Management

This section examines what is meant by knowledge and knowledge management (KM), outlines approaches to the latter with particular reference to the contribution of information and communication technologies on the one hand and changing organisations and people on the other. It concludes with a brief comment on the measurement of KM.

1.5.1 What is knowledge?

Students will be familiar with the distinction drawn between data and information. The former being defined as observations of facts outside of any context, the latter being data within a meaningful context. One way of understanding what is meant by knowledge is to think of it as being ‘information-plus’ or information combined with experience, context, interpretation, reflection and is highly contextual. It is a high-value form of information that is ready for application to decisions and actions within organisations.

Theorists make a distinction between two categories of knowledge, that which is said to be tacit and that which is explicit.

- **Tacit knowledge** Knowledge that “is subconsciously understood and applied, difficult to articulate, developed from direct experience and action, and usually shared through highly interactive conversation, storytelling and shared experience.”
- **Explicit knowledge** Explicit knowledge in contrast “is more precisely and formally articulated, although removed from the original context of creation or use...”

Examples of ‘tacit’ knowledge would be ‘best practice’ performed in an organisation, management skills, technologies, customer, market and competitor intelligence. Explicit knowledge would include for example the content of spreadsheets, management reports, procedural and training manuals.

1. Knowledge and intellectual capital

Intellectual capital is an expression that is sometimes used interchangeably with knowledge. As an ‘intangible asset’ however it usually refers to copyrights, patents, licenses, royalties’ etc a narrower definition distinct from knowledge (capital) as defined above which has definite human (capital) connotations.
These definitions may be seen as different points on a continuum with data at one end and tacit knowledge at the other. The further we move towards the tacit the more important is context.

2. **Knowledge processes**

Whether explicit or tacit, a number of processes are found in organisations in relation to knowledge. It is useful to recognise this as it gives us an insight into how knowledge may be ‘managed’ (knowledge management) to the organisation’s advantage.

Ruggles points to eight knowledge processes:

- Generating new knowledge.
- Accessing valuable knowledge from outside sources.
- Using accessible knowledge in decision making.
- Embedding knowledge processes, products, and/or services representing knowledge in documents, databases, and software.
- Facilitating knowledge growth through culture and incentives.
- Transferring existing knowledge into other parts of the organisation.
- Measuring the value of knowledge assets and/or impact of knowledge management.

As we shall see later attempts at KM focus on improving these processes within organisations (but usually towards only one or two processes at any one point in time).

1.5.2 **Knowledge management**

Knowledge management is the attempt to improve/maximise the use of knowledge which exists in an organisation. More specifically it aims to stimulate its creation and encourage its capture, sorting, sifting, access, linking, storage and distribution. In short, it addresses itself to the processes identified above.

1. **Why knowledge management is important**

Traditionally economics textbooks emphasise the quantity, quality and combination of ‘factors’ of production (land, labour, capital and enterprise) in competitive advantage. Nowadays, however, it is argued that the creation and exploitation of ‘difficult-to-replicate’ assets such as knowledge is crucial if competitive advantage is to be gained and retained.

The strength of this argument is likely to vary from sector to sector in the economy and is probably at its weakest in respect of organisations in the public sector where political influence is strong and for utilities where regulatory regimes rather than market pressures are key drivers for efficiency. The argument is strong especially in respect of web services, electronic banking, brokerage and biotechnology and to large swathes of manufacturing where a number of areas of expertise need to be brought together to bring products to market.

While communications was seen as the top priority in making their company a good one by business leaders surveyed by Smythe Doward Lambert the change management consultancy knowledge was chosen as a priority by 91%.

At a pragmatic (operational) level a survey of 1,051 organisations by the American Management Associations revealed strong agreement by respondents to the statement “Knowledge management is vital to
our company’s future success”. The same sample reported positive measurable results from knowledge management in especially higher customer satisfaction, better employee satisfaction, product/service innovation and improved profitability.

1.5.3 Approaches to knowledge management

How can organisations manage knowledge effectively through managing its creation and exploitation? To date there have been two general approaches: through the application of information and communication technologies and to a lesser extent via paying attention to the human factor in organisations.

1. Dealing with the human factor

The aim is to create an organisational climate or culture in which employees have a positive orientation towards knowledge and are not inhibited in sharing the knowledge they have. A study in 1997 carried out by the Ernst and Young Centre for Business Innovation found that among US and European organisations “changing people’s behaviour” was seen as the biggest difficulty in managing knowledge and the biggest impediment to its translation was culture.9

Knowledge has often been used in organisations to gain advantage in terms of influence and self-advancement by those who have it over those who do not. Change in culture and individual behaviour must aim towards encouraging the use of knowledge not for individual advantage but for the benefit of the organisation as a whole. The aim is to create a knowledge-sharing environment. This typically requires a change in organisational structure, values, leadership behaviour and various human resource management practices.

2. Organisation structure

Ridderstrale10 says organisation structures need to move away from the bureaucratic model with its extensive hierarchies, precise definition of role typically within ‘functions’, fixed patterns of communication and working procedures.

Figure 2 summarises Ridderstrale’s prescription for an organisational architecture favourable to effective KM. In large measure what is advocated reflects changes in organisation structure supported by most management writers in recent years and have been put into practice by many organisations.

<table>
<thead>
<tr>
<th>Figure 2 Organisational characteristics for effective KM</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Flatter and decentralised structure allowing decisions to be taken where critical knowledge is located.</td>
</tr>
<tr>
<td>• Flexibility which allows movement of personnel between functions, business areas, divisions or countries to respond to opportunities (or problems) which span boundaries.</td>
</tr>
<tr>
<td>• Use of employees in temporary and boundary spanning projects not restrained by positioning in a hierarchy, supported by resources, given influence and kept within the structure through shared norms, values and vision.</td>
</tr>
</tbody>
</table>

(From Ridderstrale op. cit.)

In addition to making recommendations to organisation structure, Ridderstrale emphasises (as do others – see below) the importance of shared ownership (e.g. through stock options through which all may benefit from improvements in organisational performance), a shared culture, vision and values and rewards for knowledge sharing. Writers on KM are in agreement in stressing the importance of shared values which have been identified in field research by the Roffey Park Management Institute as:
• openness
• trust
• acknowledgement of individual contributions
• fairness

3. Top executive behaviour

Based upon experience of working with clients, Gersling et al consultants with Andersen Consulting (now Accenture) describe the actions that top executives need to take to bring about and sustain a knowledge sharing environment or culture. Senior executives they write must demonstrate commitment through the sponsorship of KM and motivate knowledge sharing behaviour through their own actions (Figure 3).

![Figure 3 Action to change towards and sustain a knowledge-sharing environment](image)

(Based on Gersting et al. op. cit.)

4. The role of information and communication technologies (ICT).

An ICT infrastructure has, according to Zach a contribution to make in the following areas:

• Capturing knowledge.
• Defining, storing, categorising, indexing, and linking digital objects that correspond to knowledge units.
• Searching for (“pulling”) and subscribing to (“pushing”) relevant content.
• Presenting content with sufficient flexibility to render it meaningful and applicable across multiple contexts of use.

In terms of technologies the following are important:

• Intranet: to support access and exchange both within an organisation and between it and close allies such as customers and suppliers.
• Data warehousing/repositories: the storage and making available knowledge wrapped in various degrees of context.
• Decision support systems: incorporating relevant knowledge.
• Group-ware to support collaboration: facilitating the sharing of ideas in a free-flowing manner including discussion between participants.
• Desktop video-conferencing: for person-to-person contact important for the exchange of tacit knowledge.
• E-mail: as for desktop video-conferencing.
5. **Organisation, People or ICT?**

Organisations apparently adopt an approach to KM which either emphasises organisation and people (HR) or the application of ICT. Few take an integrated approach. The experience of Andersen Consulting (Accenture) consultants is that efforts by HR or ICT people alone are likely to fail in KM. For success, there also has to be support from the top, the chief executive officer (CEO).

Ives and Gordon talking about the contribution of HR, IT and the CEO write:

“It appears that if only one of the three supports knowledge management, then nothing is likely to happen, if two of the three support knowledge management then something might get implemented, but it is unclear if it will get used or have sufficient power to have a lasting impact on the business. All three working together are necessary for real and lasting success.”

6. **Defining a strategy**

It may be the case however, that what the appropriate relative combination of HR and IT should be is itself an important issue. In some circumstances a heavier reliance on HR may be justified while in others the greater application of IT.

Hansen et al have labelled an emphasis on HR a personalised strategy where knowledge is closely tied to the person who developed it and is shared via person-to-person contact. On the otherhand, a strategy reliant on IT they refer to a codification strategy, which approach which codifies knowledge which is then stored in databases and available for access by users. Hansen and his associates believe (based on their study of companies in a number of industries) that to manage knowledge effectively strategy must predominantly be of the ‘codification’ or ‘personalised’ type. Attempts to excel at both they say are doomed to failure. They even go as far as suggesting an 80:20 split between using technology or people/organisational change as optimal.

The ‘codification’ route is appropriate they argue when the aim is to provide high-quality, reliable, reusable information and knowledge quickly. Considerable reliance may be placed upon IT which codifies, stores, disseminates and allows re-use. Where on the other hand knowledge is ‘tacit’ (i.e. ‘personal’, ‘rich’, ‘subtle’ and highly ‘contextual’) and the aim is to provide creative, analytically rigorous advice through the channelling expertise. Success lies in developing networks, which link people, and a premium is placed on changing culture and individual behaviours. The contribution of IT is limited.

7. **What are organisations doing?**

Early interest in KM was directed towards the application of information and communication technologies no doubt taking what might be called ‘the line of least resistance’. The Ernst and Young study referred to earlier found 56% of respondents reporting changing people’s behaviour as the biggest problem in KM, while only 12% said ‘overcoming technological limitations’ was problematic. Current KM projects underway in the organisations studied (the study was conducted in 1997) in terms of incidence are shown in Figure 4. It is noteworthy that the top four have an unambiguous IT flavour.
Figure 4 Areas of current application of IT for KM

<table>
<thead>
<tr>
<th>Response</th>
<th>% of respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating an intranet</td>
<td>47%</td>
</tr>
<tr>
<td>Data warehousing</td>
<td>33%</td>
</tr>
<tr>
<td>Implementing decision-support tools</td>
<td>33%</td>
</tr>
<tr>
<td>Implementing groupware to support collaboration</td>
<td>33%</td>
</tr>
<tr>
<td>Creating networks of knowledge workers</td>
<td>24%</td>
</tr>
<tr>
<td>Mapping sources of internal expertise</td>
<td>18%</td>
</tr>
<tr>
<td>Establishing new knowledge roles</td>
<td>15%</td>
</tr>
</tbody>
</table>

In the UK the expenditure on specialist software for KM is growing phenomenally with estimates of from £1.7bn in 1999 to up to £9bn in 2002. As far as the writer is aware, expenditures aimed at tackling the cultural, people and organisational impediments to KM are not known. This should not be seen as surprising as it is far easier to ‘cost’ for technology.

8. **Measuring success in knowledge management**

Although there is no reluctance among writers to advise on ‘success factors’ in KM (see discussion above) the precise measurement of its success or failure is problematic. Almost half (43%) of the Ernst and Young respondents found ‘measuring the value and performance of knowledge assets’ a difficulty and a minuscule 4% rated their own organisation’s performance as ‘good’ or ‘excellent’ in ‘measuring the value of knowledge assets/impact of knowledge management’.

As is usually the case with organisational processes, practices and changes it is extremely difficult to assess impact upon the ‘bottom line’ and resort frequently has to be made to measuring ‘inputs’ and ‘processes’.

The study by Davenport of 31 KM projects (in automobiles, banking, consulting, high-tech manufacturing and other sectors) recognising the problems of measuring the economic return on knowledge used the following ‘indicators of performance’:

- Resources committed – people, money etc.
- Growth in the value of knowledge content (e.g. number of documents) and usage (volume of accessing knowledge repositories or participation in discussions).
- Likely survival of the initiative without the support of one/two individuals.
- Financial return of the KM activity itself (e.g. if linked with a profit centre) or to the organisation as a whole (perceptual if necessary).

1.5.4 **Conclusion**

For an economy in which growth is likely to be found in knowledge-based industries, knowledge management must be important. It would appear that the early faith placed in information and communication technologies in managing knowledge has been replaced by a more balanced view that recognises the need for cultural and behavioural change. Whether an 80:20 rule of thumb between a codification and a personalised strategy is the way forward remains to be seen. We can be assured that an appropriate relationship between the two strategies will exercise minds in the years to come.
Chapter roundup

- An **information system** is an organizational and management solution, based on information technology, to any challenge posed by the environment.

- **Information** is a **valuable resource** that requires efficient management.

- Organisations **require information** for recording transactions, measuring performance, making decisions, planning and controlling.

- Strategic planning, management control and operational control may be seen as a hierarchy of planning and control decisions.

- **Strategic information** is used to **plan the objectives** of the organisation, and to **assess** whether the objectives are being met in practice.

- Tactical information is used to decide **how the resources of the business should be employed**, and to **monitor** how they are being and have been employed.

- Operational information is used to ensure that **specific operational tasks** are planned and carried out as intended.

- ‘Good’ information **aids understanding**. **ACCURATE** is a handy mnemonic for the qualities of good information.

- The **cost and value** of information are often not easy to quantify—but attempts should be made to do so.

- Information management entails.
  - Identifying current and future information needs
  - Identifying information sources
  - Collecting the information
  - Storing the information
  - Facilitating existing methods of using information and identifying new ways of using it
  - Ensuring information is communicated to those who need it
  - Ensuring information is not communicated to those who are not entitled to see it


- Knowledge Management entails
  - Managing the human factor
  - The organizational structure
  - Managing the top executive behaviour
  - The information and communication technology
  - Managing people

Practice Questions

**Q no 1)** What type of information is required by each of the management levels in an organisation?

**Q no 2)** Explain some of the main characteristics of operational information.

**Q no 3)** What types of information system are available, and which management level do they provide information for?
Q no 4) Define a Management Information System.

Q no 5) What is a knowledge work system?

Q no 6) Provide some examples of office automation systems.

Q no 7) (a) Define and distinguish between 'data' and 'information'.

(b) Information is provided for decision-making at the strategic, tactical and operational level. Define and distinguish between the nature of the decisions and the types of information provided for each level, using examples based on a typical organisation.

(c) What do you consider to be the qualities that should be possessed by good information?

Answer Hint

Answer no 7)

(a) The word 'data' means facts. Any fact - a name, a quality, a price, a time, a value etc, is an item of data. The word is plural (singular datum) and, strictly speaking, one should write 'data are...' However, the word is now commonly treated as singular. ‘Raw’ data is not usually considered in itself to be useful; it has to be organised into a meaningful form.

Information is data that has been organised into a meaningful form. Information has meaning only in relation to other information.

The three data processing stages

```
INPUT - data
↓
PROCESSING - manually or by machine
↓
OUTPUT - information
```

The difference between data and information can therefore be summarised as follows:

Data + meaning = information

(b) Management can be divided into three levels

(i) strategic (top)
(ii) tactical (middle)
(iii) operational (lowest).

The types of decisions made at each level relate to

(i) strategic - policy-making and strategic planning (eg deciding on new markets and products)
(ii) tactical - tactical planning and management control activities (eg making purchasing or stock level decisions)
(iii) operational - routine planning and control (eg action on bad debts, meeting production requirements).
Decisions can be placed under two categories for this purpose:

(i) planning decisions
(ii) control decisions.

Top level management require mainly planning information, and bottom-level mainly control information. This may be illustrated in the form of a diagram.

Examples of planning and control information are:

(i) **Planning information**

Statistical data for:
- forecasting
- corporate planning
- investment appraisal
- budget models
- market research, etc.

(ii) **Control information**

- cost variance reports
- credit control information
- working capital statements
- current sales trends
- overtime and downtime statistics, etc.

In addition, information systems produce what is often called 'passive background information', for example:

- fixed asset records, depreciation summaries
- annual production statistics
- balance sheets, etc.

At the higher level within the organisation, information is frequently required for the purpose of solving ad hoc, non-routine problems, whereas at lower levels, information requirements are often of a routine nature in order to solve recurrent, routine problems. The terms **non-programmable** and **programmable** decisions are sometimes used in relation to this aspect.

For non-programmable decision-making the format and presentation of information will be unique and highly specialised. In contrast, for programmable decision-making, information will be
provided usually in the form of a standard management report on a regular basis, perhaps daily, weekly or monthly, according to user requirements.

The presentation of management information will vary according to the level of management receiving it, as follows:

(i) top management will receive information in the form of reports, showing trends. There will be no regular timing on many of these reports

(ii) middle management will typically receive weekly or monthly statements, showing actual results in comparison with budget, or with results of previous periods, or with other relevant information

(iii) the information at operational level is used mainly to issue instructions and to correct anything which is not running according to plan. Hence, accuracy and speed are more important than presentation. Information may often be given orally to save time. Typically this information consists of comparisons between actual and budgeted results.

(c) Good information possesses certain qualities. Good information should be:

(i) complete
For example, when making a purchasing decision, ideally we would like prices from all suppliers.

(ii) relevant
Information should be screened to remove any factors that are irrelevant to making the decision.

(iii) timely
Information can only be of use if it is received in time to affect the decision-making process.

(iv) accurate
Information must be reliable enough to facilitate meaningful decisions.

(v) understandable
Information that is easy to understand is more likely to produce reasoned decision-making and action.

(vi) significant
In order to keep information simple and to the point it is advisable to screen out any facts which are not significant enough to affect the decision-making process.

(vii) adaptable
As the organisation evolves, management's needs for information are constantly changing.

(viii) cost effective
The overriding consideration as regards information is that the cost of obtaining it should not exceed its value to the firm.
STRATEGIC PLANNING OF INFORMATION SYSTEMS I

Introduction

The role of information systems has changed from that of simply recording transactions and providing accounting information to the central and crucial role they now hold within almost all organizations. In this chapter we look at the strategic role of information systems.

Study Guide

What is Strategy? (Study Text Reference 2.1)

- To introduce the topic it is important that students understand what a strategy is and the need for one. Ask students for examples from their own experience.
- Discuss the differences between strategy and strategic planning.

The Strategic Plan (Study Text Reference 2.2)

- It is important for the students to understand the focus of the Strategic Plan and the level at which it is pitched.
- More and more, today’s organisations rely on technology to support their business processes and to provide the information needed for decision-making. So what is the relationship between Strategic Planning and IT Strategic Planning? How do we go about developing the IT Strategy for a business? How do we go about planning for information systems?

The IT Strategic Plan (Study Text Reference 2.3)

- IT planning occurs at a number of levels. It is important that the students understand the different levels and the reasons why each is important.
- Students need to have an understanding of the purpose behind an IT Strategic Plan.
2. **Strategic Planning of Information Systems**

2.1 **Strategic Planning**

Strategic planning is a complex process which involves taking a view of the organisation and the future that it is likely to encounter, and then attempting to organize the structure and resources of the organisation accordingly.

**KEY TERMS**

- **Strategy** - a course of action, including the specification of resources required to achieve a specific objective.
- **Strategic planning** is the formation, evaluation and selection of strategies for the purpose of preparing a long-term plan of action to attain objectives.

We view strategy as the organised development of resources to achieve specific objectives against competition from rival organisations. It is the use of all the organisation's resources, financial, manufacturing, marketing, technological, manpower etc, in the pursuit of its objectives.

| Strategy | Deployment of resources | Desired objectives |

It is a set of policies adopted by senior management, which guides the scope and direction of the entity. It takes into account the environment in which the company operates.

'Scope' used in this context relates to size and range, and 'direction' describes product/market positioning. In simple terms, an entity's 'environment' relates to the uncontrollable factors that influence it.

There general levels of strategy can be identified: corporate, business functional/operational.

2.1.1 **Corporate strategy**

Corporate strategy is concerned with what types of business the organisation is in. It denotes the most general level of strategy in an organisation.

2.1.2 **Business strategy**

Business strategy is concerned with how an organisation approaches a particular product or market.

This can involved decisions as to whether, in principle, a company should:

(a) Segment the market and specialize in particularly profitable areas.
(b) Compete by offering a wider range of products.
Some large, diversified firms have separate strategic business units dealing with particular areas.

### 2.1.3 Functional/operational strategic; information systems strategy

Information systems strategy is an example of a functional/operational strategy (although in some cases it may have strategic implications). Functional/operational strategies deal with specialized areas of activity.

<table>
<thead>
<tr>
<th>Functional area</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information systems</td>
<td>A firm’s information systems are becoming increasingly important, as an item of expenditure, as administrative support and as a tool for competitive strength.</td>
</tr>
<tr>
<td>Marketing</td>
<td>Devising product and services, pricing, promoting and distributing them, it order to satisfy customer needs at a profit.</td>
</tr>
<tr>
<td>Production</td>
<td>Factory location, manufacturing techniques, outsourcing etc.</td>
</tr>
<tr>
<td>Finance</td>
<td>Ensuring that the firm has enough financial resources to fund its other strategies.</td>
</tr>
<tr>
<td>Human resources</td>
<td>Secure personnel of the right skills in the right quantity at the right time.</td>
</tr>
<tr>
<td>R&amp;D</td>
<td>New products and techniques.</td>
</tr>
</tbody>
</table>

### 2.2 Formulating strategies: The rational model

Strategic planning divides into a number of different stages: strategic analysis, strategic choice and implementation.

#### 2.2.1 Strategic analysis

Involves the steps in the following table (relevant models referred to are covered throughout this Text).

<table>
<thead>
<tr>
<th>Stage</th>
<th>Comment</th>
<th>Key tools, models, techniques</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1. Mission and/or vision</td>
<td>Mission denotes values, the Business, rationale for Existing; vision refers to where the organisation intends to be in a few years time</td>
<td>• Mission statement</td>
</tr>
<tr>
<td>Step 2. Goals</td>
<td>Interpret the mission to Different stakeholders</td>
<td>• Stakeholder analysis</td>
</tr>
<tr>
<td>Step 3. Objectives</td>
<td>Quantified embodiments of Mission</td>
<td>• Measures such as profitability, time scale, deadlines</td>
</tr>
<tr>
<td>Step 4. Environmental Analysis</td>
<td>Identify opportunities and threats</td>
<td>• PEST analysis</td>
</tr>
<tr>
<td>Step 5. Position audit or situation analysis</td>
<td>Identify strengths and Weaknesses Firm’s current resources, Products, customers, systems, structure, results, Efficiency, effectiveness</td>
<td>• Resources audit</td>
</tr>
<tr>
<td>Step 6. Corporate appraisal</td>
<td>Combines Steps 4 and 5</td>
<td>• Distinctive competence</td>
</tr>
<tr>
<td>Step 7. Gap analysis</td>
<td>Compares outcome of Step 6 with Step3</td>
<td>• Value chain</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Product life cycle</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Boston (BCG) matrix</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Marketing audit</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SWOT analysis charts</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Gap analysis</td>
</tr>
</tbody>
</table>
2.2.2 **Strategic choice**

<table>
<thead>
<tr>
<th>Strategic options generation</th>
<th>Comment</th>
<th>Key tools, models, techniques</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategic options generation</td>
<td>Come up with new ideas:</td>
<td>• Value chain analysis</td>
</tr>
<tr>
<td></td>
<td>• How to compete (competitive advantage)</td>
<td>• Scenario building</td>
</tr>
<tr>
<td></td>
<td>• Where to compete</td>
<td>• Porter’s generic strategic choices</td>
</tr>
<tr>
<td></td>
<td>• Method of growth</td>
<td>• Ansoff’s growth vector</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Strategic options evaluation</th>
<th>Normally, each strategy has to be evaluated on the basis of</th>
<th>• Stakeholder analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Acceptability</td>
<td>• Risk analysis</td>
</tr>
<tr>
<td></td>
<td>• Suitability</td>
<td>• Decision-making tools such as decision trees, matrices, ranking and scoring methods</td>
</tr>
<tr>
<td></td>
<td>• Feasibility</td>
<td>• Environmental fit</td>
</tr>
<tr>
<td></td>
<td>• Environmental fit</td>
<td>• Financial measures (eg ROCE, DCF)</td>
</tr>
</tbody>
</table>

**Strategy selection** involve choosing between the alternative strategies

(i) The competitive strategies are the generic strategies for competitive advantage an organisation will pursue. They determine **how** you compete.

(ii) Product-market strategies (which markets you should enter or leave) determine **where** you compete and the direction of growth.

(iii) Institutional strategies (ie relationships with other organizations) determine the method of **growth**.

2.2.3 **Strategy implementation**

**Strategy implementation** is the conversion of the strategy into detailed plans or objectives for operating units. This involves:

- Resource planning (i.e. finance, personnel) involves assessing the key tasks
- Operations planning
- Organisation structure and control systems

2.3 **Why have an IS/IT strategy?**

2.3.1 **Importance of information systems**

The crucial role of information systems within an organisation can be studied from the point-of-view of the support that information systems provide to all sections of that organisation. That support will be internal and external to the organisation, and will probably assist the organisation in obtaining some benefit from working with suppliers or customers. A strategy for information systems and information technology is justified on the grounds that IS/IT.

- Involves high costs
- Is critical to the success of many organizations
- Is now used as part of the commercial strategy in the battle for competitive advantage
- Impacts on customer service
- Affects all levels of management
• Affects the way management information is created and presented
• Requires effective management to obtain the maximum benefit
• Involves many stakeholders inside and outside the organisation

The following three examples start to show how IT can benefit an organisation.

(i) A major distributor offers its customers the opportunity to enter their orders directly by using an online network. The main advantage of the system is to reduce order entry costs, while at the same time allowing customers to be flexible in the time and processing of order submission. Further advantages arise from adding value for customers and increasing sales.

(ii) Similar to the Ford Motor Company, a major aerospace company has requested all its key suppliers to implement CAD to its own CAD installation. This significantly reduces the time and cost of carrying out design changes, parts acquisition and inventory. Such a change would again lead to competitive advantage.

(iii) A national carrier can substantially reduce the competitive position of a regional airline. The national carrier, through access to the reservation levels on every one of the smaller airline's flights, can pinpoint all mutually competitive routes where the regional is doing well and take competitive pricing and service action. The fact that the regional airline is unable to gain access to the data held by the national carrier puts it at a competitive disadvantage.

One writer on information systems, McFarlan, urges companies to address five key questions regarding the impact of technology. He argues that, if the answer to one or more of the questions is yes, the information technology represents a strategic resource that requires attention at the highest level. The questions are:

• Can information technology build barriers to entry?
• Can information technology build on switching costs?
• Can information technology change the basis of competition?
• Can information technology change the balance of power in supplier relationships?
• Can information technology generate new products?

Porter has identified that barriers to entry allow the organisation to hook their customers into using products and services. In the example cited above with the distributor, the company successfully opened up a new electronic channel to its customers, which was unrivalled by its competitors.

Question 2

Nassar and Hassan Ltd is a company with an establishing base of IT applications. The finance department has a fully computerized accounting system. The marketing department has development a primitive customer modeling package. The production department does not need IT.’

Mursaleen, The Finance Director is in charge of IT at Nassar and Hassan Ltd. He proposes in the annual corporate budget a 10% increase in IT expenditure based on last year, for the relevant departments. This will enable system upgrades.

Comment briefly on the information strategy at Nassar and Hassan.

Answer

There is no strategy at all. The Finance Director regards IT as a cost. Moreover the IT ‘strategy’ is directed to enhancing its existing base (e.g. in the accounts department) rather than areas where it might prove competitively valuable (e.g. in marketing).
2.3.2 Strategic potential for IT

Using IT strategically has enhanced the competitive position of many organisations in a variety of sectors. For example, the financial services sector has witnessed vast changes brought about by new technologies such as the client server architecture, multi-tasking and 4GLs. The strategic potential for information technology can be used in a number of areas, such as:

- New business, where information technologies make whole new operations possible. For example, point of sale equipment, which includes effective stock and re-ordering facilities.
- Market research information can also be obtained from point of sale equipment.
- Sales; by giving salespeople portable computers they can check stock levels, enter orders directly and receive messages quickly. This can reduce paperwork and speed up delivery.
- Financial management can be improved if a link is set up between the bank and the organisation. This can allow financial information to be obtained more quickly.
- Product development such as in-house electronic publishing can help turn out product manuals faster for speedier introductions.
- Training, or re-training, employees using videodisks allows them to learn at their own speed and cuts training costs.
- Locking in customers by creating exclusive computer communications with customers for order entry and exchange of product and service data. This service can increase the competitive advantage.
- Selling processing power by using off-peak time to develop completely new services for outsiders.

2.4 The Information Systems Strategy

KEY TERMS

The Information Systems (IS) strategy refers to the long-term plan concerned with exploiting IS and IT either to support business strategies or create new strategic options.

Strategic information systems are systems at any level of an organisation that change goals, processes, products, services or environmental relationship with the aim of gaining competitive advantage.

Strategic-level systems are systems used by senior managers for long-term decision making.

2.4.1 Purpose of an information systems strategy

For an organisation to invest in information technology and information systems it will require some sort of information systems strategy. The IS/IT strategy should be based upon the corporate strategy, which can be defined by a study of the mission statement.

The mission statement is a statement of purpose by the organisation, and from this the aims and objectives can be ascertained. The aims and objectives state what needs to be achieved and the corporate strategy
outlines how to achieve them. Therefore, care must be taken when drawing up the IS/IT strategy to ensure it is aligned with the corporate strategy.

The purposes of an IS include:

- support for the overall corporate strategy by providing relevant information on customers, products and production etc., to decision-makers in the organisation.
- provision of the information that customers need to make a purchase from the organisation eg, from mail shots, Internet sites etc.
- provision of relevant information to user departments eg, specific operational level information such as stock.

An information strategy will comprise two parts:

(i) **Organisational** - this is the systems management which is concerned with the collecting, processing and distribution of information.
(ii) **Technical** - this specifies the means by which the information will be collected, processed and distributed.

Strategic planning for IT ensures:

- compatibility - between the various systems under development and hardware purchased within an organisation.
- commitment - from the strategic level of management.
- resource allocation - the monetary commitment from the organisation.

### 2.4.2 Contents of IS strategy

Ward, in his model of a planning process, proposes that the IS strategy plan should contain three elements:

(i) **Business information strategy** - indicates how the information will support the business. Where the organisation has priorities for system developments, these are defined at a general level, perhaps by suggesting a portfolio of current and required systems.

(ii) **IS functionality strategy** - indicates what features and performance the organisation requires from the systems. It demonstrates how the resources will be used, provides policy guidelines for the management of the information resource and policies for communication networks, hardware architectures, software infrastructures and management issues such as security, development approaches, organisation and the allocation of responsibility.

(iii) **IS/IT strategy** - defines the policies for hardware and software eg, position on preferred suppliers. It also defines the organisation's stand on whether it is to be centralised or distributed, the IS accounting techniques and what are to be the investment, vendor and human impact policies.
2.5 Developing a Strategy for Information Systems and Information Technology

There are a number of methodologies for strategic planning, to help ensure that information systems support the overall business strategy. We will look at following in models in detail:

1. The Information Engineering
2. Parson Generic IS strategies
3. Generic framework for developing IS/IT strategy
4. Earl three leg approach
5. Strategic considerations for developing IS/IT strategy (Discussed in the next chapter)

2.5.1 The Information Engineering

Key Term

The Information Engineering (IE) methodology is defined as a set of inter-related formal techniques in which business models, data models and process models are built up in a comprehensive knowledge base and are used to plan, create and maintain information systems.

Branded products based on IE include:

- Navigator System Series (NSS), developed by Ernst Young;
- Information Engineering Methodology (IEM), developed by James Martin Associates;
- Business System Planning (BSP), from IBM; and
- Strategic planning, from the London Business Management School.

The six stages of an Information Systems Project (ISP), based on an IE methodology, will normally include the following:
1. **Initiating the ISP project**

This stage includes understanding the scope of the project, the approach to be adopted and how it is going to be organised, resourced and managed. At this stage it is important to identify and document the scope, goals and objectives of the project.

In determining the scope, the project manager should ascertain whether there are any previous or current planning activities, as the relationship with other ISP projects is important. It would be unwise to duplicate effort or produce conflicting plans. The sequence in which ISP projects are carried out may also impact on the strategic advantage gained. For example, spending money on a SISP for a business that fell into the “dog” category in the BCG matrix would not be sensible when the continuing profitability of the organisation would presumably depend on those business units in the “star” or “problem child” categories.

2. **Clarifying the business strategy**

The purpose of this stage is to develop an IS strategy which is aligned to the business strategy, in a way that can give the greatest benefit. Developing a picture of the organisation using a SWOT analysis can give valuable insight into the business. The ranges of models that can contribute to this process include Porter's five forces, the generic strategies and the value chain and value system.

The preferred approach in IE methodologies is to express the business strategy by identifying the goals of the business and the business objectives set to meet

3. **Modelling the business**

Models provide a means for the project team to develop, confirm and present their understanding of the business in a form that is verifiable by the business users and the business management. The four areas that can be modelled successfully are the strategy, functions and processes, data and organisation.

(i) The strategy of a business can be modelled with goals and their dependent objectives.

(ii) Functions and processes can be modelled by drawing a functional decomposition chart. This show the functions that support the business e.g. finance, personnel and marketing, and then breaks down the main business activities (or processes) which form part of those functions.
The data can be modelled using a variety of modelling techniques, such as dataflow diagrams, entity relationship models and entity life histories.

The structure and hierarchy of the organisation can be modelled in an organisation chart.

4. **Reviewing current information systems**

It is probable that the organisation will have some IT facilities already in place and these must be recognised as a major building block for the future information systems. The IS review must take into account the views both of the people in IT areas who keep the IS application running and maintained, and also the business users who have to operate the applications.

During the review, it is important to distinguish between investment in the application and investment in the means of delivery, so that the review covers the current and planned information systems and also the technology, the management organisation and the control of information systems.

One of the activities in the current IS review is documenting resources. These resources can be divided into the following categories:

- **Information technology**: a complete inventory of the IT resource should include the technical details, the costs of maintenance, upgrades and financial commitment.

- **The IS infrastructure** review document should cover the personnel, their function and skills, the space they occupy and the facilities they use. The costs, financial commitment, revenues and expenditure, where appropriate, form a part of the review. The models that can help with this review are: Nolan's six stages of growth; McFarlan's phases of technology assimilation, with his strategic grid; and Primozic's waves of innovation.

- **The IS applications and data collections** review document identifies all of the major applications as well as any enhancements to them. The data collections are the physical groupings of data maintained by the organisation eg, computer-based files and databases.

5. **Building the information systems' architecture**

Before the strategy can be prepared, it is necessary to describe the 'vision'. This is generally called the architecture and is a framework which drives, shapes and controls the IS requirements. This encompasses, the applications, the data collections necessary, and a description of the technology, with the management and organisation required to deliver and to support them. It not only defines the vision for the future but it must identify the costs and risks associated with that vision.

The architecture must cover the new opportunities yielded by the IT, which may offer competitive advantage or create new strategic options. These opportunities may be enhanced by the use of an existing IS or a completely new IS which supports an entirely different approach to some business problem or strategy. There are four interdependent components to the architecture, as shown in the diagram below:
Each of the architectures will comprise the same components - parameters, principles, schema and plan.

- The **parameters** are concerned with the essential needs, constraints and preferences that each element should attempt to satisfy. They are assumptions, which are made so that alternative architectures may be evaluated.

- The **principles** are the policies that guide decision-making during the development of the architecture. They are concrete, practical statements of how each technological element is to be delivered.

- The **schema** describes the architecture, its requirements and how it will work. Schemas are sometimes called models or blueprints; they may be the visual, logical state of the frame as it exists now or an agreed detailed model of what is being pursued.

- The **plan** - may include project plans or performance goals plus time-phased actions that will move the framework to the next state of evolution.

**Computing architecture** - refers to the information processing hardware and its associated operating systems software. This architecture describes the platform and facilities needed to realise the IS vision of the organisation. It will include:

- the type of processing architecture e.g., mainframe, PC, client server etc;
- the processor configuration: hardware, software, development tools etc;
- the communications network: LAN and WAN;
- the facilities needed to support both the hardware and the staff.

The type of hardware, its capacity and location are influenced by the application needs and the requirement to share data. The IS management and organisation will be influenced by the location of the hardware and the type of data communications required, and vice versa.

**Communications architecture** - will describe the infrastructure required for the application, data and technology architectures. It includes an identification of: telecommunications networks and their associated devices for inter-linking. The topology of a communications network is influenced by applications needs, data transmission requirements and information processing geography, as well as by its own capabilities.

**Data architecture** - relates to the data assets of the organisation and the requirements of use, control and storage. The schema for the data architecture should include descriptions of the data collections required to support the application architecture. The costs and benefits, return on investment and payback period of the proposed architecture should be analysed and estimated.

**Applications architecture** - covers the main application systems of the organisation, their functions and relationships, as well as the development methods. The activities associated with drawing up the
schema for the application architecture will include identifying the information systems and their applications, and also describing, classifying and assigning priorities to each application. For example, cash management, accounts receivable and general ledger applications may form part of the financial information management system.

6. Developing the strategic information systems plan (SISP)

This plan is inevitably a set of compromises between development and maintenance, risks and returns, infrastructure and applications and long term and short-term benefits. There are three sections to the plan: architecture migration strategy; schedule; and maintenance and evolution of the SISP.

- **Architecture migration strategy** - this describes how the move from the current IS position to the vision that is defined in the architectures should be implemented. It shows the phases for implementation, along with an assessment of time, organisational impact, risks, resources, costs and benefits. It also defines the dependency between phases.

- **Schedule** - each architecture migration phase is reviewed and divided into manageable projects. The projects are then reviewed alongside the application portfolio and the priorities and dependencies are determined.

- **Maintenance and evolution of the SISP** - the SISP will need to be monitored and updated like all plans. Similarly the architectures will also need to be revised as the migration moves forward. The roles and responsibilities for the maintenance of both the plan and the architectures will need to be decided and the procedures to accomplish this maintenance should also be considered. Major reviews of the plan should be defined and the policies concerning them established.

2.5.2 Parson Generic IS Strategies

Finally in this section, another theorist, Gregory Parsons, has identified six possible IS strategies. As with business strategies, the IS strategies can also be deliberate or emergent and therefore can be used to name a chosen strategy or to conveniently classify a set of observed activities. The IS strategies are:

- Centrally planned
- Leading edge
- Free market
- Monopoly
- Scarce resource
- Necessary evil.

Each of these six strategies is outlined below.

1. Centrally planned

Centrally planned does not mean centrally controlled. The logic of this approach is of understanding and coordinating the strategic direction, because management believe that this strategy facilitates uncovering the whole picture and that this larger, overall view makes for better decisions. Hence, it is unlikely that this strategy will be an emergent one. For an organisation to adopt a centrally planned IS strategy, it requires a significant degree of involvement and knowledge on the part of management. It is not possible to follow this strategy unless its strategic significance is well understood and fully acknowledged. This means that the planning cycles of business and IS are closely integrated, indeed IS strategy planning should be embedded within the business strategy planning.
The management treatment of IS places its primary emphasis on the planning processes, using them as the path towards business value from IS. The resultant role of IS becomes one of a service provider, closely linked to the user community to deliver the business demands. The user role appropriate to this strategy complements this by spotting opportunities and identifying the appropriate demand to make on the IS function to make sure that its potential is fully explored throughout the organisation.

2. **Leading edge**

This strategy is implemented because of a belief that innovative technology use can create business gains and therefore the highly risky investment can generate a huge payback. To take these risks the organisation must have the motivation and ability to commit large amounts of money and other resources. The organisation must also have very innovative management, who can draw upon strong, varied and flexible technical skills.

The role of the IS function with this strategy is one of experimenter and promoter so that the boundaries of technical capabilities can be pushed forward throughout the organisation. The user role is an enthusiastic user of new technology, which incorporates technology environmental scanning with a willingness to support major in-house development initiatives.

3. **Free market**

This is a strategy where the organisation's managers believe that the market makes the best decisions and, since the users are responsible for business results, they are the most equipped to make the best decisions. This strategy requires users who are knowledgeable and able to assess the relative merit of wide-ranging options. The organisation must be willing to accept a degree of duplication of effort in return for devolved responsibility.

The role of the IS function is of competitive business unit, perhaps a profit centre, which must be prepared to achieve a return on its resources and use its understanding of the organisation as a leverage against outside competition. It must be financially accountable in order to compete and the organisation cannot exert tight financial controls over the total IS budgets. The user role will be complementary and one of service negotiation. The users must identify and acquire IS services and manage the choice, acquisition and contract process.

4. **Monopoly**

This is the opposite of a free market strategy and is adopted because of a belief that information is an organisational asset, produced across functional boundaries. Because of this it can only be cross-functionally available if it is controlled by a single service source. For such a policy to work, there must be user acceptance, backed up by policing policies to force it through. While maintaining user acceptance, the single source provision should be based on good forecasting of service demands and a strong focus on customer satisfaction.

The IS role is a reactive one of satisfying articulated requirements as soon as they arise, rather than directing future developments. The user role is one of expressing the needs and negotiating for their provision from the single source. Much of this negotiation will be one of bidding for a share of resources rather than for a service contract.

5. **Scarcere source**

This strategy probably emerges, rather than is adopted, because of a belief that information is finite and hence a limited resource, whose development requires a clear justification. For this justification to exist
there must be tight budgetary controls regarding all aspects of IS expenses and there must be policies which
ensure that both the IS function and the users stick to the budgetary controls.

The resultant role for the IS function will be to make the best of their limited resource with cost saving
measures and by effective cost control of projects. The role of users will be to bid for information resources
by project justification in terms of bottom-line cost/benefit presentations. This will have a negative effect on
information exploitation and will tend to generate a passive user community.

6. Necessary evil

This is a strategy with a very tightly controlled, grudging allocation of IT - enough to meet basic needs. It is
adopted in organisations that believe that information is not important in their business.

The IT role provides a minimum level of resource and skills and encompasses only the projects that have
been identified as having a good return on investment. The user role is very passive because they take no
part in the development or management of the information system.

2.5.3 Generic framework for developing an IS strategy

Planning an Information Systems strategy is a decision-making process. Such a crucial process should be
undertaken carefully, systematically and with a firm understanding of the business context.

This section describes and discusses a general framework that may be adopted when developing an
Information Systems strategy. This proposed framework focuses on a five-stage model. Examples are
provided detailing possible tools and techniques that can be adopted at each stage. It spans the past, present,
and future and incorporates both a planning and a review stage. Each stage poses a single question:

1. ‘W3?’ represents “Where We Were?” – the past
2. ‘W2R?’ is “Where We Are?” – the present
3. ‘W32B?’ is “Where We Want To Be?” – the future
4. ‘(GT)2?’ is “Going To Get There?” – the plan
5. ‘W4?’ is “Where We Went Wrong?” – the review.

This approach to developing an Information Systems strategy systematically focuses the mind on the five
key stages in turn. First, what has been learnt from experience in terms of successes and failures? Second is
a critical analysis of the current situation. Third is the identification of future information system objectives
(allied with business objectives). The next stage plans progression towards these objectives by exploiting
relevant experiences, strengths and opportunities whilst overcoming weaknesses and threats. The third and
fourth stages are iterative both within and between each other. Finally the whole process is reviewed, which
completes the cycle and provides an important part of the input into the first stage of the next cycle.

1. ‘W3?’ Where We Were?

Much is written about the experiences of both successful and failed IT projects that document “where we
were” for the benefit of future project teams. The risks of failure are high and the causes may be Political,
Economic, Social or Technological (PEST). Before embarking on a project it is recommended that a full
PEST analysis is conducted. The key issues that must be addressed when planning an IT strategy are:

- Commitment
  This must be spread from the very top down and across all management and user populations
affected by the project. Each must put sufficient resources and time into the project to give it a
chance to succeed, otherwise it will fail.
• **Coordination**
  IT projects must be planned and controlled in detail to ensure that “the right people are doing the right things at the right time in the right sequence”. Otherwise unforeseen details can subsequently determine success or failure. One survey suggests poor co-ordination is the most common cause of failure, contributing to 74% of all failed cases researched.

• **Communication**
  “The right people must communicate the right things at the right time and in the right media” to successfully implement an IT project. This is especially true when analysing and specifying user requirements. The cost escalation of correcting poor specifications when the system is operational has been estimated as between ten-fold and one hundred-fold.

If any of these three conditions is lacking, then the IT project will probably fail. At best, its costs and timescales will escalate dramatically.

Unfortunately, senior management does not always understand these lessons. Education and training are key to improving their understanding of the issues involved and their role in exploiting IT successfully. Every organisation planning an IT strategy should commence with workshops to help ensure that the lessons of the past are learnt by all concerned and that the same mistakes will not be made in its own IT projects.

2. ‘**W2R?** Where We Are?’

Workshops or discussions should also pave the way for a critical analysis of “where we are” with respect to the existing information systems, in terms of both “good and bad” news. This helps to ensure that the former will be retained and the latter will be corrected when designing a new or improved system. Strengths, Weaknesses, Opportunities and Threats (SWOT) analysis can be a useful technique to help ensure that criticism is structured in a systematic and comprehensive manner. A suggested framework is shown in Figure 1, as a 4 x 4 matrix. The matrix focuses on one set of issues at a time. The four columns are headed Strengths, Weaknesses, Opportunities and Threats. The first two are internal to the domain of the information system and the latter are external to it. The four rows represent the main resources that are exploited by IT projects. These can be further classified into components to assist in the critical analysis of the existing systems. SWOT analysis yields a framework for conducting, communicating and agreeing a balanced criticism of the present situation and identifies both short-term and long-term weaknesses that need to be resolved.

The SWOT matrix can be adapted to meet the particular requirements of organisations and their IT projects. Usually, a first step is to construct the model with senior management and to identify the ‘go / no go’ areas. When planning an IT strategy, it is vital to understand the present situation, because this will affect the tactical plans to achieve the strategy. To plan a route from A to B, it is helpful that we know where A is.

![Figure 1: The 4x4 SWOT Matrix](image)

3. ‘**W32B?** Where We Want To Be?’
Planning an IT strategy requires that a business strategy has already been planned or is simultaneously being planned. The business objectives and constraints may drive the IT goals or alternatively IT developments may enable the business strategy, i.e. the Internet and its accompanying technologies may enable a strategy of globalisation. A target marketing strategy of focusing competitive products and services against customer segments may generate the IT applications portfolio. The business budgets and priorities, based on competitive threats or return on investment (ROI), may dictate budgets and priorities for the IT strategy. An IT strategy cannot be planned in isolation from a business strategy – the two are inextricably intertwined.

In order that the company can benefit from technological innovations that serve the business process, an element of balance must be achieved. This requires an infrastructure whereby the hardware and systems architecture is considered along with the business applications and the business objectives as the overall business process.

**IT involves many stakeholders.** As IT becomes strategic, firms need to recognise the multiplicity of stakeholders involved and organise themselves to manage stakeholder relationships and to influence their IT environment. By ensuring that the focus of development is balanced, systems and technology can be implemented in a way that provides benefits to all of the stakeholders, internal and external to the organisation.

A key issue in setting IT goals is to establish an appropriate **balance between cost, quality and lead times.** However, many companies are preoccupied with lead times and believe speed is the essence, “stuff IT in quick and sort IT out later.” Too many senior managers are preoccupied by the short-term of this year’s performance and competitive pressures; to them, software quality, or even cost is not the main concern. However, in most cases, the trade off between cost, quality and lead times can be achieved. It is important to examine in detail the costs and timings of all aspects of an IT project. The answer often lies in getting the IT detail right. For example, costs and times can often be measured in pounds or months (albeit after the event), but the quality of information systems cannot generally be quantified. This is because “quality” is multi-dimensional and embraces such intangible and conflicting objectives as reliability, flexibility, robustness, security, portability, accuracy, compatibility, maintainability, efficiency, and so on. Each system may have its own set of quality parameters or a different hierarchy of measurement.

In addition to the requirement to balance IT objectives, there is the need to **drive the business objectives** through to detailed IT objectives. Target information systems also need to be designed that will support the strategic business plan. It is important to recognise that this target is a moving one, as detailed below.

A strategic plan may require a long time to implement, perhaps two or three years. Thereafter, possibly a number of years of operation are possibly needed to reap the benefits of the initial investment – the planning horizon may be several years or so. During this time, the **business requirement may well change.** If not, the technology will certainly change, and tomorrow’s technology will definitely be physically different from today’s. How then, can we possibly design tomorrow’s information systems today?

The answer is that we cannot design future physical systems because we do not know the costs, capacities, speeds, reliability, facilities, and so on of emerging technologies. A nanosecond is a lifetime in IT. However, what we can do is **identify logical requirements, continually track the emerging technologies** and **exploit new products** to achieve the IT objectives as and when they become available and proven.

Thus, identifying “Where We Want To Be” requires that a business strategy and an IT strategy are developed in unison. Thereafter, emerging technologies will need to be exploited in order to physically achieve the business goals within the planning horizon of the long-term IT strategy.
4. ‘(GT)²? Going To Get There?’

The tactics of ‘Going To Get There’ which are adopted to implement an IT strategy should take into account:

- the high risks of failure and the causes of past disasters (W3)
- present and short-term problems, plus the time-scales within which they must be resolved (W2R)
- the moving target nature of the long-term objectives and information systems design, particularly in light of emerging technologies (W32B) and
- the priorities imposed by the business plan in terms of achieving the IT benefits (competitive defence / attack, return on investment (ROI) etc).

Bearing in mind that the planning horizon may be measured in years, the crucial, tactical choice is between a single, total implementation of the overall IT strategy, or a phased one. Most but not all organisations opt for the latter because:

- they will not (or cannot) wait years for the IT benefits
- longer projects are more difficult to manage, particularly because they are more vulnerable to changing requirements
- management of innovation recognises that a ‘big deal’ is more difficult to sell than many ‘small deals’
- some pressing short-term problems dictate that short-term solutions are vital (or there may be no long term).

Implementation tactics should be designed to achieve the appropriate phasing, as illustrated in Figure 2, “the staircase approach”.

**Figure 2: Climbing the (GT)² Staircase**

Each step in the staircase represents a delivered application of IT resources (hardware, software, database, telecommunications etc). Their ascending sequence often commences with emergency fixes to short-term problems, then to build any necessary infrastructures to support the introduction of information systems, in
sequence of decreasing benefits, until they comprise a total, integrated system. Of course some steps may be climbed simultaneously and there may even be several staircases to ascend, but a phased approach helps to focus on “the right applications being implemented at the right time and in the right sequence”.

The systems lifecycle is usually adopted for each step (i.e. an application or project). Planning an IT strategy further requires that the total system be partitioned into steps and the staircase be designed with due regard to the continuing availability of IT resources. Thus, the staircase is initially designed to support the business plan and may then be adjusted to satisfy information systems and IT constraints. Further adjustments will also be made during its ascent due to business and IT dynamics as previously mentioned.

5. ‘W4?’ Where We Went Wrong?

Until we accept that the development of the information resource is an on-going, purposeful and systemic activity – we will remain the worst sort of fools – experienced and ignorant. Success and failure are emergent rather than engineered. The primary focus of the management of information systems should be to learn from and improve our products and practices.

During the last decade we have seen a blurring of industry boundaries, where banks sell stocks, shares, insurance and mortgages, and credit cards are issued by trade unions and car manufacturers. Wholesale deregulation has occurred in banking, air-transport, communications and the Stock Exchange.

The pace of business has increased, with a global 24 hours a day seven days a week electronic marketplace providing instant access to information. We now inhabit a global business community, dominated by international companies trading in a global (electronic) marketplace. The ‘First World’ is an information society with most of its workforce employed as knowledge workers, thus increasing the complexity of management in a business environment that is characterised by complexity, simultaneity, asynchronicity and decentralisation.

Computers, once seen as constraining and controlling, are now end-user tools seen as liberating and empowering. There is general recognition of information as a key resource or the ‘oil of the 21st century’. Information is a key determinant of the wealth of nations as world markets depend on it. Information is considered to add value to, and differentiate products and services. New working practices such as desk sharing, home working, individual learning, job sharing, contracting, and the use of satellite offices are changing the nature of work.

The world of the software systems developer is changing at breakneck speed. Each new generation of Information Technology supports a new and improved generation of Information Systems. Information management is broader and more complex and less certain a discipline now that it has ever been.

The term ‘software crisis’ was coined during the NATO software engineering conference of 1968 to indicate that software projects often ran late, cost far more than expected and frequently did not meet the needs of the client. Some seven years later, Fred Brooks reminded us that the only unforgivable failure is the failure to learn from our previous mistakes, and yet the software crisis persists. Software is still difficult to develop and often fails to meet user expectations.

A key lesson to be learned from the engineering paradigm is that failure is the key to success. Transferring the approach of learning from your mistakes from say bridge building, where the cycles of failure and success take many years, to systems strategy and software development where changes happen almost monthly, is difficult. As a general principle, however, it is sound.
Systems professionals and their clients have been making the same mistakes for decades, when as Brooks reminds us “only an idiot makes the same mistake twice”. At the very least, organisations should document and objectively analyse their major information systems failures so that they and others may learn the key to success.

6. **Strategic Tools and Techniques**

A series of action research projects, conducted by the authors, spanning over a decade, has seen the emergence of an approach to embedding a number of strategic tools and techniques in a simple cyclical framework. These projects have involved strategic, tactical and operational systems in education, health care, construction, banking and other areas of the private sector. The authors have attempted to define a general purpose framework of open utility.

The research has involved the adaptation and use of a recognised framework for the development of IS strategy. This strategic framework supports the use of a wide range of established strategic tools, which may be used in one or more stages of the framework as appropriate.

The use of Failures Theory, SWOT analysis and PEST analysis has been described here by way of example, but many other tools, techniques and methods may also be usefully employed. Many of the well-established models and methods were originally developed to describe or to model organisations as a whole. In the current business environment, where organisations often have multi-generation system platforms and applications, they may be more appropriately employed at the application or project level. Examples of appropriate tools, techniques and methods include (for detailed explanation of each tool see the next section):

- Nolan’s ‘Stage Hypothesis’
- Checkland’s ‘Soft Systems Methodology’
- Earl’s ‘System’s Audit Grid’ and his ‘Three Leg’ analysis
- McFarlan’s ‘Applications Portfolio’ and Peppard’s adaption of it
- Parson’s ‘Six Information System Strategies’
- Zuboff’s ‘Automate, Informate, Transformate’ model
- Porter’s ‘Five Competitive Forces’ theory
- The ‘Three Stage’ change process (‘Unfreeze, Change, Re-freeze’)
- McFarlan’s ‘Information Systems Strategic Grid’.

7. **Conclusion**

These and other tools, techniques and methods may be used within the framework given, to focus the mind on five key questions in turn. First, what is the historical background to the change process and what, in broad terms, has been learnt from experience in terms of successes and failures? Second, what aspects of the current situation are likely to be relevant to the strategic decision making process? Third, what are the objectives of the change process? Fourth, how can experiences, strengths and opportunities be exploited and weaknesses and threats overcome, in order to progress towards the stated objectives? Fifth, what have we learned from all of our efforts?
2.5.4 **Earl three leg approach for IS Strategy development**

Earl explained that organisations tend to produce an overall business plan in one of three different ways:

- Infrastructure led – bottom up emphasis
- Business led – top down emphasis
- Mixed – where the emphasis is inside out.

1. **Infrastructure led - bottom up planning process**

   In this planning process, the organisation is focus on ensuring that the transaction systems are in place to provide the basic operational information for the organisation. For organisations that adopt this process, information systems are the means of delivering the goods and services of the sector e.g., banks and financial services. Computer-based transaction systems underpin the business operations and the organisation depends upon IS. If a system failed it would stop operations; inefficiency would drive their costs up and inflexibility would stop product/service development.

   Because the organisation must often make choices in ignorance of future business needs, it makes this class one of inherently high risk and uncertainty.

   The bottom-up approach is suitable for any organisation that feels the impact of IS in this way. They will need to understand their current position and be able to evaluate it in a meaningful way i.e., appraise the skills, attitudes, user awareness, technical ability etc.

2. **Business led - top down planning process**

   Top down planning implies that the overall objectives of an organisation are identified first, and then the underlying IS / IT systems are put in place to ensure that these objectives are met. The business strategies of organisations that adopt this process increasingly depend on IS for their implementation. The business and functional strategies require a major information, communications and automation capability and are only made possible by these technologies. A classic example is the car industry where business plans for survival and regeneration define the investments in IT and IS for manufacturing, marketing and distribution.

   A top-down analytical approach relies on the ability to apply models such as portfolio analysis (see chapter 10) and information analysis by decomposing the organisation and its objectives to the level of business process and resultant information needs.

3. **Eclectic (mixed) planning process**

   Eclectic planning is literally a mixture of top-down and bottom-up planning. This planning method recognises that IS has the potential to provide new strategic opportunities for this class of organisation. The specific applications of technology are exploitable to develop the business and change the processes of managing it. The planning process should be inside out and opportunity led.

   Analysing needs and building upon capabilities are not the best ways to identify or pursue innovations. The formal, structured approach is not suitable. Technological innovation can come about from entrepreneurial managers outside the formal planning process. Inside out planning is a creative approach that relies on ideas for business opportunities to be generated that can be pursued by using IS. This is similar to business re-engineering.

   Inside out planning needs a creative, innovate environment that allows offbeat approaches that by-pass normal rules.
Earl, suggests a method for the development of IS strategies that has three parts, as shown in the following diagram. These are:

- **top-down** - to translate business objectives
- **bottom-up** - to develop incrementally from the current position
- **inside out** - less structured to support innovation.

This model does not prescribe in detail what techniques to use; rather it identifies a framework for that selection.

![IS/IT strategy planning diagram](image)

Since the three IS strategy planning approaches are not mutually exclusive, they may all be employed at the same time, maybe with one more dominant. It is a three dimensional model where the background and foreground can alter as the emphasis shifts. They are all simultaneously required if IS plans are to capture the true business situation, although each will enjoy stages of lesser or greater emphasis. The mixed approach allows the organisation to deal with the three vital questions:

- What are our business needs? - Business led
- What are our technical opportunities - Inside out
- What is our current position and capability? - Infrastructure led.

All three 'legs' must exist since innovation always needs a supporting infrastructure, yet all infrastructure with no direction achieves nothing, and direction without creativity is sterile. The approach that is dominant will depend on the organisation's stage of learning about IS strategy, its industry and other ideas once used to select the one approach to planning.

Earl describes five types of planning approach:

1. **Business led approach** - takes business plans as the reference point from which to analyse what IS plans must be. Business drives IS in a rational way. However, business strategies are rarely this clear.
2. Method driven approach - uses a structured IS planning method, believing that formality and rigour is necessary for quality. The plans tend not to be 'owned' by those who will make the IS decisions and remain 'unreal'.
3. **Administrative approach** - emphasises the process of resource allocations and the approvals procedures. This may fit the organisational control style, and, because financial
criteria can be manipulated as symbols of non-financial values, IS choices may closely reflect organisational values.

4. **Technological approach** - produces a model of the business to derive blueprints for IS activities. The technical complexity and the difficulty of comprehending the model generate a lack of organisational commitment. Only small-scale instances are likely to be effective.

5. **Organisational approach** - takes IS strategy planning to be a messy activity that is inextricably bound to other organisational activities. Methods are tools adopted to facilitate particular purposes as the confirmed process unfolds. Teamwork is emphasised and IS resource allocation decisions are taken constantly. The approach may be weak at creating IS infrastructures and may be vulnerable to management changes.

According to Earl, the organisational approach is the most effective. It includes mixtures of planning tools and also sees IS strategy planning as a continual unfolding process. This is in contrast to the structured planning methods that we discuss in the next section and goes against some of the benefits that can be obtained from top-down planning.
3

STRATEGIC PLANNING OF INFORMATION SYSTEMS II

<table>
<thead>
<tr>
<th>Topic List</th>
<th>Page No.</th>
<th>Syllabus Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.4 Developing a Strategy for Information Systems and Information Technology</td>
<td>1.1</td>
<td></td>
</tr>
<tr>
<td>2.5 Information systems and its Alignment with corporate/business strategy</td>
<td>1.1</td>
<td></td>
</tr>
</tbody>
</table>

Introduction
This chapter continues the methodologies discussed in Chapter 2. It further describes the tools which were previously discussed in different IS strategic planning models. Students must ensure that they have understood the concept of Strategic planning and IS strategic planning discussed in the previous chapter.

Study Guide

Considerations for IT Strategic Planning (Study Text Reference 2.4)
- Understanding the business
- Positioning the Business
- Knowing the Business Environment
- Understanding the Risks

Aligning the IT and Business Strategic Plans (Study Text Reference 2.5)
- You might want to lead a debate on what the students think might happen when an IT plan is NOT aligned with the Business plan.
- Discuss the IT trends identified in the Student Guide and open the discussion for other trends that might impact the alignment between the IT and the Business Strategic Plan.

Components of Long Range Plans (Study Text Reference 2.5)
- What is in an IT Strategic Plan? Each organisation will answer this question differently. Discuss any experience that the students might have with strategic planning.
3. **Strategic Planning of Information Systems II**

3.1 **IS/IT Strategy**

Generally the development of an IS strategy involves the following stages:

1. Establishing of organisation’s overall information requirements. (Requirement Analysis)
2. Establishing organisation’s current use of IS/IT, identifying strengths and weaknesses. (IT current situation analysis, CSA)
3. Establishing potential opportunities and threats that IS/IT can bring. (IT Environmental Analysis)
4. Establishing SWOT Analysis

3.2 **Establishing Organisational Information Requirements (Requirement Analysis)**

The organisation as an information-processing entity is shown in the diagram below:

The typical information requirements of organisations that are operating in different sectors such as manufacturing, service, the public sector and non-profit organisations such as charities will all be similar. They all have customers (sponsors, contributors, members), products or services, internal operations, competitors and the environment to obtain information from.
The identification of organisational information needs and the information systems framework to satisfy them is at the heart of a strategy for information systems and information technology. The IS and IT strategies should complement the overall strategy for the organisation. It follows therefore that the IS/IT strategy should be considered whenever the organization prepares its long-term marketing or production strategies. We will look at following methodologies for establishing the information requirement organisation –

1. Enterprise Analysis
2. Critical Success Factors (CSFs)
3. CSF Analysis.
4. Anthony’s levels of management

### 3.2.1 Enterprise analysis

**KEY TERM**

Enterprise analysis involves examining the entire organisation in terms of structure, processes, functions an data elements to identify the key elements and attributes of organizational data and information.

Enterprise analysis is sometimes referred to as business systems planning. This approach involves the following steps.

**Step 1.** Ask a large sample of managers about:
- How they use information
- Where they get information
- What their objectives are
- What their data requirements are
- How they make decisions
- The influence of the environment

**Step 2.** Aggregate the findings from Step 1 into subunits, functions, processes and data matrices. Compile a Process/data class matrix to show: What data classes are required to support particular organisational processes
Which processes are the creators and users of data

Step 3. Use the matrix to identify areas that information systems should focus on, e.g. on processes that create data

### 3.2.2 Critical success factors

The use of critical success factors (CSFs) can help to determine the information requirements of an organisation. One method of prioritising information requirements is using the idea of Critical Success Factors (CSF); in outline, this means that the organisation’s information systems will be directed to producing information on the critical areas of the organisation, rather than providing any and all of the
information that is available. CSF were formulated by John Rockart, at the Sloan School of Management at MIT, as an attempt to identify the real information needs of management, mainly chief executives. CSFs are operational goals. If operational goals are achieved the organisation should be successful.

**KEY TERM**

The limited number of areas in which results, if they are satisfactory, will ensure successful competitive performance for the business. They are the vital areas where ‘things must go right’ for the business to flourish.

The CSF approach is sometimes referred to as the strategic analysis approach. The philosophy behind this approach is that managers should focus on a small number of objectives, and information systems should be focused on providing information to enable managers to monitor these objectives.

Two separate types of critical success factor can be identified. A monitoring CSF is used to keep abreast of existing activities and operations. A building CSF helps to measure the progress of new initiatives and is more likely to be relevant at senior executive level.

- Monitoring CSFs are important for maintaining business
- Building CSFs are important for expanding business

One approach to determining the factors which are critical to success in performing a function or making a decision is as follows.

- List the organisation's corporate objectives and goals
- Determine which factors are critical for accomplishing the objectives
- Determine a small number of key performance indicators for each factor

1. **Data sources for CSFs**

In general terms Rockart identifies four general sources of CSFs.

(a) The **industry** that the business is in.

(b) The **company** itself and its situation within the industry.

(c) The **environment**, for example consumer trends, the economy, and political factors of the country in which the company operates.

(d) Temporal organisational factors, which are **areas of corporate activity** which are currently **unacceptable** and represent a cause of concern, for example, high levels.
3.2.3 CSF analysis

CSF analysis allows managers to articulate their needs in terms of the information that is absolutely critical to them. The process can be illustrated as follows:

```
Critical success factors

<table>
<thead>
<tr>
<th>Key decisions</th>
<th>Key decisions</th>
<th>Key decisions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information requirements</td>
<td>Information requirements</td>
<td>Information requirements</td>
</tr>
<tr>
<td>Information requirements</td>
<td>Information requirements</td>
<td></td>
</tr>
</tbody>
</table>
```

The relationship between the critical success factors, key decisions and information requirements is a process whereby the identification of the CSFs will allow the manager to identify the key decisions related to those CSFs and then the key decisions will give a bridge into the information requirements. The point is to structure and highlight the link between what must be done and why it is needed, either to support a key decision or because it forms a key performance indicator or because it would be a measure of situational control or situational effectiveness.

CSFs provide a way of achieving a clear definition of the information that is needed, limiting the costly collection of more data than is necessary. For example, the parts department of a large organisation may have a business strategy where the CSF is to minimise the length of time a part is kept in stock. One of the key decisions related to that CSF might be to decide what quantities must be ordered. The information requirements may be the order demand.

Meeting the CSF ensures that the investment in stock is kept low and that parts are distributed quickly. IS supplies support for this. For example, a key report would compare part purchasing with part demand patterns, to help managers anticipate order demand without overstocking, whilst at the same time help avoid shortages.

3.2.4 Using Anthony’s levels of management

As we have already discovered, the types of decision-making vary, depending on the levels of management.

The following tables outline the key decisions that must be taken in order to manage the particular CSF and the IS activity necessary for its support i.e., the information requirements. The three levels of management - strategic, tactical and operational management in a manufacturing organisation, are used to provide a framework for these decisions.

**Strategic** - the top management level is associated with long term planning that is unstructured and difficult to measure. The decisions are high risk and have a major impact on the organisation.
### Decision-making Information requirements

<table>
<thead>
<tr>
<th>CSF example</th>
<th>Key decision</th>
<th>Type of IS</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attain profits</td>
<td>Investment needs</td>
<td>Simulation models</td>
<td>Profit forecasts</td>
</tr>
<tr>
<td>New products</td>
<td>Profit targets</td>
<td>Private viewdata</td>
<td>Economic trends</td>
</tr>
<tr>
<td>Market share</td>
<td>What to make</td>
<td>Public viewdata</td>
<td>Industry trends</td>
</tr>
<tr>
<td>Customer services</td>
<td>How to sell</td>
<td>Graphical EIS</td>
<td>Sales analysis</td>
</tr>
<tr>
<td>Quality control</td>
<td>Sales targets</td>
<td>Information retrieval</td>
<td>SBU performance</td>
</tr>
<tr>
<td>Cost control</td>
<td>Location of new factory</td>
<td>Operational summaries and trends</td>
<td>Market research</td>
</tr>
<tr>
<td></td>
<td>Physical</td>
<td></td>
<td>Cost centre analysis</td>
</tr>
<tr>
<td></td>
<td>requirements</td>
<td></td>
<td>Demographic survey</td>
</tr>
<tr>
<td></td>
<td>R&amp;D investment</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Investment needs</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Profit targets</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>What to make</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>How to sell</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Sales targets</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Location of new factory</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Physical requirements</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>R&amp;D investment</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Tactical** - this management level e.g., SBU manager, is focused on control and probably has short-term (budget year), medium risk planning that is structured. The characteristics at this level are performance monitoring, setting rules and motivating.

<table>
<thead>
<tr>
<th>CSF example</th>
<th>Key decision</th>
<th>Type of IS</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effective management and control of:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Money</td>
<td>Set standards</td>
<td>Budgets</td>
<td>Sales analysis</td>
</tr>
<tr>
<td>People</td>
<td>Monitoring and action on variances</td>
<td>Modelling</td>
<td>Summary totals</td>
</tr>
<tr>
<td>Machines</td>
<td>Order levels and quantities</td>
<td>Performance and exception reporting</td>
<td>Variance reports</td>
</tr>
<tr>
<td>Resources</td>
<td>Select best option for identified need</td>
<td>Quantitative techniques</td>
<td>Cash flow forecast</td>
</tr>
<tr>
<td>Stock</td>
<td>Overtime introduction</td>
<td>Office automation</td>
<td>Personnel records</td>
</tr>
<tr>
<td></td>
<td>Specify training</td>
<td>Report generators</td>
<td>Management reports</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(for editing)</td>
</tr>
<tr>
<td><strong>Effective management</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>and control of:</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Money</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>People</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Machines</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Resources</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Stock</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Operational** - this management level e.g., supervisory, is focused on routine day-to-day control, low risk planning that is highly structured.

<table>
<thead>
<tr>
<th>CSF example</th>
<th>Key decision</th>
<th>Type of IS</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Meet targets</td>
<td>Schedule production</td>
<td>Transaction processing</td>
<td>Stock list</td>
</tr>
<tr>
<td>Follow procedures</td>
<td>Requisition materials</td>
<td>Database to support enquires e.g.</td>
<td>Picking list</td>
</tr>
<tr>
<td>Attain standards</td>
<td>Buy stock</td>
<td>Production control</td>
<td>Invoices</td>
</tr>
<tr>
<td></td>
<td>Re-order stock</td>
<td>Purchase ledger</td>
<td>Production order</td>
</tr>
<tr>
<td></td>
<td>Price an order</td>
<td>Sales ledger</td>
<td>Completion dates</td>
</tr>
<tr>
<td></td>
<td>Allow credit</td>
<td>Order processing</td>
<td>Outstanding debts</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Schedule</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>production</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Requisition</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>materials</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Buy stock</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Re-order stock</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Price an order</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Allow credit</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

There are different things that each level of management must “do right” in order for their job, and the overall results of the organisation, to be a success. CSFs and Anthony’s hierarchy of management can help determine what these things actually are. Having determined what these critical activities are, then the information system can be built to ensure that detail on these activities are provided in a timely fashion.

### 3.3 IT Current Situation Analysis
Information system resource analysis or current situation analysis (CSA) involves a review of all information system and information technology used within an organization. The review includes all aspects of hardware, software, communication devices, network topologies, system development methodologies, maintenance procedures, contingency plans and IS/IT personnel. The review looks at all of the aspects in the context of the organizational overall strategy and the IS/IT strategy. This analysis is also called resource analysis and it establishes the current status of IS/IT within an organization. Techniques that could be useful when conducting a CSA are:

1. Nolan’s stage Model
2. Earl’s Grid
3. McFarlan IS Strategic Grid
4. Application Portfolio

### 3.3.1 Nolan’s stage Model

Richard Nolan’s stage hypothesis, outlined below, attempts to model the stages organizations go through in their use of IS/IT. It looks at the following four factors at each stage: Applications, Organization, Controls and Users.

<table>
<thead>
<tr>
<th>Stage</th>
<th>Applications</th>
<th>Factors</th>
<th>Controls</th>
<th>Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initiation</td>
<td>The objective is to discover to identify suitable applications (eg payroll), and to save money on clerical processing. There are a number of separate IS/IT applications that carry out restricted, well-defined tasks.</td>
<td>IS/IT is a distinctly separate department, for technical experts.</td>
<td>There are computer controls, but few management controls and little planning.</td>
<td>Users have little involvement.</td>
</tr>
<tr>
<td>Contagion</td>
<td>Many more applications are developed, but a lot of time is spent updating old ones. This is a period of unplanned, haphazard growth.</td>
<td>The IS/IT department is still centralised, but end-users begin to influence what it does. Programmers become more sensitive to user needs.</td>
<td>are still very lax. IS/IT is a corporate overhead, and budgetary control over IS/IT expenditure is limited. Furthermore, there are few checks over requests for more applications.</td>
<td>Users are enthusiastic about IS/IT, but have little understanding as to its benefits and drawbacks.</td>
</tr>
<tr>
<td>Control</td>
<td>There are restrictions on the development of new systems; existing applications are consolidated. Users might feel frustrated.</td>
<td>The IS/IT function is properly organised and headed by a manager, who has to justify expenditure, just as is the case with other departments.</td>
<td>Financial, quality and other controls (e.g. steering committees) are introduced over projects and purchases. User departments begin to be charged for the IS/IT resource, as a way of controlling costs. However, controls are mainly exercised in and</td>
<td>Users begin to understand IS/IT.</td>
</tr>
</tbody>
</table>
## IT Current Situation Analysis

<table>
<thead>
<tr>
<th>Stage</th>
<th>Applications</th>
<th>Factors Organization</th>
<th>Controls</th>
<th>Users awareness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integration</td>
<td>Applications begin to cross the boundaries of each business function (e.g. integrating sales order processing and stock control). However, data is often duplicated, so there is an attempt to integrate information and accounting systems. <strong>A management information system</strong> enables managers to get information about many of the firm's activities from a database.</td>
<td>Perhaps a higher profile for IS/IT?</td>
<td>More planning is introduced to IS/IT</td>
<td>User involvement in policy and project management increases.</td>
</tr>
<tr>
<td>Data Administration</td>
<td>The organisation seeks to develop a single integrated database serving organisational needs, and applications are devised to use the database.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maturity</td>
<td>Applications. In theory, data about all the organisation's activities find their way into can information system, which can be interrogated in a variety of ways. If the information is analysed with sufficient rigor it may be possible to discover those areas in the organisation's value chain where savings can be made or advantages delivered.</td>
<td>Information is now able to be used as a source of competitive advantage. There is an emphasis on strategic issues.</td>
<td>Control data is used flexibly.</td>
<td>Users become more accountable themselves for the integrity and correct use of information.</td>
</tr>
</tbody>
</table>
3.3.2 **Earl’s Grid**

An extremely useful tool at this stage of planning is the systems audit part of Earl's model (Earl 1989). The approach acknowledges the fact that most organisations have some form of computerised information system already in place. These existing systems need to be audited in terms of their technical merits, their use to the business, their age (and hence maintainability) and their ease of use. Earl suggests a useful tool to help in such an analysis which is a form of grid, the 'systems audit grid'. Each of the current systems is allocated a place on the grid shown below. The illustration indicates possible strategies for dealing with the organisation’s existing systems by identifying the quadrant in which they fall.

```
<table>
<thead>
<tr>
<th>Business value</th>
<th>Low</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Divest</td>
<td>Re-assess</td>
</tr>
<tr>
<td>High</td>
<td>Renew</td>
<td>Maintain/ enhance</td>
</tr>
</tbody>
</table>
```

**EXISTING SYSTEMS STRATEGY**

The assessment of the technical merit of the system can be determined by answering the following questions (Warwick):

- What is the cost-effectiveness of the system?
- What is the system's maintainability? This is a measure of the time taken and the cost involved in both routine maintenance and enhancement. It is dependent on the age and amount of structural degradation that the system has undergone.
- How reliable is the system, and is that reliability showing signs of decreasing?

The business value of the system would be established by consultation with the strategic managers of the business, possibly by discussion at the IS steering committee.

3.3.3 **McFarlan IS Strategic Grid**

The importance of IT to the organisation was examined by McFarlan and McKenney in 1983. They suggested that dependence on IT of any organisation could be classified into a matrix based on the Boston Consulting Group (BCG) matrix.
This matrix classifies organisations into four types:

- **Support.** The business sees no strategic value in its Information Systems.
- **Factory.** The business sees the strategic significance of its Information Systems now, but predicts that this will disappear in the future.
- **Turnaround.** The business expects that the Information Systems will become strategically important in the future.
- **Strategic.** The business depends on its Information Systems for competitive advantage and expects to continue to do so.

**Support** - where IT has a support role and is also a necessity to the working of the organisation, information systems have little relevance to the organisation's core activities. The current information system may include accounting operations and payroll but there are no new developments that can contribute significantly to the competitiveness of the organisation, other than a reduction of administrative costs.

There is usually a low level of senior management involvement in this situation because the commitment to information systems planning is low, and any development would rely on localised management.

Michael Earl in *Management strategies for information technology* gives a cement manufacturing company as an example in this sector. Information technology may be used to speed up administration and make occasional improvements to the processes but it is not vital or critical to the manufacture or distribution of cement.

**Factory** - if information technology has a factory role, the organisation depends heavily on information systems support for smooth operations. Future IT developments are not likely to add to their competitive edge. Earl mentions a steel works with an on-line real time system for controlling production. Even one hour of disruption to these organisation's booking systems or order processing systems could fundamentally damage their competitive performance.

McFarlan and McKenney maintain that strategic goal setting and linkage of information systems to the corporate plan are not too important if IT has a factory role.
**Turnaround** - information technology's turnaround role is where existing IT is not too important, but future development is likely to have a significant impact. In these organisations the applications under development have a high potential to contribute to the organisation's strategic objectives. Many supermarket chains have relied on routine information systems for accounting, stock control and ordering. However, most of the chains, to reduce wastage on perishable items and to maximise sales, are investing heavily in communication systems to link their suppliers and stock control systems. They are also installing electronic funds transfer (EFT) at the point of sale.

The performance of firms in a turnaround situation is often inhibited by lack of support from the information-processing department. There is a need for planning in this cell because the firm cannot maintain control over its rapidly expanding operations without the new computer applications.

**Strategic** - in some organisations the information technology's strategic role is where existing and future developments are at the heart of the organisation's future success. Banks and insurance companies are typical of this sector. They have applications, which they rely on for the smooth running of their day-to-day activities, and they have future developments, which are vital to their competitive success and are integral to the organisation's strategic objectives. These firms need significant amounts of planning, as the firm would be at a disadvantage if the information processing did not perform well.

**Case Example**

In 1991 British Airways was spending £150 million on information technology. Although the core of their business activity was transporting people by aeroplane, doing this profitably and maintaining excellence of service was highly dependent on the management of information. To help sell seats, one of the largest computers outside the defence industry was used. The BA system could extract data from anywhere in their network in two seconds. The airline could link seat availability to the currency a potential passenger used, limiting the availability for those paying in weaker currencies. It also included sophisticated overbooking management to ensure that the majority of passengers would not be upset and, if they were, they would be compensated. The management of BA regarded IT as a key strategic tool for competitive and profitable performance. The airlines continue to spend large amounts on IT.

### 3.3.4 The applications portfolio

A development of the strategic grid that can be used to look at the portfolio of systems is the ‘applications portfolio’ suggested by Peppard. This looks at the strategic impact of individual applications within the organisation, and classifies them as if they were products in the BCG matrix.

<table>
<thead>
<tr>
<th>Strategic importance in the predicted competitive environment</th>
<th>High potential</th>
<th>Strategic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Support</td>
<td>Key operational</td>
</tr>
<tr>
<td>Low</td>
<td>High</td>
<td>Strategic importance in the current competitive environment</td>
</tr>
</tbody>
</table>
Like McFarlan, Peppard suggests four classifications. This time, an organisation would use the grid to target those applications within its portfolio that have the greatest strategic potential. The four categories are as follows:

- **Support.** These are applications that improve management effectiveness but are not critical to the business. The benefits they deliver are mainly economic. Examples include accounting systems, payroll systems, spreadsheets and legally required systems.

- **Key operational.** These applications are critical to sustain the existing business. Such applications generally support core organisational activities. Examples include inventory control, production control and order management.

- **Strategic.** These applications are critical to future business.

- **High potential.** These applications are innovative, and might be of future strategic potential. Examples might include the use of the Internet, expert systems, or multimedia.

### 3.4 IS/IT Environmental Analysis

All managers should seek to understand the relationship between the organisation and its environment, whether they operate a business, government agency, charity or university. One method to achieve this is to consider the various groups, both internal and external, that can affect or be affected by the accomplishment of its objectives. Each of these groups has a ‘stake’ in the survival of the organisation. The various environmental forces impacting on the organisation are outlined in the diagram below:

![Environmental Analysis Diagram](image)

We will analyse the impact of environment on the IS/IT strategy using the following tools:

1. Opportunities and Threats
2. PEST Analysis

#### 3.4.1 Opportunities And Threats

The identification of opportunities and threats that could impact on IS/IT strategy relies on **creative thinking**. Threats are often opportunities that have not been identified by the organisation, but have been by competitors. There are three ways in which creative thinking and opportunity ‘spotting’ can be encouraged.
(a) Techniques to foster innovation, such as think tanks, brainstorming sessions and do so forth, are useful if they encourage ideas. Some of the most successful systems developments have resulted from ideas that users have had about how a system should evolve, or come from customers.

(b) Processes for innovation require organisational investment. Fostering innovation activities include:

(i) Recruiting outsiders.

(ii) Experimenting with innovative projects outside the main business.

(iii) Looking to users and suppliers for ideas.

(c) Technology. Providing user-friendly systems enables users to develop creative applications. For example, providing an easy-to-use expert system shell might enable users to develop their own. The organisational environment has to allow innovation to happen.

External analysis is also necessary in all the stages in IS strategy, for example in monitoring developments in technology, or where possible, examining systems used by competitors. Organisations exist within an environment which strongly influences what they do and whether they survive and develop. Strategic must take account of environmental influences if they are to be realistic and achievable. These environmental influences are shown in the following diagram.

### 3.4.2 PEST Analysis

PEST analysis is a general technique that can be applied in a range of situations. Below sets out some examples of how PEST factors may influence the strategic planning of information systems. The relevant factors will depend to a large extent on the actual situation or scenario.

<table>
<thead>
<tr>
<th>PEST factor</th>
<th>Possible influence on IS strategic planning</th>
</tr>
</thead>
</table>
| **Political** | - Tax legislation, e.g. can the system cope with changes  
- Employment legislation; e.g. attitude to contractors  
- Data protection legislation; e.g. does the system comply, is it flexible  
- Nationalisation; e.g. is the company at risk and therefore should investment in the system proceed  
- General stability; e.g. is the business environment stable enough to justify further investment  
- Intellectual property laws; e.g. does the system comply, is our software protected |
| **Economic** | - Economic growth; e.g. the level of demand and volume of transactions  
- Relative strength of the national economy; e.g. relatively low economic growth in the home economy, compared with overseas, may lead to disparity in salary levels and a loss of skilled systems developers to other countries  
- Business partners; e.g. are those organizations we depend on for sales and supplies likely to be affected by economic trend |
| **Social** | - Relevant social attitudes; e.g. an information system for a pharmaceutical company conducting research using animals may need greater security.  
- Relative strength of the national economy; e.g. relatively low economic growth in the home economy, compared with overseas, may lead to disparity in salary levels and a loss of skilled systems developers to other countries  
- Business partners; e.g. are those organizations we depend on for sales and supplies likely to be affected by economic trend |
| **Technological** | - Infrastructure development; e.g. are communications links of sufficient standard |
### SWOT Analysis

The general management technique of SWOT analysis can be applied to the development of information systems strategy.

#### KEY TERM

SWOT analysis, when used as a technique for identifying opportunities information systems development, aims to determine:

- What strengths does our (overall) information system have? (How can we take advantage of them?)
- What weaknesses does the system have? (How can we minimize them?)
- What opportunities, outside the information system, are there in the organisation or beyond? (How can we capitalize on them?)
- What threats, outside the information system, might prevent us operating or improving the information system?
- (How can we protect ourselves from them?)

The strengths and weaknesses analysis has an internal focus. The identification of shortcomings in a system could lead to a decision to enhance the current system or to purchase a new system. Opportunities and threats are considered as part of an external appraisal, or environmental scan. The internal and external appraisals of SWOT analysis will be brought together. The analysis aims to ensure that a strategy is not followed without considering the wider implications.

(a) Major strengths and profitable opportunities can be exploited especially if strength and opportunities are matched with each other.

(b) Major weaknesses and threats should be counted, or a contingency strategy or corrective strategy develop.

The application of SWOT analysis to an information systems scenario is shown in the following question.

### Question 1

Scenario

Nasar & Co. operates 150 retail stores nation-wide. Each store sells a wide variety of consumer goods including kitchenware, clothing, electrical appliances, computers and peripherals, sporting goods, toys and hardware. Very few goods are displayed in Nasar & Co. stores. Customers choose items they wish to purchase from copies of the Nasar & Co. catalogue. Customers write the product code on order slips and take completed slips to sales counter staff to complete the sale. Most goods are held at the back of the service area, enabling customers to take their items with them when leaving the store. Larger, or out-of-stock items are delivered within 48 hours to the customer's address. Nasar & Co. has been established for over 50 years and has developed a reputation as an efficient, reputable retailer of good quality goods. However, sales have stagnated over the last three years- Senior management believe sales are being lost to
competitors, particularly those that offer customers on-line purchasing using an Internet website. Nasar & Co. is now considering an investment of Rs.10 million in a system that would provide on-line purchasing to customers over the Internet. Much of the Rs.10 million is necessary to replace existing back-office systems that would not be able to integrate with the web-based system.

Required
Produce a brief SWOT analysis relevant to the proposed new system at Nasar & Co.

Answer

Strengths
- Rs.10 million is available for the new system
- Existing warehouses and delivery infrastructure could be used with the new system
- Although Nasar & Co. has no experience of web technology, the organisation is IT literate

Weaknesses
- The amount of extra sales the site will generate is unclear
- Nasar & Co. has no in-house web expertise
- Stock holding levels may need to be higher to ensure prompt delivery
- The on-going costs of staff time and expertise to keep the site operational and up-to-date

Opportunities
- E-commerce provides a new sales channel and revenue stream
- Partnerships with suppliers may be forged allowing delivery direct from the factory
- The use of 'cookies', database and data mining technology to establish more profitable customer relationships

Threats
- The security implications of establishing Internet links
- Timing - Nasar & Co. has missed 'first-mover' advantage
- Consumer resistance to on-line purchasing
- The possibility of losing Nasar & Co. distinct catalogue-based market position (becoming just and retailer with a web-site).

The following general points may be of use when applying SWOT analysis to a particular information systems scenario.

1. **Economic/industry context**

**IT is an enabling technology,** and can produce dramatic changes in individual business and whole industries, especially where there are other major forces for change.

2. **Stakeholders**

Stakeholders are affected by an organisation's use of IT.

(a) **Customers and suppliers** have preferences as to how IT should be used (e.g., electronic data interchange, intranet).

(b) **Governments** have an interest in the legal aspects of copyright, data protection, security and e-commerce.

(c) **IT manufacturers** pioneer the development and use of new technology.
(d) **Consumers:** both their expectations of IT and their willingness to use it are important for its success.

(e) **Employees** and other internal users are interested as IT affects work practices.

### 3. Technical issues

A strategic view of IT must take detailed technical issues into account. For example, two UK building societies abandoned a merger because of incompatibility between their computer systems. The security of IT-based systems must be considered.

### 4. The importance of management

Success or failure in implementing IS/IT depends on the systems themselves and the management effort behind them. An implementation or strategy will fail if:

(a) The system is designed to tackle the wrong problem, that is, the use of IT has not been thought through in the wider organisational context.

(b) If senior management are not interested in, and do not appreciate the significance of, IT based choices.

(c) If users are ignored in design and development.

(d) When no attention is given to behavioural factors in design and operation.

---

**Case example**

An example of the importance of the wider organisational processes for the success of information technology is provided by the Taurus project.

This was a project, funded by various institutions in the City of London and managed by the Stock Exchange, to computerise certain aspects of share trading and registration. There was an existing computer system, Talisman, but for various reasons it was regarded as being no longer suitable.

(a) A new system was felt to be necessary to cope with increased trading volumes.

(b) Stock markets and bourses elsewhere in Europe already used computerised settlement systems, giving increased competition to London as a financial centre.

However, the plans to develop a computer system failed, at a substantial cost to City institutions and damage to London's reputation as a financial centre. What went wrong? There was nothing inherently impossible about the task: automated settlement has been achieved in other financial centres. A number of reasons were suggested.

(a) Poor project management with inadequate control.

(b) The system was designed to replicate existing structures. Rather than use one central database, it was decided to use a system of separate but linked databases. Not to do so would have taken away business (and profits) from share registrar companies. The design was made unnecessarily complex in order factor for all the vested interests. This then is an instance of the neutralization of technology's possible benefits by wider social and organisational choices.
3.6 **Information Systems and Competitive Environment**

Environmental analysis for development of IS strategy should also consider the competitive advantage that could be attained by using IS/IT. Porter and Millar state that IS/IT has the potential to change the nature of competition within an industry in three ways. IS/IT can:

1. **Change the industry structure**
2. **Create new businesses and industries**
3. **Be used to create competitive advantage**

Following Sections of this chapter look at these three areas.

### 3.6.1 Changing the industry structure

Porter's five forces model can be used to analyse the effect of IS/IT on an industry. Porter identified five competitive forces operating in a competitive environment.

(a) The threat of new entrants.
(b) The bargaining power of suppliers.
(c) The bargaining power of customers.
(d) The threat of substitute products/service.
(e) The existing competitive rivalry in the industry.

**New entrants**

IS/IT can have two possible roles in relation to barriers to entry,

(a) Defensively, IS/IT can increase economies of scale, raise the capital cost of entry (by requiring a similar investment in IS/IT) or effectively colonising distribution channels by tying customers and suppliers into the supply chain or distribution chain.

(b) Offensively, IS/IT can leap over entry barriers. An example is the use of telephone banking, which sometimes obviates the need to establish a branch network.

**Suppliers**

Supplier power can derive from various factors such as geographical proximity and the fact that the organisation requires goods of a certain standard in a certain time. The bargaining power of suppliers can be eroded by IS/IT in three ways.

a) By increasing competition between suppliers- IS/IT can provide a purchases database, which enables easy scanning of prices from a number of suppliers.

(b) Suppliers' power can be shared. An example is using CAD and so forth to design components in tandem with suppliers. Such relationships might be developed with a few key suppliers. The supplier and the organisation both benefit from performance improvement.

(c) Suppliers can be integrated, in purely administrative terms, by a system of electronic data interchange.
Case example

Some German companies have reported losing lucrative home markets because the Internet has made it easier for customers to access and compare prices from other suppliers. Geographical price discrimination is becoming harder to sustain in an age where 'a shopper with a credit card and computer can sit at home and order from around the world'. The Internet has therefore increased competition, and is used by many organisations as a competitive weapon.

Customers

The bargaining power of customers can be affected by using IS/IT to 'lock them in'.

(a) IS/IT can raise switching costs (in both cash terms, and in terms of operational inconvenience). An example is where IS/IT provides a distribution channel for certain services (e.g. airline tickets). Another example comes from the computer industry itself—until the advent of the PC, most computers were run with proprietary software: in other words, you could not run ICL software, say, on IBM mainframes. This made any switch in supplier (of hardware or software) too much trouble to contemplate.

(b) Customer information systems can enable a thorough analysis of marketing information so that products and services can be tailored to the needs of certain segments.

Substitutes

IT has the following relationship to existing and substitute products and services.

(a) In some cases IT/IS itself is the 'substitute'. PC-based word processing packages are a substitute for typewriters, e-commerce is a substitute for a high street shop.

(b) IT is the basis for new leisure activities (e.g. computer games). Alternatively, IT based systems can imitate existing goods (e.g. electronic keyboards imitating pianos).

(c) IT can add value to existing services by allowing more detailed analysis (as in a geographical information system), by generating cost advantages, or by extending the market.

(i) The cost advantages of microprocessors massively extended the market for computing.

(ii) Earl quotes the example of an econometrics firm, whose innovation enabled PC users to access its database, broadening the reach of the company's services.

Rivalry

IT can be used to compete - as a source of competitive advantage. This is covered later in this chapter. Alternatively, IT can be used as a collaborative venture, perhaps to set up new communications networks. An example is the perceived threat that IT-based firms like Reuters pose to stock exchanges and commodities exchanges. A communications network soon becomes something that can be marketed. Some competitors in the financial services industry share the same ATM network—(Also see the following section.)

Porter's five forces model has come in for criticism in recent years.

(a) The model relies on a static picture of the competition and therefore plays down the role of innovation.

(b) It over emphasises the importance of the wider environment and therefore ignores the significance of possible individual company advantages with regard to resources, capabilities and competence.
3.6.2 Creating new businesses and industries

There have been many examples in the last decade of IT affecting the competitive business environment by creating new businesses. This may take the form of a completely new business or a significant change to an existing business.

For example, the Internet Service Provider industry is a completely new industry result from technological change. The publishing industry provides a good example of an existing industry affected by IS/IT. Encyclopaedia publishers such as Encyclopaedia Britannica have moved in recent years from solely paper-based products to paper and CD-ROM, and then again to a hybrid CD-ROM/Web-based product. The nature of competitors can also be influenced by developments in technology. For example, Encyclopaedia Britannica now has to compete not only against traditional encyclopaedia producers, but also against software companies such as Microsoft (with Microsoft Encarta).

Technology has increased the amount of information that can be collected. For example, the use of bar-code scanners in retail outlets means accurate sales data is available across all product ranges. This data is then available for further analysis, perhaps against customer profiles obtained under 'customer loyalty' schemes. This information could be used internally, and/or could be offered for sale to producers or other interested parties.

3.6.3 Using IS/IT for competitive advantage

As the importance of information has increased over the last two decades, organizations have realised that Information Systems (IS) and Information Technology (IT) can be used as a source of competitive advantage. We will analyze the competitive advantage in the light of following theories:

1. Porter Generic Strategies
2. Porter’s Value Chain
3. Other writers

KEY TERM

Competitive advantage is a profitable and sustainable position. It exists in the minds of customers, who believes the value the will receive from a product or service is greater than both the price they will pay and the value offered by competitors.

1. Generic strategies for competitive advantage

Porter proposes three generic strategies for achieving competitive advantage.

(a) Cost leadership means being the lowest-cost producer in the industry as a whole. A cost leadership strategy seeks to achieve the position of lowest-cost producer in the industry.

(b) Differentiation is the exploitation of a product or service which the industry as a whole believes to be unique. A differentiation strategy assumes that competitive advantage can be gained through particular characteristics of a product or service.

(c) Focus involves a restriction of activities to only part of the market (a segment or niche) through:
(i) Providing goods and/or services at lower cost to that segment (cost-focus)

(ii) Providing a differentiated product or service to that segment differentiation-focus

Cost leadership and differentiation are industry-wide strategies. Focus involves segmentation - pursuing within the segment a strategy of cost leadership or differentiation. Examples of how IS/IT can support each of these strategies are shown in the following table.

<table>
<thead>
<tr>
<th>Strategy</th>
<th>How IS/IT can support the strategy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost-leadership</td>
<td>By facilitating reductions in cost levels, for example by reducing the number of administration staff required.</td>
</tr>
<tr>
<td></td>
<td>Allowing better resource utilisation, for example by providing accurate stock information allowing lower 'buffer' inventories to be held.</td>
</tr>
<tr>
<td></td>
<td>Using IT to support just-in-time and advanced manufacturing systems.</td>
</tr>
<tr>
<td>Differentiation</td>
<td>Differentiation can be suggested by IT, perhaps in the product itself or in the way it is marketed.</td>
</tr>
<tr>
<td></td>
<td>The publishing example quoted earlier provides evidence of this with the move from paper-based products to electronic.</td>
</tr>
<tr>
<td>Focus</td>
<td>IT may enable a more customised or specialised product/service to be produced.</td>
</tr>
<tr>
<td></td>
<td>IT also facilitates the collection of sales and customer information that identifies targetable market segments.</td>
</tr>
</tbody>
</table>

2. Porter's value chain

Michael Porter analyses the various activities of an organisation into a value chain. This is a model of value activities (which procure inputs, process them and add value to them in some way, to generate outputs for customers) and the relationships between them. Value chain analysis can be used to assess the impact of IS/IT, and to identify processes where IT could be used to add value. IT can be used to automate and improve physical tasks in the manufacturing sector. It also, provides extra information about the Operations.

(a) Process control. Computer systems enable tighter control over production processes.

(i) It is possible to measure many aspects of the production process.

(ii) A variety of control techniques are available.

(b) Machine tool control. Machine tools can be automated and, it is hoped, be made more precise.

(i) Numerical control: information to operate the machine tool is prepared in advance to generate a set of instructions,

(ii) Computer numerical control is where the computer produces the instructions.

(iii) Direct numerical control is where the computer is linked directly to the machine tool.

(c) Robots can automate some of the process.

(d) Computer aided manufacturing (CAM) involves a variety of software modules.

- Production control) supervisory systems
• Materials requirement planning (MRP) and MRP II
• Capacity requirements planning

(e) Computer Integrated Manufacturing (CIM) integrates all aspects of an organisation's manufacturing activities. "IT cannot solve basic organisational problems, but the essence is the use of the IT to provide integration though communication, effectiveness and efficiency." Flexible manufacturing systems include:

• Machine tools
• Materials handling conveyor sets
• Automatic guided vehicles

(f) Enterprise Resource Planning (ERP) systems take MRP II systems a step further, and are not restricted to certain types of organisation. ERP systems are used for identifying and planning the enterprise-wide resources needed to record, produce, distribute, and account for customer orders.

In both inbound logistics and outbound logistics IT can have an impact.

(a) The use of IT in inbound logistics includes stock control systems such as MRP, MRPII, ERP and JIT.

(b) Warehousing. The use of barcodes can increase knowledge about the quantity and nature of stock in hand.

(c) It is possible to create computer models, or virtual warehouses, of stock actually held at suppliers. For example an organisation with several outlets might have each connected to a system which indicates the total amount of stock available at different sites.

Marketing and services can be made more effective by customer databases enabling market segmentation.

(a) Buying and analysing a mailing list is a more precise method of targeting particular groups of consumers than television advertising.

(b) A variety of market research companies use IT to monitor consumers' buying habits.

(c) Supermarkets can use automated EPOS systems to have a precise hour-by-hour idea of how products are selling to enable speedy ordering and replenishments.

Customer relationship management (CRM) describes the methodologies, software, and usually Internet capabilities that help an enterprise manage customer relationships. For example, an enterprise might build a database about its customers that described relationships in sufficient detail so that management, salespeople, service staff, and maybe the customer, could access information, match customer needs with product plans, remind customers of service requirements and know what other products a customer had purchased.

As far as support activities are concerned IT has some impact.

(a) Procurement. IT can automate some purchasing decisions. Paperwork can be saved if the organisation's purchase systems are linked directly to the sales order systems of some suppliers (e.g. by electronic data interchange).

(b) Technology development. Computer automated design (CAD) is, in a number of areas, an important influence.

(i) Drafting. CAD produces engineer's drawings, component design, layout (e.g. of stores, wiring and piping) and electronic circuit diagrams in complex systems.
(ii) Updating. It is easy to change design in CAD systems and to assess ramifications of any changes. Some CAD systems have archive data (e.g. for reference).

(iii) CAD enables modelling to be checked without the necessity of producing working prototypes. Some 'stress testing' can be carried out on the model.

(c) There is perhaps less impact on human resources. However, the HR applications include the maintenance of a skills database, staff planning (e.g. using network analysis), computer based training, time attendance systems, payroll systems, pension systems.

3. **IS/IT and competitive advantage - other writers**

- **Ward and Griffiths** suggested four ways that IS/IT could be used for competitive advantage:
  
  (a) Linking the organisation to customers or suppliers, eg EDI, website, VAN, extranet.
  
  (b) Creating effective integration of the use of information in a value-adding process, e.g. data-mining, ERM.
  
  (c) Enabling the organisation to develop, produce, market and distribute new products or services, e.g. CAD, CRM.
  
  (d) Giving senior management information to help develop and implement strategy, e.g. knowledge management.

- **Moriarty and Swartz** provide an example of how the application of IS/IT can generate a competitive advantage in relation to the sales and marketing function. They explain how technology can increase productivity through providing better marketing information (e.g. databases), and more efficient sales and marketing tools (e.g. direct mail, websites). To be classed as a competitive advantage the increased productivity would not be available to others. This is unlikely unless the technology is too expensive (entry barrier), or competitors are unaware of how to utilise it. Increased productivity may lead to reduced fixed costs. For example, fewer sales and marketing staff may be required, allowing a move to smaller premises. The effect of reduced fixed costs is shown in the following diagram,

- **Peppard** summarises the ways in which IS/IT can be used for competitive advantages as:
  
  - Establishing entry barriers
  - Affecting the cost of switching operations
  - Differentiating products/services
  - Limiting access to distribution channels
  - Ensuring competitive pricing
  - Decreasing supply costs
  - Increasing cost efficiency
  - Using information as a product
  - Building closer relationships with supplies and customers
### 3.7 Information Systems and Its Alignment with Corporate/Business Strategy

The stages associated with a top down matching of business strategies to IS strategies might look like the following diagram. This model can be used to select relevant planning techniques for each stage in the process.

![Diagram of IS alignment process]

**Business objectives**  
What we want to achieve

**SMIS requirements**  
What we need to do and where we need to be

**Current position**  
Where we are now

**Position comparison**  
Analyse/map the gap

**IS policies**  
Strategic decisions

**Plans for IS/IT**  
Project selection

**Implementation**  
Project management

**Review**  
Analyse what changed and what was learnt

There may be several techniques to choose from for each of the stages and therefore issues such as the familiarity with the technique and the nature of the planning environment can be the motivation of the selection process, provided the objective of that step is achieved.

All the top down methods are formalised and aim to appeal to managers. They have the advantage of being re-done as business needs change and they give IS direction setting rather than detailed plans. Examples include Ward’s strategic information systems planning approach; King’s strategy set transformation and CSF analysis (discussed earlier in this chapter).

#### 3.7.1 Ward's Top down aligning of IS and business strategies

Ward, in *Integrating Information Systems into Business Strategies*, outlined a framework that is a rational, clearly explained approach suggesting how a collection of models can be combined. Ward's model uses pointers to strategies for IS resourcing, structure and management that are demonstrably linked to business objectives.

Below is an overview of Ward's model identifying the frameworks that it explores:
(i) Porter's generic competitive strategies  
(ii) Parson's generic IS strategies  
(iii) Default relationship between Porter's and Parson's strategies  
(iv) Nolan's stages of IS maturity  
(v) Default relationship between Nolan's model and Parson's strategies  
(vi) McFarlan's strategic importance of IS  
(vii) Relationship between McFarlan's model and Parson's strategies  
(viii) BCG product portfolio analysis  
(ix) Relationship between BCG analysis and Parson's strategies  

**To build consistency**

```
<table>
<thead>
<tr>
<th>Business value</th>
<th>IS maturity</th>
<th>Business strategy</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Portfolio of IS strategies</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- which includes the management and resource demands</td>
</tr>
</tbody>
</table>
```

However, Ward's approach will only be appropriate at the SBU level where a single competitive stance is definable because this is the starting point - the definition of the organisation's generic business strategy e.g., low cost, differentiation or focus. For any given generic business strategy, Ward suggests that there is a default relationship to Parson's generic IS strategies. Given a particular business approach, certain approaches would be expected to emerge where there is perhaps no conscious direction of the pattern of IS resource allocation.

For example:

- Overall cost leadership leads to: Scarce resource  
  - Free market

- Differentiation leads to: Monopoly  
  - Leading edge

- Focus/niche leads to: A secondary business strategy.

Although this may be the default relationship, the default or emergent strategy may be entirely inappropriate, particularly for organisations where IS has great importance.

The relevant strategy is one that is business consistent. Ward suggests a process for this which builds consistency with the IS management maturity (Nolan) and with the strategic importance IS has for it. By building on these two particular analysis tools an IS strategy that is both feasible (matching the IS maturity stage) and desirable (matching the strategic importance segment) will be implemented.

The first step is to use the notion of match between IS strategy and the state of maturity. Having established at what stage the organisation (or SBU) is with respect to a specific form of IS, then the suggested IS strategy can be 'read off'. This means that different IS strategies are going to be consistent with different stages of maturity of use and management of IS. The relationship is shown in the diagram below:
The IS strategy indicated by this model may not be the one emerging as a result of the nature of the organisation's competitive position. Also, depending on the stages of growth model used, repeating cycles of stages 1-3 are to be expected but associated with different, new technologies.

4.3 The strategic grid

McFarlan’s strategic grid can also be used to help define the planning process. The strategic importance grid can define two things:

(i) the combined strategic importance of IS to the organisation;
(ii) the business value weightings of different elements of the IS portfolio.

The current and planned systems portfolio represents a collection of IS activities, each of which holds a different value to the organisation and so should be treated differently. As shown in the diagram below, the generic IS strategies have a relationship to the four segments of McFarlan's strategic importance grid. Each segment has a 'best fit' IS strategy.
Since the strategic importance grid is closely related to the Boston Consulting Group (BCG) growth-share matrix, the product portfolio management implications can be lifted into the IS strategy world. The growth-share matrix helps organisations with a portfolio of SBUs decide whether to invest to increase market share, use a business as a source of finance for investment in other businesses or whether to divest. So it contributes to the strategic planning process by supporting strategic option generation.

The diagram below shows the BCG matrix segment name matched onto the strategic importance grid. It also illustrates the viability of the IS strategy, the dominant structural pressure, the strongest influencing factor, the level of justified resource use and behavioural focus of the responsible manager or group.

Not all of the organisation's applications will be strategically important and so a scarce resourcing strategy will be relevant for some parts of the portfolio. Similarly, not all of their applications will be valueless and a centrally planned strategy may be appropriate for some parts of the portfolio.

### 3.7.2 Management and Behavioural styles

The IS strategy planning process can learn from the experience of product portfolio management and can be sensitive to the fact that different management styles are required to reflect the different segments.

<table>
<thead>
<tr>
<th>Segment</th>
<th>Managerial style</th>
<th>Behavioural style</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategic</td>
<td>Needs flexible and sensitive handling to exploit opportunities to the full, with the management skill of a developer to head an adept team.</td>
<td>Developer - organisation goal seeker; risk accommodating</td>
</tr>
<tr>
<td>Support</td>
<td>Should be starved of unnecessary resources - resourcing only to reduce net costs and so needs the management skills of a caretaker</td>
<td>Caretaker - immediate and efficient risk avoiding</td>
</tr>
<tr>
<td>Factory</td>
<td>Needs the care of a controller to milk applications for their possible benefits by well-judged enhancements. Resourcing should increase the quality of applications but not cause any business</td>
<td>Controller - long-term and quality solutions; risk reducing</td>
</tr>
<tr>
<td>Segment</td>
<td>Managerial style</td>
<td>Behavioural style</td>
</tr>
<tr>
<td>---------</td>
<td>------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Turnaround</td>
<td>Associated with uncertainty and so needs the risk handling skills of an entrepreneur to push for advances when required but willing to drop unsuitable developments.</td>
<td>Entrepreneur - personal achiever; risk taking</td>
</tr>
</tbody>
</table>

Conclusion

There are various methods used to try and match the Information Strategy in an organisation with its business objectives. The over-riding requirement is to be clear on what the business objectives are, and then to try and ensure that the information system provides the information to help the organisation meet those objectives.

3.7.3 Business objectives and IS/IT resources

The identification of business needs and the information technology framework to satisfy them is at the heart of a strategy for information systems and information technology. This is not always feasible, especially if an organisation's use of IS/IT has grown in a haphazard fashion. The purpose of the strategy in this situation may be to impose some sort of order on a disorganised situation.

The ability to use information and/or information systems to provide better quality information, or to facilitate more efficient processes and therefore establish competitive advantage, is referred to as information leadership.

We discussed critical success factors (CSFs) in the preparation of resource plans earlier in this Chapter - CSFs can translate business objectives into IS/IT objectives - they function as linking pins between IS/IT and business planning. The process is as follows.

(a) Define business objectives (eg raise earnings per share, develop new businesses).
(b) Identify the CSFs whose success is necessary for the organisation to flourish (eg new markets, new products, core activities).
(c) Develop the information systems to support the CSFs (eg develop customer information systems, improve the financial control reporting system).

3.7.4 Components of Long Range plans

The structure of the plan is:

(a) Executive summary - a statement containing the main points of the scheme. The document should have a section on the goals, specific and general, of information processing in the organisation.
(b) Goals - a general goal might be to provide a different customer service, whilst a specific goal could be to completely update the database enquiry system.
(c) Assumptions - the plan will be based on certain assumptions about the organisation and the current business strategy. It is essential that this plan is linked to the organisation's strategic plan.
(d) **Scenario** - sometimes it is helpful to draw up a scenario of the information-processing environment that will result from executing the plan.

(e) **Application areas** - the plan should outline and set priorities for new application areas being planned and for those applications which are in the process of development. A report on their progress and status should be produced. For major new applications there should be a breakdown of costs and schedules. The plan should outline and set priorities for the application areas. A corporate steering committee containing high-level representation should set the priorities as this committee can make the trade-offs among functional areas.

(f) **Operations** - the current systems will be continuing and the plan should identify the existing systems and the costs of maintaining them.

(g) **Maintenance** - the plan should incorporate the budget for the maintenance of, and enhancements to, the existing system. The resources required for maintenance and enhancement of existing applications should also be planned if the operation of existing systems is to continue.

(h) **Organisational structure** - the plan should describe the existing and future organisational structure for the technology, in terms of location, and human and financial resources.

(i) **Impact of the plan** - management is interested in the impact of a plan on the organisation, particularly its financial impact.

(h) **Implementation** - the plan should identify implementation risks and obstacles.

---

**Case Example**

**Components of Long Range plans**

*A sample strategic plan developed by Plan ware (http://www.planware.org/index.html)*

**Strategic Plan for AnyBiz Inc**

**Strengths, Weaknesses, Threats & Opportunities**

This strategic plan addresses the following key strengths, weaknesses, threats and opportunities for AnyBiz Inc:

<table>
<thead>
<tr>
<th><strong>Strengths:</strong></th>
<th><strong>Weaknesses:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• R and D almost complete</td>
<td>• Overdependent on borrowings - Insufficient cash resources</td>
</tr>
<tr>
<td>• Basis for strong management team</td>
<td>• Board of Directors is too narrow</td>
</tr>
<tr>
<td>• Key first major customer acquired</td>
<td>• Lack of awareness amongst prospective customers</td>
</tr>
<tr>
<td>• Initial product can evolve into range of offerings</td>
<td>• Need to relocate to larger premises</td>
</tr>
<tr>
<td>• Located near a major centre of excellence</td>
<td>• Absence of strong sales/marketing expertise</td>
</tr>
<tr>
<td>• Very focused management/staff</td>
<td>• Overdependence on few key staff</td>
</tr>
<tr>
<td>• Well-rounded and managed business</td>
<td>• Emerging new technologies may move market in new directions</td>
</tr>
<tr>
<td>Threats:</td>
<td>Opportunities:</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>• Major player may enter targeted market segment</td>
<td>• Market segment is poised for rapid growth</td>
</tr>
<tr>
<td>• New technology may make products obsolescent</td>
<td>• Export markets offer great potential</td>
</tr>
<tr>
<td>• Economic slowdown could reduce demand</td>
<td>• Distribution channels seeking new products</td>
</tr>
<tr>
<td>• Euro/Yen may move against $</td>
<td>• Scope to diversify into related market segments</td>
</tr>
<tr>
<td>• Market may become price sensitive</td>
<td></td>
</tr>
<tr>
<td>• Market segment's growth could attract major competition</td>
<td></td>
</tr>
</tbody>
</table>

**Vision**

The promoters' vision of AnyBiz Inc in 3-4 year's time is:

AnyBiz will be operating from a xxx sq. ft. unit near xxx Town. It will have annualized sales of $xxx and be profitable. It will employ xxx people mainly engaged in R and D, marketing, support and admin. AnyBiz will offer xxx core products and provide added-value services to a large customer base throughout the xxx market segments and in xxx countries overseas. AnyBiz's offerings will be technically advanced and offer many clear-cut advantages and improvements over competitors' possible offerings. AnyBiz will continue to expand through organic growth and acquisitions in related technology/market segments. It will have recently received mezzanine finance prior to a public offering.

**Mission Statement**

The central purpose and role of AnyBiz Inc is defined as:

AnyBiz designs, develops and markets advanced systems for specialist data capture and transaction processing management. These web-based systems work with specialist hardware supplied by major integrators. They are sold to small, medium and large-sized companies within the xxx industries for a range of specialist applications. AnyBiz's systems are distinguished from competition by their sophisticated interfaces, scalability and ease of modification and are extensively patented. Sales are made directly and through major distributors/OEMs in the home market and overseas.

**Corporate Values**

The corporate values governing AnyBiz Inc's development will include the following:

• AnyBiz operates in accordance with the highest standards in all relationships with customers, suppliers, environment and the community.

• AnyBiz fosters a climate which encourages innovation and diligence amongst staff and rewards accordingly.

**Business Objectives**

 Longer term business objectives of AnyBiz Inc are summarized as:

• To expand the business aggressively and offer above-average returns to shareholders.

• To become the leading, innovative systems company within the xx market segments.

**Key Strategies**

The following critical strategies will be pursued by AnyBiz Inc:

1. Accelerate product launches by strengthening R and D team
2. Extend links with key technology centres
3. Raise additional venture capital
4. Expand senior management team in sales/marketing
5. Recruit non-executive directors
6. Strengthen human resources function and introduce share options for staff
7. Appoint advisers for intellectual property and finance
8. Seek new market segments/applications for products

The following important strategies will also be followed:

1. Locate new premises adjacent to xxx
2. Commission assessments of key markets
3. Start participating in trade shows and missions
4. Develop overseas market entry plans
5. Pursue strategic alliances with complementary players
6. Strengthen web presence and promote
7. Seek new market segments/applications for products

**Major Goals**

The following key targets will be achieved by AnyBiz Inc over the next 3-4 years:

- Achieve sales of $xx million by 200X
- Report annualized profits of $xx million in 200X
- Secure xx% of the xx market segment by 200X
- Become largest supplier of xxx systems in xx countries within xx years
- Undertake an IPO by 200X
- Employ xxx people including xx% technically qualified by 200X
- Have sales offices or agents in xx key markets before 200X

**Strategic Action Programs**

The following strategic action programs will be implemented:

1. CEO: Prepare comprehensive business plan and develop contacts to raise VC within 6-9 months.
2. CFO: Recruit Marketing Director and other key staff for marketing/sales and HR Director within 3-4 months.
3. Technical Director: Review R and D resources and scope for technical alliances - expand with arrival of VC.
4. Board: Expand BOD to include further independent financial, technical and industrial expertise prior to seeking VC.
5. All: Develop and implement accelerated market entry and development plans.
Chapter roundup

- **Strategic planning** is the formulation, evaluation and selection of strategies for the purpose of preparing a long-term plan of action to attain objectives.

- Information systems strategy is an example of a functional/operational strategy, although it often has **strategic implications**.

- A **strategy for Information systems** and information technology is justified on the grounds that IS/IT:
  
  - Involves high costs
  - Is critical to the success of many organisations
  - Is now used as part of the commercial strategy in the battle for competitive advantage
  - Impacts on customer service
  - Affects all levels of management
  - Affects the way management information is created and presented
  - Requires effective management to obtain the maximum benefit
  - Involves many stakeholders inside and outside the organisation

- Organisations should develop an information systems plan that supports their overall business plan.

- There are two main methodologies for establishing the information requirements of organisation - **Enterprise Analysis** and **Critical Success Factors (CSFs)**.

- **Enterprise analysis** involves examining the entire organisation in terms of structure, processes, functions and data elements to identify the key elements and attributes of organisational data and information.

- **Critical success factors** are a small number of key operational goals vital to the success an organisation.
  
  - Organisations exist within an environment which influences their activities. The general environment consists of Political/legal, Economic, Social/cultural and Technological (PEST) factors.

- The identification of business needs and the information technology framework to satisfy them is at the heart of a strategy for information systems and information technology.

- Richard Nolan's stage hypothesis attempts to model the stages organisations go through in their use of IS/IT. A key lesson of the stage hypothesis is that an organisation's use of IS/IT must be planned and managed.

- Porter and Millar state that IS/IT has the potential to change the nature of competition within an industry in three ways. IS/IT can:
  
  - Change the industry structure
  - Create new businesses and industries
  - Be used to create competitive advantage
• Porter’s five forces model can be used to analyse the effect of IS/IT on an industry. Porter identified five competitive forces operating in a competitive environment:
  o The threat of new entrants
  o The bargaining power of suppliers
  o The bargaining power of customers
  o The threat of substitute products/service
  o The existing competitive rivalry in the industry

• Porter proposes three generic strategies for achieving competitive advantage:
  o Cost leadership
  o Differentiation
  o Focus (either cost or differentiation)

• Michael Porter’s Value Chain models activities (inputs, process and add value to generate outputs for customers) and the relationships between them. The value chain can be used to design a competitive strategy.

• Ways in which IS/IT can be used for competitive advantage include:
  o Establishing entry barriers
  o Affecting the cost of switching operations
  o Differentiating products/services
  o Limiting access to distribution channels
  o Ensuring competitive pricing
  o Decreasing supply costs
  o Increasing cost efficiency
  o Using information as a product
  o Building closer relationships with supplies and customers

• The general management technique of SWOT analysis can be applied to the development of information systems strategy.

• Critical success factors (CSFs) function as linking pins between IS/IT and business planning. The process is as follows.

  **Step 1.** Define business objectives.

  **Step 2.** Identify the CSFs whose success is necessary for the organisation to flourish.

  **Step 3.** Develop the information systems to support the CSFs.

### Practice Questions

**Q no. 1)** Why do companies develop IT Strategic Plans? In your own words describe at least 3 reasons why a company might develop an IT strategic plan.

**Q no. 2)** Identify at least 4 possible requirements from customers that might impact an IT Strategic Plan and describe the implications.

**Q. no 3)** Rate the following examples in terms of risk where L is Low, M is medium and H is high

   i) a small manufacturer using a financial package to record their financial transactions from paper records
   
   ii) a large but conservative bank using commercial packages that are readily available with minimal modification
iii) a medium sized bank with in-house developed system which are regularly changed to ensure that the bank stays ahead of the competition

**Q no. 4)** “All organisations should prepare their IT Strategic Plans for a period of 3-5 years and review their long term plans regularly”.

**In your opinion, should the horizon or period for a Strategic Plan be the same for all organisations?**

**Should the review period be defined the same for all organisations? Would the IT Strategic Planning time frame differ for organisations in different industries? Give examples to highlight your views.**

**Solution Hint:**

**Answer to Question No. 1**

Students need to have an understanding of the purpose behind an IT Strategic Plan. Suggested solution should include some of the following reasons:

- Effective management of a costly but essential part of the organisation
- Improving communication between the business and the IT departments in an organisation
- Ensuring that the business direction can be supported and is linked with the IT direction
- Planning the priorities of IT to work with those of the organisation
- Provide a framework for effective resource management
- Provide a focus on what IT does so that costs and benefits are recognised.

**Answer to Question No. 2**

Answers will vary for this question. There are many things that customers might require or need within the current business environment that would impact on the IT Strategic Plan. Students should be able to demonstrate an understanding of how customer needs might be reflected in the Plan. Answers could include:

- Credit card processing. Customers wanting to use credit cards will mean that the organisation will have to look at online verification with credit card providers or alternate providers. Changes will need to be made for database access, new external partnerships and networking capabilities etc.
- Improved lead times. This might necessitate a review of the current ordering systems and/or inventory systems and plans to upgrade systems, acquire or redevelop.
- Ability to provide electronic documentation (e.g. CD-ROM). This might mean the purchasing of new equipment to provide CD-ROMs, and systems to control publishing and distribution.
- Bar-coding. Introducing bar coding into a company needs careful planning. It can impact right across the organisation and supply chain – new printers, bar-code readers, systems to work with the codes etc.
- Ability to handle special orders and requests. This sort of requirement (improvements to existing processes) could mean upgrades to systems, investigations into new systems or review of ordering process and resources.
- Ability to interface with distributors of customers and affiliates. This could mean allowing for further investigation into the requirements to see how widespread the need is and assess the sort of changes that might need to be made to existing systems.
Answer to Question No. 3

i) L

ii) M

iii) H

Answer to Question No. 4
The student’s answers will very a great deal. The question seeks to explore the student’s understanding of how the IT Strategic Planning process differs across organisations of different sizes and in different industries.

The answer should emphasise that IT Strategic Planning will differ across industries and that every organisations will need to determine what is an appropriate time frame for the planning and review process.

- A small company will usually have a less formal process for IT Strategic Planning.
- The position of IT within the company structure will impact on how IT is viewed and how it rates as a strategic consideration.
- Young companies will usually be less structured in their planning and focus on short term issues as they struggle to survive.
- Business planning is key to smaller companies as they seek to establish their business credentials.
- Industries can affect the time frame for planning. An organisation in a more traditional sector such as agriculture may have a longer time frame for strategic planning than an industry in a more contemporary industry such as electronics.
- Consider those companies in industries that have been spawned as a direct result of technology such as electronic commerce. With the rapid pace of change and new developments and trends almost daily, a company in this industry would need to almost constantly revise its IT Strategic Plan.

Exam Type Case Study I

Nasar (Pvt) Ltd

Nasar (Pvt) Ltd are a large manufacturing company, who have developed computer systems over a number of years in response to business demands. The Managing Director believes that they need to develop an information systems and information technology strategy in order to address the long term objectives of the organisation.

Evaluate the case for Nasar (Pvt) Ltd developing a strategy for information systems and information technology.
The case for developing a strategy for information systems and information technology

Computers have come to dominate the world of business over the past forty years but not more so than in the last decade when the introduction of the microcomputer led to most businesses having access to information technology. However there has been a growing recognition that organisations must plan their adoption of IT carefully and fit it to their business needs. IT can bring competitive advantage to an organisation if the development of their information systems corresponds with their information requirements and business strategy. A company strategy is a statement of their long term objectives for the business and the way they will be achieved. Planning a strategy is not done over night and must be done cautiously. Companies need a strategy where decisions have a major impact on the long-term future of the organisation.

A company such as Nasar (Pvt) Ltd will benefit from having an information systems strategy (IS) and an information technology strategy (IT) for a number of reasons. First Nasar (Pvt) Ltd have been developing information systems for a number of years and are continually investing large amounts of money in IT. Some people within the organisation may argue that the money has not always been spent wisely. The company needs to focus on how much money they will spend on IS and IT in the future and how well the funds are spent.

There is a growing trend towards end-user computing within the company and a growing number of staff are wanting access to computers for CAD (computer-aided design), business modelling using spreadsheets etc. There have even been discussions about CIM (Computer Integrated Manufacturing). All of this costs money and in the case of CIM, millions of pounds maybe spent.

Even with the introduction of the new technology the business may not feel the benefit until the users have been trained on the various systems.

Information systems and information technology have become critical to the operation of the business in Nasar (Pvt) Ltd. The Sales Department could not function without the on-line order processing system. On the factory floor the information system is crucial to their current operations. The company relies heavily on its telecommunications links with suppliers and customers.

The company need IS and IT to give them a strategic advantage over rivals in the market. IT can be used within Nasar (Pvt) Ltd to improve productivity and the quality of services offered. For example moving to JIT (Just-in-time) or CIM the company can couple various sub-systems within the organisation to cut down on stock holdings and increase productivity.

Management and organisational structures can be changed by moving to electronic mail, teleconferencing or even telecommuting. IT can be used to access previously inaccessible markets abroad.

IT can completely revolutionise business practices and whole industries e.g. banking with their ATMs (automated teller machines) and electronic funds transfer; retail businesses with their POS (point of sales systems) and bar-coding. IT can be both the cause of major changes in doing business and a response to them.
IT now affects every aspect of business life in large organisations and will continue to do so well into the 21st century. Everyone in business will have access to IT and use IT in their working life. IT is no longer a centralised resource.

Well-designed information systems can now provide high quality management information. This will lead to decision support and executive information of the highest level.

IT and IS involves many different stakeholders within an organisation such as Nasar (Pvt) Ltd and external to the company. People who would be interested in the IS and IT of Nasar (Pvt) Ltd might be:

- Other businesses;
- IT manufacturers;
- Consumers;
- Employees and internal users - how IT affects working practices.

Any strategic plans involving IS/IT must consider technical issues. Compatibility of future systems with those already present is a major issue.

Finally the success of any implementation of IS or IT can be influenced by the management. It is essential that they are educated in IS and IT in order that they can make the right decisions in relation to design and development of the business systems.

IS and IT is such a large aspect of business at Nasar (Pvt) Ltd to require proper planning and management. IS and IT issues cannot be tackled simply and all implications need to be thought out in advance. Hence there is a need for an IS/IT strategy.

**Exam Type Case Study II**

**X Ltd**

X Ltd's directors are concerned that there is evidence of a declining trend in the sale of its lawnmowers and associated equipment. As the sale of equipment for estate maintenance is considered to be insufficiently rewarding, the marketing of an electrically-propelled baby carriage (pram) is being considered. None of the four firms making prams offers such a vehicle. Three of the firms are subsidiaries of the same international conglomerate. The other firm (K Ltd) has carved out its own up-market niche as a one-product company. Its cost structure, disclosed in accounts filed with the Department of Trade and Industry, is as follows:

<table>
<thead>
<tr>
<th>% of turnover</th>
<th>2000</th>
<th>2001</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost of sales</td>
<td>85.4</td>
<td>85.2</td>
</tr>
<tr>
<td>Distribution costs</td>
<td>7.4</td>
<td>7.8</td>
</tr>
<tr>
<td>Administration costs</td>
<td>3.8</td>
<td>4.0</td>
</tr>
<tr>
<td>Operating profit</td>
<td>3.4</td>
<td>3.0</td>
</tr>
<tr>
<td>Labour (and associated) costs</td>
<td>11.5</td>
<td>11.7</td>
</tr>
<tr>
<td>Depreciation</td>
<td>0.7</td>
<td>0.5</td>
</tr>
</tbody>
</table>

It is believed that K Ltd's production overheads are approximately twice its labour (and associated) costs.
Relevant official statistics are available as follows.

<table>
<thead>
<tr>
<th>UK live births</th>
<th>UK pram sales (non-collapsible)</th>
<th>England and Wales median months’ marriage to first live birth</th>
</tr>
</thead>
<tbody>
<tr>
<td>'000 pa</td>
<td>£m</td>
<td>Professionals**</td>
</tr>
<tr>
<td>1981-1991736</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1982</td>
<td>719</td>
<td>1982</td>
</tr>
<tr>
<td>1984</td>
<td>730</td>
<td>1984</td>
</tr>
<tr>
<td>1985</td>
<td>751</td>
<td>1985</td>
</tr>
<tr>
<td>1986</td>
<td>755</td>
<td>1986</td>
</tr>
<tr>
<td>1993-2001</td>
<td>764*</td>
<td></td>
</tr>
<tr>
<td>2001-2010</td>
<td>808*</td>
<td></td>
</tr>
</tbody>
</table>

* projections
** class of father

X Ltd believes that an assisted vehicle could appeal to many families as a status symbol.

A selling price of £500 + VAT is proposed, half of which will represent the retailer's margin.

X Ltd's actual and projected turnover figures are as follows:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>£'000</td>
<td>£'000</td>
<td>£'000</td>
<td>£'000</td>
<td>£'000</td>
<td>£'000</td>
</tr>
<tr>
<td>Lawn mowers</td>
<td>750</td>
<td>650</td>
<td>600</td>
<td>500</td>
<td>350</td>
</tr>
<tr>
<td>Shopping trolleys</td>
<td>150</td>
<td>175</td>
<td>200</td>
<td>250</td>
<td>325</td>
</tr>
<tr>
<td>Hospital trolleys</td>
<td>850</td>
<td>860</td>
<td>875</td>
<td>900</td>
<td>950</td>
</tr>
<tr>
<td>Industrial trucks</td>
<td>50</td>
<td>75</td>
<td>80</td>
<td>90</td>
<td>95</td>
</tr>
<tr>
<td>Prams</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>10</td>
<td>50</td>
</tr>
<tr>
<td>_____</td>
<td>_____</td>
<td>_____</td>
<td>_____</td>
<td>_____</td>
<td>_____</td>
</tr>
<tr>
<td>1,800</td>
<td>1,760</td>
<td>1,755</td>
<td>1,750</td>
<td>1,770</td>
<td></td>
</tr>
<tr>
<td>_____</td>
<td>_____</td>
<td>_____</td>
<td>_____</td>
<td>_____</td>
<td></td>
</tr>
</tbody>
</table>

Required

(a) Advise X Ltd, in the context of the above information and specifying what other information you would regard as appropriate, whether or not the proposed strategic development should be further investigated, explaining how information costs affect your recommendation. (15 marks)

(b) Explain the methods by which the attributes required of the proposed product and the attitudes of prospective purchasers can be measured. (5 marks)

(Total: 20 marks)
X Ltd

(a) X Ltd's directors are concerned that there is evidence of a declining trend in the sale of its lawn mowers and associated equipment. The organisation is considering the marketing of an electrically propelled pram.

In order to decide whether this proposed strategy should be taken any further, it is recommended that additional information be obtained in order to reduce the uncertainty. It is believed the following information should be obtained.

(i) The first step should be objective, systematic research into market opportunities - what are potential competitors' activities and plans? How big is the market sector? What percentage of the market will X Ltd be able to gain?

(ii) What is the economic climate forecast and how will this affect disposable income?

(iii) The 1986 sales figures for non-collapsible prams are the lowest since 1982, yet since 1982 there has been an increase in live births. This may be explained by such factors as the birth of second/third children and the increase in sales of collapsible prams. Further investigation is therefore required into the decline in sales.

(iv) An assumption has been made that the target market is the more affluent population, if the selling price is £500+ VAT. Does the lifestyle of this population fit in with a non-collapsible pram, or are they looking for a model, which can be put into a car, thus allowing more flexibility and mobility? A market research study of potential customers should be carried out to ascertain whether there is a want/need for this product.

(v) A detailed breakdown should be obtained of the costs relating to the R&D required for the pram, labour, distribution, marketing, guarantees and after-sales service.

(vi) The profit margins associated with each product should be compared to the pram. Will the pram produce enough profit to justify the investment involved?

(vii) X Ltd's costs and pricing strategy for all of its products should be reviewed in detail to ascertain if the organisation is working as effectively and efficiently as possible.

Until the above information has been collected and analysed it is difficult to recommend the pram strategy. Management must determine the value of information and seek a balance between the cost of gathering information and the quality of decisions made on the basis of the information gathered.

(b) The attributes of the proposed product could be ascertained by:

(i) A 'pilot study' covering a sample of the prospective consumer group. This study could consist of group interviews, or in-depth interviews, which would identify the attributes of and attitudes towards the proposed product.

(ii) A 'placement test', where the proposed product is issued to a representative sample of users. The recipients note their reactions to and opinions on the product, suggesting modifications where appropriate.

(iii) Questionnaires completed by retailers to identify what customers are looking for in conventional prams. This would be relevant where features of conventional prams and the proposed products are the same, eg. colour and interior padding.
From the results of the above, X Ltd may then decide to carry out a test marketing study. The study would cover a small area where the targeted customer lives. Results of the marketing and sales activities could then be projected for the total forecasted market.

The results of the above surveys can be analysed by various statistical methods, such as factor analysis. This method would allow X Ltd to establish the underlying pattern of dimensions and bring about certain relationships between groups of measurement.

**Exam Type Case Study III**

You are the finance function representative on a project team charged with carrying out a cost benefit analysis on a proposed on-line order entry system. It is envisaged that the system will involve field sales staff using portable computers and communications links to enter data into a central computer system.

(a) What factors would you expect to take into account under each of the following headings?

(i) The cost of developing, installing and operating the system;
(ii) The benefits which might result from the introduction of the new computer application.

(b) What techniques would you make use of to establish the potential profitability (or otherwise) of your proposed new system?

**Suggested Answer case study III**

(a) **Costs and benefits**

(i) **Costs of development**

The costs associated with producing the system can be divided into three categories - the building of the system, its initial implementation, and ongoing running costs.

**Building the system**

- **Costs of personnel**: various people will have to be co-opted onto a project team. Each member of staff in the project team will have to dedicate time to the investigation. Their salary costs and expenses are a major part of the development costs. The project team will contain representatives of each interested group - sales management, one or more members of the sales force, marketing, the finance function, the sales office, the systems analyst, the person currently responsible for the entry of orders, etc. There will also be personnel costs of the people who will be developing the system - the analyst, programmers, operating staff, salesmen. A 'wastage' factor must be built into these costs to cover eventualities such as illness and holidays.

- **Extra personnel**: some people with expertise in the kind of system being adopted may need to be hired, or consultants used.

- **Software costs**: the computer programs to run the system will have to be acquired. Some software may be produced in house, and some may be purchased from outside. If software is purchased, it is likely to need tailoring to fit the precise needs of the organisation. Bought-in software must be licensed. Software requirements will include the order entry programs and communications software. The computer time on the existing machines that will be used for development will need to be paid for.
• **Hardware costs:** a great deal of hardware will need to be acquired (purchased, leased or hired). This will include portable computers for the sales force, communications equipment, and possibly a mini-computer or large micro-computer to act as a front end processor, linking the sales order system to the main computer. Costs to be considered are not only the purchase prices of the machinery, but also the cost of financing the capital expenditure.

• **System investigation:** in order to define what is needed from the system in question, an investigation is needed. Information is gathered by the systems analysts using interviews, questionnaires and observation. Various documents will need to be printed, and the time of interviewees and interviewer will cost money.

### Implementing the system

• **Printing costs:** various manuals, training materials and stationery required for the operation of the system will need to be printed.

• **Training:** both sales staff and operations staff must be trained in the operation of the system. The training costs and the cost of lost time for trainees must be included in a cost-benefit analysis.

• **Changeover costs:** the changeover from the old system may involve parallel running - where both old system and new run concurrently - until the system has been proven. This will lead to a temporary doubling of staff requirements. The system is not likely to be adopted for the whole company simultaneously, a safer way of implementation is to phase in a region or sales force at a time. This implies that the old system and the new will run together for some time.

• **Redundancy costs:** some existing staff may lose their jobs. They will need to be paid redundancy money, and facilities provided to help them get new jobs.

• **Security costs:** allowing external access to the company's computer system has many implications for security. Procedures will have to be set up to make sure that no unauthorised person can 'hack' into the machine.

• **Dysfunctional behaviour:** this is behaviour where employees work against the interests and objectives of the organisation because they are antagonistic to the new system. Procedures and schemes to encourage the sales force to be positive towards the new scheme must be adopted. Any such schemes are likely to cost money but are extremely important.

### Ongoing costs

• **Maintenance costs:** all hardware and software will need to be maintained. Typical external maintenance costs are 12% of the initial purchase price per annum. Because the system will be so vital to the success of the business, it is essential to ensure that any down time is minimised. In order to ensure that no sales person is without a machine, there will need to be 'redundant' machines available for immediate replacement of any that go wrong or are damaged by the rough treatment that they are likely to receive. Hardware must be replaced as it becomes worn out.

• **External running costs:** there is likely to be lease or rental costs for hardware and communications equipment. There may also be annual software license fees. Telephone costs will be incurred each time a sales person accesses the main computer system. Upgrades to hardware and software may be required as they become available.

• **Help desk:** because the sales force will be relatively unskilled at using computers, personnel should be available to answer queries and solve problems.

• **Control mechanisms:** systems must be in place to ensure that the sales orders are being processed correctly. Security must be tight to prevent unauthorised access. Access
must be prevented not only from non employees but from people who leave the company after the system has been set up.

(ii) Benefits from developing the system

It is more difficult to quantify the likely benefits from a system than it is to quantify costs, but it is important to do so as accurately as possible. Benefit may be quantified by comparing the increase (or avoided decrease) in market share due to the new system.

The benefits are likely to include:

- **Reduced labour costs:** a complete series of processes, filling out order forms and sending them to head office, will be eliminated.

- **Increased accuracy:** because the sales person recording the sales will be familiar with the customer, there are likely to be less errors provided that the sales person has been properly trained.

- **Improved cash flow:** the process of recording sales is speeded up. This will mean that the money will be received quicker and the company's cash flow improved.

- **Better customer service:** the customer will receive goods quicker. On-line access to the main computer will avoid the taking of orders which cannot be satisfied because stock levels are too low. Customer satisfaction will be improved by the elimination of promises that cannot be kept being made.

- **On-line credit reference:** before a new customer is accepted, a credit reference must be available. A credit reference database can be accessed on line, and the customer order can be taken (or refused) without delay.

- **Improved communication:** other uses can be made of the portable computers. An electronic messaging system can be used to communicate with sales persons, and sales leads can be transmitted directly without delay.

- **Computerised customer record cards:** among the other systems that would be possible once the customer order system is adopted is a computerised record card system. This would record details of existing customers, potential customers and indirect customers (those supplied through distributors).

- **Improved information:** information would be available faster, which would improve the quality of decision making. Other information can be made available that would not be possible under the old system because of time factors. The sales person can be made aware, for example, of major traffic hold ups on his or her likely route.

(b) Cost-benefit techniques

Once all costs and benefits have been evaluated, it is then possible to carry out a cost-benefit analysis that will assess if the investment in the new system is justified. A cash flow analysis will be prepared. Once it has been established that the project will yield a positive cash flow the project's payback can be examined and compared with that of competing projects. Some techniques for comparing paybacks are:

- **Payback period:** this measures the length of time that a project will take to break even. The shorter the payback period the better. This minimises the risks of unforeseen eventualities.

- **Return on Investment (ROI) and Return on Capital Employed (ROCE):** these evaluate the investment in terms of a percentage return per year. The calculation of these
indices is fairly simple, and the investment with the higher percentage will be the preferred option.

- **Discounted cash flow**: inflation and the cost of borrowing mean that it is better to receive money now than in a year's time. A technique that takes into account when money will be generated as well as how much is discounted cash flow. The value of an investment can be estimated using such measures as Internal Rate of Return (IRR), and Net Present Value (NPV). In order to evaluate these, it is necessary to know the cost of capital for the firm.

- **Risk analysis**: the returns from the system are not certain, there is a risk associated with each category of benefit. By assigning a probability to different levels of return, the accountant can calculate the expected value of the return.
4 Internet & E-Commerce

<table>
<thead>
<tr>
<th>Topic List</th>
<th>Syllabus Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1 The Internet- An Overview</td>
<td>1.1</td>
</tr>
<tr>
<td>3.2 Encryption and other safety measures</td>
<td>1.1</td>
</tr>
<tr>
<td>3.3 Electronic Commerce</td>
<td>1.2</td>
</tr>
<tr>
<td>3.4 Globalisation</td>
<td>1.1</td>
</tr>
<tr>
<td>3.5 E-Business Models</td>
<td>1.1</td>
</tr>
<tr>
<td>3.6 Electronic Payment Systems</td>
<td>1.1</td>
</tr>
</tbody>
</table>

Introduction

The Internet is potentially the most significant business and social development since the advent of the telephone. As with any new technology the Internet provides both opportunities and risks. In this chapter we look at how the Internet can be exploited to provide enhanced value to businesses and their customers. We also cover the security Issues associated with e-commerce along with discussion on E business Models. The Internet is a 'hot topic' in both the academic and business worlds - so ensure you understand the issues raised in this chapter.

Study Guide

E Business (1.1)

- It is timely for the students to revise the concept and meaning of e-business. You might wish to lead a discussion on what is e-business before commencing this section to ensure that the students have a sufficiently broad definition.

E-Business Models (1.1)

- You might want to demonstrate some websites that demonstrate some of these models or ask the students to share their experiences.
- Business to Consumer (B2C)
- Business to Business (B2B): Lead discussion about the emergence of this model. Discuss some of the possible benefits that B2B offers.
- Business to Employee (B2E)
- Consumer to Consumer (C2C): This is an interesting model to discuss as it has also introduced new business types
- Government to Citizen (G2C): Many governments have a strategy to deliver online services and information. You might want to lead a discussion about the issues of inequity and access that this introduces into societies.

Electronic Payment Systems (1.1)

- Lead a discussion on electronic payment systems.

EDI and Electronic Commerce (1.2)

- Lead a discussion about EDI. There may be logical industry examples that you can quote.
- Ensure that the students understand the difference between EDI and other forms of ecommerce
4. **INTERNET & E-COMMERCE**

4.1 **THE INTERNET- AN OVERVIEW**

**KEY TERMS**

The **Internet** (an abbreviation for International Network) is a global computer network connecting governments, companies, universities and many other networks and users. It is a voluntary, and almost unregulated, collection of hardware and software owned by private individuals and organisations.

The **World Wide Web (WWW)** is a system of Internet servers that support specially formatted documents. Most documents on the web are formatted in HTML (HyperText Markup Language) that supports links to other documents, as well as graphics, audio, and video files.

A group of documents accessed from the same base web address is known as a **website**.

The origins of the Internet lie in the research and development network ARPANET, established in 1969 by the US Department of Defense. ARPANET’s objectives were to facilitate the sharing of research findings and resources between government (particularly defence) scientists and researchers, and academic researchers in the universities, via email. During the early years of this network, other academic institutions were also sharing research resources via the Joint Academic Network (JANET). With the growth of the home PC market through the 1990’s and the advances in Telecommunications technology over the same period, universal access to these vast networks was inevitable. With the creation of the World Wide Web to aid navigation across the networks, that access became possible, and not only researchers and information seekers were able to use them; providers of telecommunications products, commercial services, leisure products and their customers quickly found that this infrastructure could be exploited easily, profitably and enjoyably.

<table>
<thead>
<tr>
<th>URL element</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>http://</strong></td>
<td>'http' tells the browser to use the Hypertext Transfer Protocol when retrieving the document from the Internet server. The two forward slashes after the colon introduce a 'host name' such as <strong>www</strong>.</td>
</tr>
<tr>
<td><strong>www</strong></td>
<td>This stands for <strong>World Wide Web</strong>. As noted before, to put it simply the web (via its use of HTML), is what makes the Internet user-friendly.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>URL element</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bbc</td>
<td>This is the domain name of the organisation or individual whose site is located at this URL</td>
</tr>
<tr>
<td>Co</td>
<td>CO This indicates the type of organisation concerned, in this case a company, Other designations include: .corn Commercial .ac or.edu Educational and research</td>
</tr>
</tbody>
</table>
The Internet provides opportunities to automate tasks which would previously have required more costly interaction with the organisation. These have often been called low-touch or zero-touch approaches. Tasks which a website may automate include:

(a) **Frequently-Asked Questions (FAQs)**: carefully-structured sets of answers can deal with many customer interactions.

(b) **Status checking**: major service enquiries (Where is my order? When will the engineer arrive? What is my bank balance?) can also be automated, replacing high-cost human service processes, and also providing the opportunity to proactively offer better service and new services.

(c) **Keyword search**: the ability to search provides web users with opportunities to find information in large and complex websites.

(d) **Wizards (interview style interface) and intelligent algorithms**: these can help diagnosis, which is one of the major elements of service support.

(e) **E-mail and systems to route and track inbound e-mail**: the ability to route and/or to provide automatic responses will enable organisations to deal with high volumes of e-mail from actual and potential customers.

(f) **Bulletin boards**: these enable customers to interact with each other, thus facilitating self-activated customer service and also the opportunity for product/service referral-Cisco in particular has created communities of Cisco users who help each other – thus reducing the service costs for Cisco itself.

(g) **Call-back buttons**: these enable customers to speak to someone in order to deal with and resolve a problem; the more sophisticated systems allow the call-centre operator to know which web pages the users were consulting at the time.

(h) **Transaction processing**: the taking of orders and payment on-line.

### 4.1.1 Problems with the Internet

The major risks that concern businesses and customers who are thinking of using the Internet for transactions are as follows:

(a) The high cost of establishing security and encryption procedures to protect confidential information and customer credit card or bank details from deliberate misuse by third parties.

(b) The lack of a paper-based audit trail for transactions.

(c) The possibility of misuse of customer bank details by an unscrupulous trader.
Although these risks are significant, they are reducing as more companies market E-business software that is specially designed for conducting business on the Internet.

The lack of security on the Internet is generally perceived as the greatest current threat. Security affects companies in two ways:

- the security of information eg, the ability of outsiders to hack into a company's system or for a virus to be imported; and

- the security of sensitive data and transactions over the Internet, which is crucial if it is to become a principal medium for marketing and sales.

Speed is a major issue. Data only downloads onto the user's PC at the speed of the slowest telecommunications link - downloading data can be a time-consuming procedure. However, future developments will mean that speeds will improve. A number of faster services have recently become available, but cost is preventing widespread installation of these technologies by consumers.

a. **Integrated Services Digital Network (ISDN)** is an international communication standard for sending voice, video, and data over digital telephone lines or normal telephone wires. ISDN supports data transfer rates three times faster than modem?

b. **ADSL** (Asymmetric Digital Subscriber Line) is offers data transfer rates of up to 8 Mbps, considerably faster than ISDN. ADSL allows information to be sent out over ordinary copper wires and simultaneous use of the normal telephone service.

So much information and entertainment is available that employers worry that their staff will spend too much time browsing through non-work-related sites. **Security** is perhaps the biggest worry of all; this is covered in the next section.

### 4.1.2 INTERNET SECURITY ISSUES

Establishing organisational links to the Internet brings numerous security risks.

a. Corruptions such as **viruses** on a single computer can spread through the network to all of the organisation's computers. (Viruses are described at greater length later in this chapter.)

Disaffected employees have much greater potential to do **deliberate damage** to valuable corporate data or systems because the network could give them access to parts of the system that they are not really authorised to use.

If the organisation is linked to an external network, persons outside the company (**hackers**) may be able to get into the company's internal network, either to steal data or to damage the system.

Systems can have **firewalls** to prevent unauthorised access into company systems. Firewalls are used to prevent Internet users from accessing private networks connected to the Internet, especially intranets. All communications entering or leaving the intranet pass through the firewall, which blocks those that do not meet the specified security criteria.

Employees may **download inaccurate information** or imperfect or **virus-ridden software** from an external network. For example 'beta' versions of forthcoming new editions of many major packages are often available on the Internet. Beta versions are not fully tested and may contain bugs that could disrupt an entire system.

Information transmitted from one part of an organisation to another may be **intercepted**. Data can be 'encrypted' (scrambled) in an attempt to make it unintelligible to eavesdroppers. (See below.)
The communications link itself may break down. The worldwide telecommunications infrastructure is improving thanks to the use of new technologies, and there are communications 'protocols' governing the format of data and signals transferred.

### 4.1.3 Hacking

Hacking involves attempting to gain unauthorised access to a computer system, usually through telecommunications links. Hackers require only limited programming knowledge to cause large amounts of damage. The fact that billions of bits of information can be transmitted in bulk over the public telephone network has made it hard to trace individual hackers, who can therefore make repeated attempts to invade systems. Hackers, in the past, have mainly been concerned to copy information, but a recent trend has been their desire to corrupt it. Phone numbers and passwords can be guessed by hackers using electronic phone directories or number generators and by software which enables rapid guessing using hundreds of permutations per minute. Default passwords are also available on some electronic bulletin boards and sophisticated hackers could even try to 'tap' messages being transmitted along phone wires (the number actually dialled will not be scrambled).
**4.1.4 Viruses**

**KEY TERMS**

A virus is a piece of software which infects programs and data and possibly damages them, and which replicates itself.

Viruses need an opportunity to spread. The programmers of viruses therefore place viruses in the kind of software which is most likely to be copied. This includes:

a. **Free software** (for example from the Internet).

b. **Pirated software** (cheaper than original versions).

c. **Games software** (wide appeal).

d. **E-mail attachments** (often with instructions to send the message on to others).

1. **Types of viruses**

I. **Boot viruses:**

These viruses infect floppy disk boot records or master boot records in hard disks. They replace the boot record program (which is responsible for loading the operating system in memory) copying it elsewhere on the disk or overwriting it. Boot viruses load into memory if the computer tries to read the disk while it is booting.

Examples: Form, Disk Killer, Michelangelo, and Stone virus

II. **Program viruses:**

These infect executable program files, such as those with extensions like .BIN, .COM, .EXE, .OVL, .DRV (driver) and .SYS (device driver). These programs are loaded in memory during execution, taking the virus with them. The virus becomes active in memory, making copies of itself and infecting files on disk.

Examples: Sunday, Cascade

III. **Multipartite viruses:**

A hybrid of Boot and Program viruses. They infect program files and when the infected program is executed, these viruses infect the boot record. When you boot the computer next time the virus from the boot record loads in memory and then starts infecting other program files on disk.

Examples: Invader, Flip, and Tequila

IV. **Stealth viruses:**

These viruses use certain techniques to avoid detection. They may either redirect the disk head to read another sector instead of the one in which they reside or they may alter the reading of the infected file’s size shown in the directory listing. For instance, the Whale virus adds 9216 bytes to an infected file; then the virus subtracts the same number of bytes (9216) from the size given in the directory.

Examples: Frodo, Joshi, Whale

V. **Polymorphic viruses:**
A virus that can encrypt its code in different ways so that it appears differently in each infection. These viruses are more difficult to detect.

Examples: Involuntary, Stimulate, Cascade, Phoenix, Evil, Proud, Virus 101

VI. Macro Viruses:
A macro virus is a new type of computer virus that infects the macros within a document or template. When you open a word processing or spreadsheet document, the macro virus is activated and it infects the Normal template (Normal.dot)—a general purpose file that stores default document formatting settings. Every document you open refers to the Normal template, and hence gets infected with the macro virus. Since this virus attaches itself to documents, the infection can spread if such documents are opened on other computers.

Examples: DMV, Nuclear, Word Concept.

VII. Active X
ActiveX and Java controls will soon be the scourge of computing. Most people do not know how to control their web browser to enable or disable the various functions like playing sound or video and so, by default, leave a nice big hole in the security by allowing applets free run into there machine. There has been a lot of commotion behind this and with the amount of power that JAVA imparts, things from the security angle seem a bit gloom.
These are just few broad categories. There are many more specialized types. But let us not go into that. We are here to learn to protect our self, not write a thesis on computer virus specification.

VIII. Worms
A computer worm is a self-contained program that is able to spread functional copies of itself or its segments to other computer systems. The replication of a worm virus usually takes place across network connections, email attachments or IRC (Internet Relay Chat). To get rid of a worm you just need to delete the program.

Example of a Worm virus is the 'WORM.LINONG.A' virus which spreads via network drives and Email. Similar to 'Melissa', this virus also propagated itself by E-mailing itself as an attachment to all recipients in the users address book. Although this virus did not have any destructive payloads, it sometimes performed some or all of the following: Resetting the default homepage in Internet Explorer, display a message on the users screen or create 600 new folders at the root of the users c:/ drive

IX. Trojans
A Trojan horse is a program that performs an unexpected or unauthorized, usually malicious, action such as displaying messages, erasing files or formatting a hard disk. A Trojan does not infect other files, thus cleaning is not necessary. To get rid of a Trojan, you can simply delete the program.

Example of Trojan virus was the 'MungaBunga' virus. This destructive Trojan, when triggered, modifies the root directory and formats the c:\ drive.

X. Hoax Viruses:
These are probably the most basic of all viruses, and do not rely on any special programming or scripting to cause disruption. A hoax virus generally consists of an Email message containing a warning about a new virus, and asks the users to forward on the message to as many people as they can. This consequently causes large amounts of Email traffic over the Internet, and ultimately results in the overload of Email servers.
4.2 Encryption and Other Safety Measures

4.2.1 Encryption

Encryption aims to ensure the security of data during transmission. It involves the translation of data into secret code. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text; encrypted data is referred to as cipher text.

**KEY TERM**

Encryption involves scrambling the data at one end of the line, transmitting the scrambling data, and unscrambling it at the receiver’s end of the line.

4.2.2 Authentication

Authentication is a technique of making sure that a message has come from an authorized sender. Authentication involves adding an extra field to a record, with the contents of this field derived from the remainder of the record by applying an algorithm that has previously been agreed between the senders and recipients of data.

4.2.3 Firewalls

Systems can have firewalls (which disable part of the telecoms technology) to prevent unwelcome intrusions into company systems, but a determined hacker may well be able to bypass even these.

4.2.4 Dial-back security

It operates by requiring the person wanting access to the network to dial into it and identify themselves first. The system then dials the person back on their authorized number before allowing them access. All attempted violations of security should be automatically logged and the log checked regularly. In a multi-user system, the terminal attempting the violation may be automatically disconnected.

4.2.5 Cryptography, keys and signatures

The parties involved in e-commerce need to have confidence that any communication sent gets to its target destination unchanged, and without being read by anyone else.

One way of providing electronic signatures is to make use of what is known as public key (or asymmetric) cryptography. Public key cryptography uses two keys - public and private. The private key is only known to its owner, and is used to scramble the data contained in a file.

The 'scrambled' data is the electronic signature, and can be checked against the original file using the public key of the person who signed it. This confirms that it could only have been signed by someone with access.
to the private key. If a third party altered the message, the fact that they had done so would be easily detectable.

An alternative is the use of encryption products which support key recovery, also known as key encapsulation. Such commercial encryption products can incorporate the public key of an agent known as a Key Recovery Agent (KRA). This allows the user to recover their (stored or communicated) data by approaching the KRA with an encrypted portion of the message. In both cases the KRA neither holds the user's private keys, nor has access to the plain text of their data.

**Case example**

**Sci/Tech Deadly virus warning**

Computer users across the world are on alert for a malicious virus that is due to strike on Monday. The virus, known as CIH, is capable of lurking in a computer until 26 April and then causing havoc to the data stored there. It is also called the Chernobyl virus because it is timed to go off on the anniversary of the Russian nuclear accident, one of technology's worst disasters. CIH is a potentially deadly virus for computers. As well as deleting files stored on the hard drive, it also attempts to corrupt the heart of any computer - the flash BIOS. This can cause complete loss of data, and possibly render the computer unusable.

**Risk to W95/W98 users**

Users of DOS, Windows, Windows NT or Macintosh users are not at risk from CIH. It only replicates and activates under Windows 95 and Windows 98. The virus is designed to hide from view by inserting itself into empty coding slots on a computer's software utilities. But most up-to-date anti-virus software will spot it. There are various free checking programs that can be downloaded from the Internet to scan a computer for the bug.

**Common virus**

The virus was first located in Taiwan in early June 1998 and then spread to the wider world. It has been among the 10 most common viruses for several months, spreading very quickly as it has been distributed through pirated software and the Internet. It is not widespread in Europe or the US, but very common on computers in Asia. CIH is a program, so it must be activated before it can take effect. "There would be no way of knowing that you had downloaded this virus and run it, it's completely invisible to the user," said virus expert Mikko Hypponen of software company DataFellows. The CIH virus is far more dangerous to individual computers than Melissa, the much-publicised macro bug that spread relatively benign problems far and wide on the Internet last month. Melissa was mainly spread by e-mail, and relied on people opening a document attached to e-mail messages.

*BBC News*

---

### 4.3 Electronic Commerce

**KEY TERM**

*Electronic commerce* means conducting business electronically via a communications link.
E-commerce means literally conducting business electronically via some form of communication link. E-commerce is not necessarily new; exchanging information via Electronic Data Interchange (EDI) has been available for a number of years, so e-commerce can be seen as an extension of this trend. The main different is e-commerce is now possible between any two parties with an Internet connection, rather than the specialised formatting and communication systems required with EDI.

The options for commencing e-commerce are:

- Building a bespoke system in-house, having purchased the appropriate hardware for a web-server etc.
- Purchasing a ready-made packaged e-commerce system and implementing this in-house, or
- Outsourcing the provision of e-commerce to a specialist third party.

### 4.3.1 Electronic Data Interchange (EDI)

EDI is a form of computer-to-computer data transfer. For instance instead of sending a customer a paper invoice through the post the data is sent over telecommunications links. This offers savings and benefits to organisations that use it.

a. It reduces the delays caused by postal paper chains.

b. It avoids the need to re-key data and therefore saves time and reduces errors.

c. It provides the opportunity to reduce administrative costs e.g. the costs associated 'the creation, recording and storage of paper documents.

d. It facilitates shorter lead times and reduced stock holdings which allow reduction working capital requirements, (e.g. Just-In-Time policies).

e. It provides the opportunity to improve customer service.

The general concept of having one computer talk directly to another might seem straightforward enough in principle, but difficulties may arise.

- Businesses hold records in computer files to their own file structure specifications. A translation mechanism may be required to allow transfer between the systems.

The problem of compatibility between different makes or types of computer was a serious one in the past; and some form of interface between the computers had to be devised to enable data interchange to take place.

Businesses often work to differing time schedules and time-zones. Organisations may conduct system maintenance late at night thinking this will not affect business. However, an overseas company in a different time zone, may need to access the system.

As the number of trading partners grows the number of one-to-one links eventually becomes unmanageable.

### 4.3.2 Opportunities over E-commerce and the web

Over the last few years, electronic commerce or e-commerce has increasingly been used to describe the use of the internet find websites in the sale of products or services. A simple definition is that 'e-commerce is the process of trading on the Internet'.

The Internet allows businesses to reach potentially millions of consumers worldwide and extends trading time to seven days, around the dock. Electronic commerce worldwide is valued at USS12 billion, and is set
to reach US$300-500 billion by 2002. The OECD forecasts global e-commerce to be worth $1 trillion by 2003-05. An e-business start-up has a considerable advantage over more established companies working in the same business area, because it does not have to take existing systems into account. This gives the start-up the ability and flexibility to launch new services far more quickly and cheaply than established rivals. For established companies e-commerce reduces expensive sales and distribution workforces and offers new marketing opportunities. Some of the facilities provided by e-commerce include:

1. **Distribution**

   The Internet can be used to get certain products directly into people's homes. Anything that can be convened into digital form can simply be uploaded onto the seller's site and then downloaded onto the customer's PC at home. The Internet thus offers huge opportunities to producers of text, graphics/video, and sound-based products. Much computer software is now distributed in this way.

2. **Electronic marketing**

   Besides its usefulness for tapping into worldwide information resources businesses are also using it to provide information about their own products and services. For customers the Internet offers a speedy and impersonal way of getting to know about the services that a company provides. For businesses the advantage is that it is much cheaper to provide the information in electronic form than it would be to employ staff to man the phones on an enquiry desk, and much more effective than sending out mail shots that people would either throw away or forget about when they needed the information.

   Companies will need to develop new means of promoting their wares through the medium of the Internet, as opposed to shop displays or motionless graphics. Websites can provide sound and movement and allow interactivity, so that the user can, say, drill down to obtain further information or watch a video of the product in use, or get a virtual reality experience of the product or service. For many companies this will involve a rethink of current promotional activity.

   E-marketing is particularly useful for any size of organisation because it:

   - Provides access to a global market-place
   - Provides a “level playing field” for marketing opportunities; even a small organisation can maintain a website which is viewable worldwide. Small organisations can therefore compete with larger ones without incurring the cost of setting up sales departments in many different countries.
   - Setting up and maintaining an Internet site is relatively cheap
   - Brand awareness can be increased by appropriate use of Internet advertising and production of corporate web sites.

   E-marketing can also be expanded to allow suppliers to access in-house systems and manage inventory levels, in effect providing e-marketing opportunities for suppliers. The use of Extranets in this way is described in the next section.
Peapod.com is an online supermarket and one of the more sophisticated recorders and users of customers' personal data and shopping behaviour. With over 200,000 customers in various US cities, Peapod's website sells groceries that are then delivered to customer's homes- a list of previous purchases (including brand, pack size and quantity purchased) is kept on the site, so the customer can make minor changes from week to week, saving time and effort.

Peapod creates a database on each shopper that includes their purchase history (what they bought), their online shopping patterns (how they bought it), questionnaires about their attitudes and opinions, and demographic data (which Peapod buys from third parties). A shopper's profile is used by the company to determine which advertisement to show and which promotions/electronic coupons to offer.

Demographically identical neighbours are thus treated differently based on what Peapod has learned about their preferences and behaviours over time.

Shoppers seem to like this high-tech relationship marketing, with 94% of all sales coming from repeat customers. Manufacturers like it too, the more detailed customer information enables them to target promotions at customers who have repeatedly bought another brand, thereby not giving away promotion dollars to loyal customers.

3. Collecting information about customers

People who visit a site for the first time may be asked to register, which typically involves giving a name, physical address and post code, e-mail address and possibly other demographic data such as age, job title and income bracket.

When customers come to, the site on subsequent occasions they either type their (self-chosen) username and password or more usually now, if they are using the same computer; the website recognises them using a cookie, which is a small and harmless file containing a string of characters [that uniquely identify the computer.

From the initial registration details the user record may show, say, that the user is male; aged 20 to 30 and British. The website can respond to this by displaying products or services likely to appeal to this segment of the market.

4. Clickstreams

As users visit the site more often, more is learned about them by recording what they click on, since this shows what they are really interested in. On a news site for instance, one user may always go to the sports pages first, while another looks at the TV listings. In a retail sense this is akin to physically following somebody about the store recording everything they do (including products they pick up and put back) and everything they look at, whether or not they buy it.
5. Virtual companies and virtual supply chains (VSC)

**KEY TERM**

A **virtual company** is a collection of separate companies, each with a specific expertise, who work together, sharing their expertise to compete for bigger contracts/projects than would be possible if they worked alone.

A traditional supply **chain** is made up of the physical entities linked together to facilitate the supply of goods and services to the final consumer.

**A Virtual Supply Chain (VSC)** is a supply chain that is enabled through e-business links (e.g., the web, extranets or EDI).

The **virtual company** concept has been around since the mid-1990s. Initially, companies attempted to work together using fax and phone links. The concept only really became a reality when technology such as extranets came into common usage. Companies are now able to work together and exchange information on-line. For example, engineers from five companies could design a product together on the Internet.

Many companies have become, or are becoming, more 'virtual'. They are developing into looser affiliations of companies, organised as a supply network.

Virtual Supply Chain networks have two types of organisation: producers and integrators.

a. **Producers** produce goods and services. They have core competencies in production schedule execution. Producers must focus on delivery to schedule and within cost. The sales driver within these companies is on ensuring that their capacity is fully sold through their networking with co-ordinators. Producers are often servicing multiple chains, so managing and avoiding capacity and commercial conflicts becomes key.

**Integrators** manage the supply network and effectively ‘own’ the end customer contact. The focus of the integrating firms is on managing the end customer relationship. Their core competence is in integrating and controlling the response of the company to customer requirements. This includes the difficult task of synchronising the responses and performance of multi-tiered networks, where the leverage of direct ownership is no longer available, and of often outsourced services such as warehousing and delivery.

Many of the most popular Internet companies are, integrators in virtual company’s e.g., Amazon.com and Lastminute.com. These organisations ‘own’ customer contact and manage customer relationships for a range of producers.

4.3.3 Impact of e-commerce and Internet on the traditional business

There are several features of the Internet which make it radically different from what has gone before. The Internet is having, and will continue to have, significant effects on business organisations.

   (i) **Electronic Data Interchange becomes standard method of trading**

   Trading via EDI provides many benefits to an organisation including speed and accuracy of information transfer as well as less input of data for manual form filling. Some organisations have been using this method of information transfer for a number of years, although some organisations are only now adopting this as a standard method of communication.
The effect of this is that some organisations may need to invest heavily in the appropriate IT infrastructure to support EDI. Alternatively, the services of a Value Added Network may be employed.

(ii) Decreased transaction costs

Using some form of EDI also decreases significantly the costs of individual transactions. For example, an electronic bank transaction costs about 15% of the cost of a manual transaction, while processing a purchase order electronically may be as little as 5% of the manual cost.

(iii) Elimination of intermediary organisations

Electronic commerce provides the opportunity for the manufacturer of a good or service to communicate directly with the customer. For example, a supplier of washing machines can produce a web site to provide information on the different machines being sold, and then sell those machines directly to a consumer. The consumer can purchase the machine without having to visit a showroom. This means that the services of the wholesaler to take the washing machines to a central warehouse, and the retailer to provide a shop to view the washing machines, are no longer required.

Electronic commerce has the effect of disintermediation, that is removing intermediary organisations from the supply chain. This process affects not only wholesalers and retailers, but also more mundane tasks such as newspaper delivery. If you can view a newspaper on the Internet, then why bother to have a paper copy delivered to your door?

(iv) Decreased use of cash

Payments are already being made over the Internet using credit card details over secure Internet links, although a standard credit card invoice is still received and is paid at the end of each month. However, electronic trading also makes possible the use of digital cash, that is, money that only has some electronic representation.

There is also the possibility that “smart card” technology can eliminate the use of cash altogether, meaning that all money will be electronic.

(v) “Individualised” marketing

Most marketing campaigns are targeted at specific groups of people e.g. middle-income families who want to buy a new car. However, the use of databases to store purchasing information about individual customers allows marketing to take place at an individual customer level. Rather than receiving generic advertising for motor vehicles, the individual could receive an advertisement for the vehicle that precisely suits that person’s circumstance in terms of number of seats, fuel economy (for town or long distance driving) as well as options such as CD player and choice of colour.

This approach may result in more sales of specific products, but it will also mean organisations may need to make additional investment in data collection and retrieval systems.

(vi) Increased use of Intranets

As already discussed in earlier chapters, Intranets provide an easy-to-use internal communication system. Distinct benefits of protection by firewalls from outside access.
and the use of Internet technology, which employees are already familiar with, means that they may become the standard for sending messages in an organisation.

Intranets allow employees to communicate securely, not just within one office, but also worldwide. Internet technology therefore makes co-ordination of geographically distributed workgroups much easier, compared to sending telephone messages and paper memos around the world.

(vii) Telecommuting

One of the effects of the Internet is to provide faster and more reliable communication systems, not just within organisations but also throughout the whole of society. This means that work, especially knowledge work, is not dependant on location. As long as a telephone, or similar high-speed line is available, then work can take place in any location.

The Internet may well result in increase use of home working as organisations seek to limit expense office space and provide appropriate communication tools to their employees.

(viii) Connectivity

The Internet provides an easy and inexpensive system that allows anyone, anywhere in the world, to connect a computer to the Internet and communicate with any other person or computer similarly connected. This means that individuals can communicate with friends, family and businesses worldwide as well as business organisations having in effect a global market. There is even the phenomenon of the Internet Café, whereby backpackers, for example, wherever they are in the world, can keep family and friends apprised of all their adventures!

The Internet also provides a “level playing field” in terms of advertising. Even small organisations can establish a web site and publicise their products against those of the largest organisations. Large advertising expenditure to reach global markets is no longer required.

(ix) Communication costs

Using the Internet is not free, although it can significantly reduce communication costs. For example, advertising information can be sent to a group of e-mail addresses for the cost of connection to the Internet. However, sending a fax or letter to those customers would cost significantly more as individual telephone calls would have to be made or letters stamped.

Using e-mail over the Internet can also reduce Internet communication costs. Although there are some security issues with this system, any employee can log onto the organisation’s e-mail system from anywhere in the world to collect messages via the Internet. This system saves the cost of having to build a global IT infrastructure, and also costs of couriers where documents are sent electronically rather than on paper.

(x) Faster access to data

Internet connectivity means that as soon as some information is placed on a web page it can be accessed and read by anyone with appropriate Internet or Intranet access. This ability increases the speed of communications and distribution of knowledge. Employees or researchers can also obtain information from any source, worldwide. Prior to using the Internet, this information is likely to have been too difficult or too expensive to obtain.
This list is unlikely to be complete, but it does provide the “feel” for the effect of the Internet across many sections of business.

These new trends are creating pressure for companies. The main threat facing companies is that prices will be driven down by consumers' ability to shop around.

Case example

Airlines

The impact of the web is seen clearly in the transportation industry. Airlines now have a more effective way of bypassing intermediaries (i.e., travel agents) because they can give their customers immediate access to flight reservation systems. British Airways aims to sell at least half of its tickets on-line by the year 2003; one of the new low-cost airlines in the UK, EasyJet, has become the first airline to have over half of its bookings made on-line.

Travel agents

The web has also produced a new set of on-line travel agents who have lower costs because of their ability to operate without a High Street branch network. Their low-cost structure makes them a particularly good choice for selling low margin, cheap tickets for flights, package holidays, cruises and so forth. These low-cost travel agents have been joined, furthermore, by non-travel-agents who simply specialise in opportunistic purchasing (e.g., lastminute.com).

Tesco

In another arena, Tesco is already the UK's largest Internet grocery business, but other companies are rapidly developing new initiatives. Waitrose@work allows people to order their groceries in the morning (typically through their employer's Intranet communication system) and then have them delivered to the workplace in the afternoon. This approach achieves significant distribution economies of scale so far as Waitrose is concerned.

Financial services

The impact of the Internet is especially profound in the field of financial services. New intermediaries enable prospective customers to compare the interest rates and prices charged by different organisations for pensions, mortgages and other financial services. This means that the delivering companies are losing control of the marketing of their services, and there is a downward pressure on prices, especially for services which can legitimately be seen as mere commodities (e.g., house and contents insurance).

4.3.4 Disadvantages of e-commerce

E-commerce involves an unusual mix of people - security people, web technology people, designers, marketing people - and this can be very difficult to manage. The e-business needs supervision by expensive specialists. In spite of phenomenal growth the market is still fuzzy and undefined. Many e-businesses have only recently reported making any profit, the best-known example being Amazon.com the Internet book-seller.
Unless the e-business is one started completely from scratch, any new technology installed will need to link up with existing business systems, which could potentially take years of programming. Under-estimating the time and effort involved is a common obstacle. The international availability of a website means that the laws of all countries that transactions may be conducted from have to be considered. The legal issues surrounding e-commerce are complex and still developing.

1. **Lack of trust**

Above all, however, the problem with e-commerce is one of trust. In most cultures, consumers grant their trust to business parties that have a close physical presence; buildings, facilities and people to talk to. On the Internet these familiar elements are simply not there. The seller's reputation, the size of his business, and the level of customisation in product and service also engender trust. Internet merchants need to elicit consumer trust when the level of perceived risk in a transaction is high. However, research has found that once consumers have built up trust in an Internet merchant such concerns are reduced. Internet merchants need to address issues such as fear of invasion of privacy and abuse of customer information (about their credit cards, for example) because they stop people even considering the Internet as a shopping medium.

2. **Confidentiality**

Potential consumers are (rightly) concerned about providing unknown vendors with personal, sometimes sensitive information. Connecting to the Internet via a browser requires running software on your computer that has been developed by someone you do not know. Moreover, the medium of the Internet is a broadcast network, which means that whatever is placed on it is routed over wide-ranging and essentially uncontrolled paths.

3. **Integrity**

Data both in transit and storage could be susceptible to unauthorized alternation or deletion (i.e., hacking or the e-business system itself could have design or configuration problems).

4. **Availability**

The Internet holds out the promise of doing business on a 24-hour, seven-days-a-week basis. Hence, high availability is important with any systems failure becoming immediately apparent to customers or business partners.

5. **Authentication and non-repudiation**

The parties to an electronic transaction should be in a known and trusted business relationship, which requires that they prove their respective identities before executing the transaction. Then, after the fact, there must be some manner of ensuring that the transacting parties cannot deny that the transaction was entered into and the terms on which it was completed.

6. **Power:**

The Internet gives consumers unparalleled access to market information and generally makes it easier to shift between suppliers. Firms participating in e-business need to make their offerings attractive and
seamless in terms of service delivery. This will involve not only system design but also reengineering of business process. Back-end support processes need to be as efficient as possible because, in many cases doing business over the Internet forces down prices, e.g., online share broking. To avoid being subject to the commodization effect of doing business online, firms need to make their service offerings information rich to differentiate them from the competition and build additional value. Hence, the drive to personalize web sites by targeting content based on analyzed customer behavior and allowing direct contact with staff through instant messaging technology and other means.

**Question 1**

Up to now, many companies have ignored e-commerce. They have watched as a succession of much-publicised ventures have failed to get off the ground and even the best have struggled to translate success into profits. This has created an impression that the internet is a confusing and dangerous sales channel that can, for now, be left to others.

Why, do you think, is this view increasingly untenable?

**Answer**

Relevant points include:

(a) The likely scale and speed of development is immense: by the end of 20C2, Internet business between, for example, US businesses is thought likely to exceed 3300bn, rising from only $4.5bn in 1997.

(b) Every part of the value chain is up for grabs. Any participant in the in the value chain could usurp the role of any other participant.

i) The free flow of information about buyers and sellers undermines the role of intermediaries.

ii) A book publisher could bypass retailers or distributors and sell directly.

iii) A book seller could decide to publish books, based on the information it has obtained about readers' interests.

(c) Net pioneers can secure important advantages over latecomers. They can use information about their customers to tailor their offerings and they may even be able to foster a sense of community among users. For example, part of the appeal of Amazon.co.uk (the Internet bookseller) is the book reviews posted by other readers.

**4.4 E-business Models**

**Key Terms**

A *business model* is an organization’s core logic for creating value in a sustainable way. For profit-making enterprises that means how it makes money over the long haul— not just the most recent quarter”

E-business models are similar to traditional business models in that they follow the same conceptual guidelines as any normal business model. They seek to describe, in conceptual terms, how certain business practices or activities are to be created and implemented for the long-term benefit of the organisation.

The purpose of this section is to give a brief overview of different e-business models. Effective e-business models are the overall result of successfully carrying out business analysis in that they document the concept of HOW AND WHY. The selection of effective e-business models is based on successful business analysis, in that it will allow us to match an organisation to an appropriate e-business model.
4.4.1 **Types of E-business Models**

Business models such as B2C and B2B have been widely referred to in the business media. Several new models have emerged; a summary of the current models is:

<table>
<thead>
<tr>
<th></th>
<th>Government</th>
<th>Business</th>
<th>Consumer</th>
<th>Employee</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Government</strong></td>
<td>G2G</td>
<td>G2B</td>
<td>G2C</td>
<td>G2E</td>
</tr>
<tr>
<td><strong>Consumer</strong></td>
<td>C2G</td>
<td>C2B</td>
<td>C2C</td>
<td>X</td>
</tr>
</tbody>
</table>

The key models can be described as follows:

- **B2C (Business to Consumer)** — typically a retailer selling directly to the consumer; at present, this is the sector that has shown the fastest growth (lately B2B has shown the most growth potential — the B2C growth rate now appears to be decelerating).
- **B2B (Business to Business)** — typically a business selling up, down or across the supply chain, involving business partners or business consortia.
- **B2E (Business to Employee)** — typically a system enabling intercompany (intragroup) e-mails over the Internet to be directed to the correct department.

Examples for two of the other models would be:
- **B2G** — Electronic submission of corporate tax returns.
- **C2G** — Electronic submission of individual income tax returns.

1. **Business to Consumer Models**

In general terms B2C e-business models can be broadly grouped into 5 different sub-categories. An overview of these sub-categories is outlined as under for your reference and consideration.

<table>
<thead>
<tr>
<th>Category</th>
<th>Examples</th>
<th>Business Objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td>Portals</td>
<td>Yahoo</td>
<td>Maximize Audience</td>
</tr>
<tr>
<td></td>
<td>IVillage</td>
<td>Sell Advertising</td>
</tr>
<tr>
<td>Manufacturer’s Direct-sell-sites</td>
<td>General Motors</td>
<td>Disinter-mediate</td>
</tr>
<tr>
<td></td>
<td>British Airways</td>
<td>Improve CRM</td>
</tr>
<tr>
<td>Bricks &amp; Clicks E-tailers</td>
<td>Tesco</td>
<td>Increase Market Share</td>
</tr>
<tr>
<td></td>
<td>Wal-Mart</td>
<td>Improve CRM</td>
</tr>
<tr>
<td>Dot-Com E-tailers</td>
<td>Amazon</td>
<td>Reduce Friction</td>
</tr>
<tr>
<td></td>
<td>CDNow</td>
<td>Create Loyal customer base</td>
</tr>
<tr>
<td>E-Marketplaces</td>
<td>Expedia</td>
<td>Aggregate buyers and sellers</td>
</tr>
<tr>
<td></td>
<td>E-bay</td>
<td>Create Loyal customers</td>
</tr>
<tr>
<td></td>
<td>Letsbuyit.com</td>
<td>Reduce prices through competition and consumer power</td>
</tr>
<tr>
<td></td>
<td>Kosmo.com</td>
<td>Save consumers time and trouble.</td>
</tr>
<tr>
<td></td>
<td>Priceline.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Lastminute.com</td>
<td></td>
</tr>
</tbody>
</table>
I. Portals

Portals seek to aggregate end users (buyers) into a single community by supplying free content and resources. Revenue in this model is normally generated as a result of selling advertising space to manufacturers. Portals seek to be “infomediaries” and supply the end user with all the available information about a certain products or services in order to reduce their friction and retain their patronage. Friction in this context refers to the amount of effort required by the end user to achieve their goal of buying what they want. “From a practical point of view, most shopping is an inefficient process. To find the right product at the right price, pay for it and get it home often involves a considerable amount of time and effort – what economists call ‘friction’

Case Example

As with so many things in life, only a few could play the game; at least, few could play profitably. These are the elite sites on the Web that function as choke points for traffic because they offered content and services that are either essential for practical reasons or compelling for divergent ones. The former includes search engines such as Yahoo! or Excite; these provide navigational tools for finding useful stuff on the Web and hence become the “start” pages. The latter includes sites that built huge audiences for reasons of content, community or commerce, such as CNN Interactive or ESPN Sportszone, Geocities or Gamesville, CDnow or Amazon.com. The commercial promise was crystal clear: When Yahoo! could report 140 million page views a day, Gamesville could boast more than four hours a month per average user on the site, or Amazon.com could register more than six million customers, there was a payback for helping advertisers reach their audiences.

II. Manufacturer's Direct-sell-sites

Models of this nature are normally used to describe situations where the manufacturer utilises their online services to provide an alternative means of selling their product in addition to (or instead of) its traditional distributors and retailers. This creates the risk of disintermediation to parties further down the supply chain. The risk of disintermediation occurs as a result of the removal of traditional sales channels with the replacement of traditional distributors with direct selling to the end user by the manufacturer. This makes the traditional distributor redundant.

III. Bricks & Clicks E-tailers

This is the online version of the shop front. It seeks to enhance the offline presence of the seller, but not directly compete against it. It may, or may not, provide an online sale channel. Depending on the focus of the seller’s business strategy. But it will generally always cover areas such as after sales service, support and advertising. In theory the Internet allows E-tailers (both Bricks & Clicks and Dot-Coms) to practice marketing on a one-to-one basis instead of the broad advertising tactics of one-to-many as seen through traditional channels such as radio and television. This has led to the development CRM (Client Relationship Management) tools that seek to improve the sales and service efficiency of the organisation.

IV. Dot-Com E-tailers

This is also an online version of the traditional shop front but it exists only online. The difference between the Bricks & Clicks E-tailer and the Dot-Com E-tailer is that they have no physical shop front to compliment the online shop front. All services and contact with the end user (except delivery) are dealt with online. Sales, support, etc are dealt with online and organisations of this nature are generally characterised by an interactive web site focusing on sales and the processing (including collection) of those sales. The entities real world, or physical presence, is normally limited to a warehouse or administration facilities. For example the sales information is sent from the online web application to the warehouse that handles the
physical distribution of the product, there is no need for the client to come to a shop front to carry out the transaction.

Case Example

E-commerce referred to the practice of selling real products for real money through online channels. The argument was that a lower-cost channel structure resulting from the “disintermediation” of middlemen such as distributors, wholesalers and bricks-and-mortar retailers could reward new intermediaries, such as Web-based retailers, with fatter margins, even as those Web players shared overall channel cost savings with end-users or Web consumers through lower prices. However, the most celebrated of such e-commerce businesses, Amazon.com, managed to raise more questions about e-commerce in many people’s minds than it answered. For one thing, Amazon.com did not disintermediate its channel because it depended critically on existing physical book distributors, Ingram and Baker & Taylor, to stock and source inventory. Amazon.com simply substituted a virtual retailer for a physical one in an otherwise traditionally configured supply chain. Moreover, Amazon.com spent so heavily on marketing, brand awareness and technology that it has yet to record a profit despite achieving gross margins of a healthy 19 percent.

Finally, Amazon.com expanded into the sales of non-book items, with an apparent lack of regard for the underlying profitability of these new lines. For example, the site sells music CD’s at an average price of $12.99 while incurring costs of $14 per unit. It is hard to make up those losses in volume. But there was a rationale: build a customer base of loyal site users and profitability will follow.

Reasonable people can, and do, disagree about Amazon.com’s future — and, specifically, whether it can turn the corner to profitability at any point given the heavy investments required to maintain its e-commerce leads, marketing and technology. But, while skepticism about Amazon.com may not be justified, a beady eye should surely be cast on many Internet startup companies that have followed in its wake but with a twist.

V. **E-Marketplaces**

E-marketplaces are the online version of the traditional weekend market where parties come together to exchange goods and barter over prices. There are a number of different models within this category, such as online auctions vs reverse auctions, however their objectives are still the same, i.e. to facilitate a medium for buyers and sellers to come together, therefore an in depth analysis on the different models within this category is not warranted.

2. **Business to Business Models**

It should be duly noted that the B2B models may include each of the above B2C business models i.e. manufactures may come together to buy products and services, which in turn are aggregated or are further developed prior to selling to the end user or consumer. One entities client may be another entities supplier. Where B2B and B2C depart ways is in the development of e-business models that focus on generating benefits and savings in the tighter integration of suppliers and manufactures in addition to technology based business improvements between the parties. This tighter integration is reflected in the development of business models that propose alliances with not only suppliers and manufactures but also competitors. The linkages between organizations or alliances can be described in terms of the following business models within this context the e-business models facilitate the interaction and communication pathways between the entities via extranet or other means:
4.5 Electronic Payment Methods

4.5.1 Introduction to Electronic Payments

Electronic payment methods have been in place since the advent of the computer. Consumers and businesses use electronic payments to transmit money between institutions. With the rapid growth of the Internet, business-to-consumer and business-to-business e-commerce firms and consumers whom...
conducted their monetary transactions online are demanding more robust and secure methods of electronic payment systems. This section attempts to survey the electronic payment market and provide some insight from the security perspective.

It is also estimated that over 80% of Internet users will make a purchase on the Internet in the course of their usage. This gives tremendous potential to the electronic payment market. Electronic payment method requires the following qualifiers in order to be accepted by consumers and businesses:

- Electronic payment schemes must provide a trusted facility by which a seller is guaranteed payment and that the buyer is assured that the prescribed payment is distributed to the seller.
- The certification of the buying and selling parties must be ensured.
- A buyer needs assurance that the buyer is whom he claims to be.
- The intermediary of the payment method must ensure that the seller is getting the proper payment and that the buyer is debited accordingly.
- The payment method must also be free from all conceivable attempts of attacks and fraudulent activities.
- Contingencies must also be set up and clearly defined to the users in the event there are signs of fraud.

The Internet is growing at a rapid rate and the amount of transactions conducted over the Internet is growing exponentially. More Internet and PC use growth data. Increasingly, consumers are worried over possibility of fraud in online transactions.

4.5.2 **Electronic cash**

This is another form of automation of cash into electronic form. It addresses circumstances in which the payer is *not* present at the point of sale or service, but has electronic communications facilities available, e.g. is connected to the Internet, or to some other manifestation of the emergent global information infrastructure, such as a cable-TV installation with enhanced capabilities.

Classification of schemes for electronic cash is as follows:
- pre-registered credit / debit card numbers
- electronic cash-pool
- value-token creation and passing
- stored-value card payment

4.5.3 **Electronic payment protocols**

1. **Secure Socket Layer (SSL)**

This protocol was developed by staff at Netscape Corporation in late 1994 and progressed as an Internet draft standard late the following year. SSL is a general purpose protocol designed to be used to secure any dialogue taking place between applications communicating across a “socket” inter process communications mechanism. The SSL protocol is transparent to the application using it. Once both sides are equipped with SSL implementation, application data should pass through the secure socket in the same way as it would a normal (insecure) socket.

2. **Secure-HTTP**

Secured HTTP encapsulates HTTP messages in various forms. When encapsulating, it can include encryption, signing, or MAC based authentication. A message can have several security transformations
applied to it, encapsulating an already encapsulated message. In its header definition, S-HTTP provides key
transfer, certificate transfer, and similar administrative functions.

3. **Secure Electronic Payment Protocol (SEPP)**

SEPP is a protocol developed by MasterCard in October 1995 for secure payment processing using bank
card transactions over public networks and is based on 3KP. In 3KP all the parties possess public key pairs
and corresponding certificates. Some of the important characteristic of SEPP is that this protocol provides a
mechanism to prevent fraudsters from posing as legitimate merchants and “collecting” card data and defines
a certificate management system to control certificates supporting security services.

4. **Secure Electronic Transactions (SET)**

SET is a message protocol designed to verify the authenticity and legitimacy of credit card transactions for
cardholders, merchants and acquirers over open networks, such as the Internet. In addition, SET uses a
combination of symmetric (private key) and asymmetric (public key) encryption techniques plus certificates
of authority to facilitate:

- **Confidentiality** of the trading data between supplier and customer.
- **Authentication** of the trading entities’ legitimacy.
- **The integrity** of the financial data setting the trade.

5. **ECML**

Announced in June 1999, is a universal format for online checkout form data fields. ECML is an open
specification for the exchange of order and payment information. Provides guidelines for web merchants
that enables digital wallets, from multiple vendors, to automate the exchange of information between
consumers and merchants. Wallet software vendors, electronic commerce software vendors, merchants, and
payment card organizations all support ECML. The following digital wallet vendors have adopted the
ECML standard: Brodia, CyberCash, IBM, Microsoft and Trintech.

6. **Automated Clearing House (ACH)**

This service allows a customer to disburse payments and make collections electronically. It is usually
applied to payments to state agencies or government/state related.

7. **Digital Signature**

Digital signature means the result of applying to specific information certain specific technical processes.
This recognizes any mark made with the intention of authenticating the marked document. A signature is
not part of the substance of a transaction, but rather of its representation or form. Digital signatures are
created and verified by cryptography and uses "public key cryptography," which employs an algorithm
using two different but mathematically related "keys;" one for creating a digital signature or transforming
data into a seemingly unintelligible form, and another key for verifying a digital signature or returning the
message to its original form.

The complementary keys of an asymmetric cryptosystem for digital signatures are arbitrarily termed the
private key, which is known only to the signer and used to create the digital signature, and the public key,
which is ordinarily more widely known and is used by a relying party to verify the digital signature. If many
people need to verify the signer's digital signatures, the public key must be available or distributed to all of
them, perhaps by publication in an on-line repository or directory where it is easily accessible. Thus, although many people may know the public key of a given signer and use it to verify that signer's signatures, they cannot discover that signer's private key and use it to forge digital signatures. This is sometimes referred to as the principle of "irreversibility."

The encryption mechanism used for documents is termed a hash algorithm and the output is called message digest. The message digest is created with the sender's private key, which produces a unique digital signature for the original document. The recipient is given the sender's public key, which is used to verify the digital signatures on the document in a process termed signature verification.

The primary uses for digital signatures are for electronic mail, document submission, Electronic commerce over a public network, and electronic data interchange (EDI). Many other uses can be anticipated. Basically, we foresee the technique being used by any application that requires irrevocable authentication of information. This can long as you trust the privacy of private key.

4.5.4 Electronic payment systems/methods

1. Micro Payment

One important aspect of “micro payments” is that the definition varies with the audience. There are varieties of systems claiming to be “Micro payments.” All of them are capable of handling arbitrarily small amounts of money. This was never a real problem; the problem is keeping the cost for the individual transaction low. A very practical approach can be derived from the MPTP Working Draft (Micro Payment Transport Protocol, at the IETF). Micro payments have to be suitable for the sale of non-tangible goods over the Internet. This imposes requirements on speed and cost of processing of the payments: delivery occurs nearly instantaneously on the Internet, and often in arbitrarily small pieces. With the rising importance of intangible goods in global economies and their instantaneous delivery at negligible cost, “conventional” payment methods tend to be more expensive than the actual product. On the other hand, billing for small portions of a product or service reduces the need of security. MPTP is optimized for use for low value transfers between parties who have a relationship over a period of time. It also provides a high degree of protection against fraud making it applicable in wider scenarios, including sale of tangible goods. MPTP is an asynchronous protocol. Much of the processing required may be done offline. In particular payment does not require an online communication with the broker (unless the symmetric signature option is used). MPTP is also symmetric; there is no distinction between customer and vendor accounts except in relation to specific transactions where the flow of payment is generally in a single direction. Use of public key signature screening as opposed to verification makes it economic for use by small publishers.

2. Smart Cards

A smart card is a credit card-sized, tamper-resistant security device that offers functions for secure information storage and information processing that rely on VLSI chip technology. A smart card actually contains a secure microprocessor chip embedded in the card. The chip can implement a secure file system, compute cryptographic functions, and actively detect invalid access attempts. With proper application of file system access rights, a smart card can be safely used by multiple, independent applications. The reason for the growth in smart card’s applications is the smart cards' intrinsic portability and security. Applications are the driving force behind the new smart card market. The most popular application areas for the smart card technology are:

- Loyalty. Identifying loyal customers and rewarding them.
- Information Technology.
3. **Online Banking**

Online Banking can take different forms. Some online banking systems are software based—meaning you will need software such as Quicken, Microsoft Money, or some proprietary, in order to access your account (and you will only be able to handle your banking from your own computer). Other systems are Internet based—meaning you can access your bank account from any computer that is connected to the Web - from your home, office or while travelling. Many PC Banking programs also allow the consumer to access account information, such as personal account balances, account activity or to initiate transfers between accounts. Some systems will allow consumers to initiate electronic payments from their personal computer. Using a personal computer and modem to call the financial institution or other payment agent, a consumer selects payment options from a menu of services. The consumer determines which companies to pay from the list provided (commonly, utility companies). A withdrawal is made from the consumer's account and payments are sent to the companies. The withdrawal is reported on the customer's bank account statement and a record of the specific payments is kept on the PC Banking software (in case one was used).

4. **E-cash (Digicash)**

E-cash is an online software solution allowing payment for information, hard goods, and even payout services. E-cash is said to be fully anonymous because clients withdraw coins from a bank in such a way that the bank cannot know the serial number of those coins. The coins can be spent anonymous with a merchant, and even collusion between both the bank and merchant will to fail to identifier the spender. This method provides the privacy of paper cash with the added security required for open networks. The participants within the system are clients, merchants, and banks. Clients and merchants have accounts at an E-cash bank or any other bank that works with this method. Clients can withdraw coins against their account and store them in their E-cash wallet software that resides on their computers or on a server. The withdrawal protocols prevent the bank from being able to see the serial number of the coins it is issuing. At the time of purchase, the merchant must forward the coins to the minting bank to ensure the validity; this is on way to be sure that be sure that the e-coins have not been spent. If the coins are valid, they will be deposited into the merchant’s account. The merchant can then send the purchase goods or a receipt to the client. A merchant can also make payments to a client using the same procedure. This is useful for making refunds or providing pay out services. Currently, both client and merchant must have account at the same E-cash bank. Another will not accept coins obtained from one bank. As E-cash becomes more widespread, it is likely that third parties might exchange coins from different banks or the banks might provide this exchange themselves.

5. **E-Checks**

The FSTC (Financial Services Technology Consortium) E-checks are the way funds are transferred from the Client’s (payer’s) bank account to the merchant’s (payee’s) bank account at the time the transaction takes place. With electronic checks it is possible to verify funds availability while the payment is done. Also e-checks allow digital signature validation and it can enhance security. Therefore, check payments can be more easily integrated into electronic ordering and billing processes.

A payer issues a check by assembling much the same information as is present on a paper check. For security purposes it is assumed that users are enrolled in some kind of public key based identity scheme.
The users possess an electronic checkbook device or software, which stores secret key and certificate information as well as maintaining a register of what checks have been signed or endorsed. Then the check is transported to the payee in a secure envelope. The payee endorses the check when it is received, again making use of a secure hardware device before forwarding it to the payee’s bank. Once it has reached this point the bank involved would clear the check using the normal automated clearing house (ACH) or electronic check presentment (ECP) methods.

6. **E-Wallets**

An electronic wallet is essentially an online version of the physical wallet where we store personal and payment information safely in one place. At the time of a transaction the information is used to pay for something online. The electronic wallet helps to fill online order forms quickly and easily whenever we shop. The original product concept was a very small software application, linked to a web browser that stored all the information the user needed to buy products online, (credit card number, expiration date, billing address, shipping address). As an example we have Q-wallets (www.qwallets.com), where it is possible to have an e-wallet by simply filling out some information and chooses a Log Id and a password to access the information. In addition, there are several electronic wallets to choose from, each with specific features and benefits. However, electronic wallets fall into two general categories: Server-based and client-based. For the pros and cons of each type, see the comparison below.

<table>
<thead>
<tr>
<th>Wallet Type</th>
<th>Server Based</th>
<th>Client Based</th>
</tr>
</thead>
<tbody>
<tr>
<td>Features</td>
<td>Main software resides on computer servers run by a bank or service bureau. Order form completion usually with a “single click”</td>
<td>(software resides entirely on your computer) Order form completion mainly through “drag and drop”</td>
</tr>
<tr>
<td>Security</td>
<td>May also store transaction history, remember passwords and provide additional services such as store directories, comparison shopping, and automatic notification of special offers and discounts.</td>
<td>More time required for installation. Upgrades may not be automatic.</td>
</tr>
<tr>
<td>Downloading time and installation requirements</td>
<td>Less time required for installation. Upgrades can be done quickly online.</td>
<td>Information stored solely on home PC.</td>
</tr>
<tr>
<td>Information Storage</td>
<td>Information stored on home PC as well as on computer servers run by wallet provider.</td>
<td>Information stored solely on home PC.</td>
</tr>
</tbody>
</table>

7. **Financial electronic data interchange (F-EDI)**

F-EDI involves the transmission of payment transaction data, and associated remittance advice data, from a payee to their bank, for on-forwarding (via banks and/or value-added network operators) to the payee's bank and the payee;
Chapter roundup

- The Internet is a global network linking millions of computers. The World Wide Web (WWW) is a system of Internet servers that support specially formatted documents. A document accessed from the same base web address is known as a **website**.

- Most organisations now have a **website**, and some conduct **transactions** over the Internet.

- The major growth of **e-commerce** so far has been in the Business to Business (B2B) sector.

- The Internet provides opportunities to **automate tasks** which would previously have required human intervention.

- Establishing links to the Internet brings **security risks**. Suitable systems, policies and procedures should be implemented to minimise these risks.

- **Hacking** involves attempting to gain unauthorised access to a computer system, usually through telecommunications links. A virus is a piece of software which infects programs and data and possibly damages them, and which replicates itself. Viruses often use e-mail links to spread.

- **Encryption** aims to ensure the security of data during transmission. Encryption involves scrambling the data at one end of the line, transmitting the scrambled data, and unscrambling it at the receiver's end of the line.

- **Firewalls** are used to prevent Internet users from accessing private networks connected to the Internet, especially intranets. All communications entering or leaving the intranet pass through the firewall, which blocks those that do not meet the specified security criteria.

- **Electronic commerce** means conducting business electronically via a communications link. An older technology that is covered under the electronic commerce umbrella is **Electronic Data Interchange** (EDI).

- The Internet and e-commerce **challenge traditional business models**.

- Ensuring 'back-office' operations complement web-based operations is vital.

- When developing a **strategy for e-commerce** consider:
  - Organisation and culture
  - Systems and infrastructure
  - Training
  - Customers

- **Globalisation** describes the trend towards standardised products, tastes, pricing and organisational policies worldwide.

- The global economy is a **knowledge economy**, in which knowledge is an important source of competitive advantage.

- **Global Business Drivers** (GDBs) may be used to assess high-level global information requirements.
• An organisation’s global information system should complement the organisation’s global business strategy.

Practice Questions

Q No.1) Choose 2 electronic payment systems prepare a comparison addressing issues such as Description of system, target market, advantages & disadvantages.

Q No.2) Review the article at http://b2b.ebizq.net/exchanges/kenjale_1.html Choose an industry and describe a B2B example. Give your opinion about the future of the B2B model. Do you agree with the authors that this term may soon become obsolete?

Q No.3) Prepare a list of information that is shared in a normal business i.e. information to which everyone needs access.

Q No.4) Research the emergence of the B2E model and describe the technologies that could be used by an organisation to support this model. Describe 2 issues that might impact the success of such a model.

Q No.5) Research this model on the Internet and describe it in your own words. Provide some examples of this model. Identify one product that could be used to create a C2C opportunity. Describe the scenario and the benefits that this would provide.

Q No.6) Identify 3 common communication processes or transactions that a citizen must conduct with government. Describe the transactions and how technology could be used to improve the current processes.

Q No.7) Research the objectives of the Citizen Online Project of the Pakistan Government. Give a list of at least 6 types of information that will be available. Site is at http://www.itcommission.gov.pk/itnews/images/citizenproj.htm

Q No.8) Consider a company that produces fabrics for export and which is restricted in its IT resources. Identify as many partners as you can with whom the IT Department might consider a partnership and describe the broad technology environment that might be adopted for each.

Q No.9) Summarise the benefits of EDI and provide examples of how the EDI benefits could be achieved if applied to the traditional order processing systems of a business.

Suggested Solutions

Answer No.1) Students might choose 2 of the following to compare:

• **e-cash:** Various products developed which attempted to provide the online equivalent of cash by utilising public key cryptography. The banking industry was the greatest barrier as there was no general acceptance of this as valid currency.

• **Smart card e-payments:** Similar to phone cards where smart cards are built with a microchip as an online “purse” to store money. Suitable for smaller valued transactions, the “purse” is reloaded from banking machines or proprietary systems. Required the user to have card readers attached to PC.

• **Electronic Purse:** developed by several online vendors. Consumer could purchase a large denomination using standard credit card details that was “held” by the online store for purchases within that store. As the consumer purchases smaller valued transactions the value was deducted from the purse value automatically. The consumer would “reload” the virtual “purse” with value as
required. Great for smaller transactions but restricted the consumer’s choice of where they could shop – if tied to one online store.

- **Credit Cards**: Traditional credit cards such as MasterCard, Visa, and American Express have been accepted as the most common way of purchasing online goods. The main challenges are that these transactions are not suitable for smaller amounts and there have been issues with authorisation and security of the cards.

**Answer No.2** There is no ‘correct’ answer to this question. What we are looking for is demonstration that student understands the model and its position in the business environment. If there are no such models locally in Pakistan, you might like to lead a discussion on whether the students think that the local market will follow the same trends as the western world or if it will take shortcuts and learn from other experiences.

**Answer No.3** Students might suggest the following information:

- Spreadsheet and document templates which are corporate standards
- Policy and procedures manuals
- Quality document (e.g. ISO 9000)
- Software and hardware manuals
- Telephone directories (both internal and external)
- Training manuals
- Company newsletters
- Forms required for administration e.g. annual leave forms. Absentee forms.

**Answer No.4** Suggested solution could cover technologies such as Intranet, Extranet, CUCMe, and bulletin boards. Issues that might arise include:

- The current technology infrastructure of the organisation and whether it is capable of supporting the technologies required.
- The skills of the staff
- The level of access to the technology by all staff
- The willingness of staff to use the technology
- The need to keep it up to date and ensure that the right people have responsibility.

**Answer No.5** All students will answer this differently. The most common answers will probably introduce technologies such as bulletin boards, Chat forums, and online auctions where consumers directly interact with other consumers.

Students might choose an online auction where consumers post what they want to sell and other consumers can purchase. Expected benefits from this type of model could include:

- Cost savings – no expensive paper communications
- Time savings – electronic communications are faster
- Provides greater power to the consumer – greater choice and more control over the purchases
- Greater power to the seller – can reach far greater audiences than ever before

**Answer No.6** Suggested solution could include:

- Taxation
• Notifying departments of change of addresses
• Registering on the electoral role
• Applying for a visa or passport

The students might identify the use of the following technologies as a way of improving access:
• Internet,
• WWW
• Email
• Public information kiosks
• Video-conferencing
• SMS – mobile solutions

**Answer No.7)** Students should identify some of the following:
• organizational details,
• rules and procedures,
• contact persons
• e-mails addresses,
• downloadable forms and
• data of interest to the general public.

**Answer No.8)** The students might identify many different partners for this example. Suggested solution might include:
• **Customers.** Using a website for reaching out to global customers might be a desired outcome so the IT Department might consider using an outsource provider for their services such as web development and hosting or could consider an ASP service.
• **Suppliers.** Adopting an online system with suppliers so that orders for raw materials, can be readily sourced when needed could help. This could be approaching suppliers to establish extranets with them or to develop an industry portal.
• **Government.** The IT department should consider forming a relationship with Government so that export, customs documents can be simply used and more effective communications forged.
• **IT Vendors.** Many IT vendors give partners direct access to their order systems which can be used without the need to develop costly systems.

**Answer No.9)** Some of the suggested benefits include:
• Save costs
• High costs of resources for preparation, handling and data entry of orders can be eliminated.
• Increase Sales and Reduce time for fulfilment
• Reduce Errors
• Improve Security
• Improve Integration
• Reduce Inventory levels
5

Management of Information Technology

<table>
<thead>
<tr>
<th>Topic List</th>
<th>Syllabus Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1 Management of IT Operation</td>
<td>1.2</td>
</tr>
<tr>
<td>5.2 Management of inter-organizational Computing</td>
<td>1.2</td>
</tr>
<tr>
<td>5.3 Management of end-user computing</td>
<td>1.2</td>
</tr>
<tr>
<td>5.4 Financial analysis and control</td>
<td>1.2</td>
</tr>
<tr>
<td>5.5 Accounting for IS Costs</td>
<td>1.2</td>
</tr>
</tbody>
</table>

Introduction

This section has defined “Computer Operations” in a broad sense as everything concerned with ensuring that an organisation can access and use its information systems.

IT is still a relatively new industry and the most rapidly developing industry that the world has even known. The role of IT management has changed from the centralised operation of the Electronic Data Processing (EDP) department to the contemporary IT Department. Many new technologies have had a profound impact on the organisation of IT. This section has defined “Computer Operations” in a broad sense as everything concerned with ensuring that an organisation can access and use its information systems.

After reading through this chapter a student must be able to evaluate IS operational practices to ensure efficient and effective utilization of the technical resources that are used to support the organization’s IS processing and business requirements.

Study Guide

Management of Computer Operations (Study text reference 5.1)

**IT Operations Strategy**
- Ensure that the students understand the relationship of the IT Operations Strategy with the other Strategic Plans.

**Technology Planning**
- Discuss the diagram included in the Student Guide.
- Lead a discussion on who the students think should be included in this activity.

**Measuring and Managing Capacity**

**IS Operations Staffing**
- IS staffing issues are not just confined to the Operations area. However there are increasingly technical skills required to work in this complex area. You might want to discuss the issue of Operations staffing with the class.
<table>
<thead>
<tr>
<th>Study Guide</th>
</tr>
</thead>
</table>

**Production Planning and Control**
- You might want to lead a discussion about what Production Planning and Control means in a small business.

**Security**
- Security is a complex issue and the IT infrastructure of an organisation must be protected.

**Privacy**

**Management of Interorganizational Computing (Study text reference 5.2)**

**Collaborative computing**
- You might want to discuss concepts and if any of the students have direct experience with collaborative computing.

**Distributed Systems**

**Outsourced Services**
- Outsourcing can involve a little of the organisation or the whole IT department. And there are various ways of outsourcing specific functions. Discuss the role of ISPs as outsource providers. Lead into a discussion of ASPs.

**Management of end-user computing (Study text reference 5.3)**

- “End-user” is a term that can have several different connotations and as a consequence different implications for management. You might wish to lead a discussion on the various levels of end-user computing

**Financial analysis and control (Study text reference 5.4 & 5.5)**

**Capital Costs**
- There are several choices to obtaining IT hardware and software including renting, leasing and buying outright.
- Capital costs can also incur other costs that are sometimes ignored. Also there are many flow-on costs associated with capital investments that are often hidden.

**Time and expense Tracking**
- Lead a discussion with the students about mechanisms they may have seen that allow the time and expense tracking.

**Cost charge out and Monitoring**
- Lead a discussion on the different ways that an IT department might operate.
5. MANAGEMENT OF INFORMATION TECHNOLOGY

5.1 MANAGEMENT OF IT OPERATION

IS Operations control the day-to-day functioning of IS hardware and software. IS processing environments vary among organization depending on the size of the computer installation and workload. Computer operations can have various meanings. In these mainframe environment, it is described a physical process whereby someone managed the actual hardware and associated processing. Hardware was restricted to mainframe computers, dump terminals, peripherals (e.g. printers, scanners, drives etc) and some communications. In today’s environment, the term can have vastly different meaning. It can be extensive and can include all IT or can be restricted to just computers or just to the technology operated for a particular organization unit. If we take the broad sense and define it as everything concerned with ensuring that an organization can access and use its IS, then there are many tasks involved with managing computer operations. It is not only restricted to the managing the hardware or physical assets but the information assets and systems as well.

An organization embrace integrated and networks systems, the impact of failure of the technology, network or systems is increasingly jeopardizing the entire organization can incur large losses. So what should be the management of computer operations address? IS operations generally include the following functional areas:

- Computer operations
- Controlling input/output of data
- Management of IS operations
- Control Function
- Planning and scheduling : Service level
- Job Accounting
- Scheduling
- Monitoring use of resources
- Problem management
- Program change control
- Quality assurance
- Technical support/help desk
- Librarian function
- Management of physical and environmental security

Management sometimes formulates a strategy for the management of its computer operations, termed as IT Operation Strategy.

IT Operation strategy must deal with the following issues

- **IT Architecture:** Ensure that a realistic architecture has been planned and is being implemented. Standards, protocols, networks, and interconnectivity must be addressed and will serve as the basis of organization’s change and procurement decisions.
• **System Development**: Ensure that the new systems are developed in a way that makes them feasible and operationally viable. Operational staff must be included in the systems development life cycle so that the operational feasibility issues can be addressed early and tested as the part of the system testing. This will also contribute to the capacity planning tasks of the operations area.

• **IT Sourcing**: Ensure that the internal and external sourcing decisions are carefully considered as a part of the overall architecture. Policies and procedures of procurement of technologies or for external information exchange must be established and staff informed about them particularly if these decisions are decentralized. Without the overall architecture in place, the organization faces risk from vendor viability, cost and poor relationships with providers. This will ensure that overall capacity, maintenance and operational issues are considered and strategies implemented to support them.

Now we will look at all the functional areas in detail, that must be addressed by an IT Operation Strategy:

### 5.1.1 Computer Operations

1. **Operator Assisted Operations**

Computer operators are responsible for the accurate and efficient operation of scheduled computer jobs. The operator’s tasks include:

- Running jobs/macros/programs
- Restarting computer applications after an abnormal termination has been investigated and resolved by the responsible department
- Facilitating timely back up of computer files
- Observing the information processing facility for unauthorized entry
- Monitoring adherence to documented job schedules as established by IS and business management
- Participating in test of disaster recovery plans

Procedures detailing instructions for operational tasks and procedures, coupled with appropriate IS management oversight, are necessary parts of the IS control environment. This documentation should include:

- Operator procedures based on computer and peripheral equipment operating instructions and job flows
- Procedures for rectifying machine or program failures and the escalation of unresolved failures
- Instructions for output report distribution
- Procedures for obtaining files from the off-line library and returning files to the library
- Procedures for reporting run delays
- Procedures for reporting and correcting equipment of failures and job processing delays.

2. **Lights Out Operations (Automated Unattended Operations)**

Lights out operations are the automation of key computer room operations whereby tasks can take place without human intervention. The types of tasks being automated with the use of system operations software are:

- Job scheduling
- Console operation
• Report balancing and distribution
• Re-run/re-start activates
• Tape mounting and management
• Storage device management
• Environmental monitoring
• Physical and data security

5.1.2 Input/Output Control Function

Input/output (1/0) control personnel are responsible for ensuring that batch processing information is processed accurately and completely in accordance with IS management’s intent and authorizations. In online environments where processing is generally paperless, the interrelationships among various applications are most appropriately dealt with during the processing control portion of an applications review. For example, in a paperless order processing system where customers initiate and are invoiced via PIM, 20 or more separate applications may be involved. In such a system the output from one system is the input for the next system in sequence. In general while the individual applications are maintained online, files are transferred between the applications using a batch file transfer mechanism controlled by the job scheduler. If the standard job schedule is modified, it is conceivable that input files expected by a successor application may not be present and cause production processing to halt.

Based on the aforementioned example and on the responsibilities associated with this position, the typical tasks performed by 1/0 control personnel include ensuring the following:

• Input is processed accurately and in a timely manner.
• Output is produced in the proper format and is distributed to the appropriate people. With the availability of communication facilities, the high-speed printing of paper documents (i.e. reports, bills etc.) is often accomplished at a remote and sometimes separate location from the IS department.
• Output that becomes input to the next system in sequence is accurate and complete and produced in a timely manner.
• Correct in a timely manner.
• Correct files were used during processing.
• Proper actions were taken by operators.
• No evidence exists that indicates that data was altered in an unauthorized manner.

1. Data Entry Personnel

Data entry via a computer terminal though the production environment to secondary storage media such as magnetic tapes and disks is the most common procedure requiring human interaction with the computing environment. Data entry controls include:

• Key verification - While many types of certification techniques may be employed during the data entry process, one-to-one verifications though often impractical for verifying large amounts of data entry, will yield the highest degree of confidence that data entered is error-free.
• Segregation of data entry functions from data entry verification
• A log/record detailing the time date employee’s initials/user-ID and progress of various data preparation and verification tasks.
5.1.3 Management of IS Operations

IS management has the overall responsibility for all operations within the IS departments. Operations management functions include:

- **Resource allocation** – IS management is responsible for ensuring that the necessary resources are available to perform the planned activates within the IS function.
- **Standards and procedures** – IS management is responsible for establishing the necessary standards and procedures for all operations in accordance with the overall business strategies and polices.

5.1.4 Control Function

Management control functions include:

- Ensuring that detailed schedules exist for each operating shift
- Planning to ensure the most efficient and effective use of an operations’ resources
- Authorizing changes to the operations schedules
- Monitoring operations to ensure compliance with standards
- Reviewing console log activities during system shutdown and hardware/software reinitialization
- Reviewing the operator log to identify variances between scheduled and actual activity
- Ensuring information systems processing can recover in a timely manner from both minor and major disruption of operations
- Monitoring system performance and resource usage to optimize computer resource utilization
- Anticipating equipment replacement/capacity to maximize current job throughput and to strategically plan future acquisitions
- Monitoring the environment and security of the facility to maintain proper conditions for equipment performance
- Ensuring changes to hardware and software do not cause undue disruption to normal processing
- Maintaining job accounting report and other audit records
- Limiting physical access to computer resources to those which require it

5.1.5 Planning and Scheduling: Service Level

The IS department is a service organization for end users. As such, the success of the IS department is dependent upon satisfying end user processing and service requirements. These services include accuracy, completeness, timeliness and proper distribution of output related to application processing. Many tools are available to monitor the efficiency and effectiveness of services provided by IS personnel. These tools include:

- **Abnormal job termination reports** - these automated reports identify all application jobs, which were terminated before successful completion and generally include an explanation or indication of the abnormal termination conditions.
• **Job Rerun Report** - an additional automated report that should be considered within this process is the job rerun report that identities all application re-runs and restarts. This would provide additional, useful information regarding IS operations since most abnormal job terminators result in job restarts.

Excessive abnormal terminations can indicate:

- Poor application design development or testing
- Inadequate operation instructions
- Inadequate operations support
- Inadequate operator training or performance monitoring

• **Operator problem reports** - These manual report are used by operators to log computer operations problems and their resolutions. Operator responses should be reviewed by IS management to determine whether operator actions were appropriate or whether additional training should be provided to operators,

• **Output distribution reports** - These reports identify all application reports generated and their distribution locations. They can be either manual or automated and can be helpful for tracking lost, delayed or misrouted reports.

• **Console logs** - These automated reports identify most of the activities performed on the computer. Because of its size and complexity, it is difficult to use the console log for monitoring computer activity. Programs have been developed which analyze the system log to report on specifically defined item. Using this software, the auditor can carry out tests to ensure that:

  - Only approved programs access sensitive data,
  - Utilities or service aids that can alter data files and program libraries are used only for authorized purposes
  - Approved programs are run only when scheduled and conversely that unauthorized runs do not take place.
  - The correct data file generation is accessed for production purposes.
  - Data files reported to be password protected are protected.

• In addition there are software packages similar to the console logs that provide facilities to log and report all incidences of terminal logon/logoff, hardware malfunctions system start-up and shutdown and job start or stop.

• **Operator work schedules** - These schedules are generally maintained manually by IS management to assist in human resource planning. By ensuring proper stalling of operation support personnel, IS management is assured that service requirements of and users will be met. This is especially important during critical or heavy computer usage periods. These schedules should be flexible enough to allow for proper cross training and for emergency staffing requirement.

1. **Service Level Agreements**

Many IS departments define the level of service that they will guarantee to users of the IS facilitates. This level of service is often documented in service level agreements (SLA). It is particularly important to define service levels where there is a contractual relationship between the IS department and the end user. For example, when the functions of the IS department are performed by a third party under an outsourcing agreement.

Service levels are often defined to include hardware and software performance targets (such as user response time and hardware availability) but can also include a wide range of other performance measures. Such measures might include financial performance measures (such as resource planning, staff turnover,
development or training) or risk management measures (compliance with control objectives). The IS auditor should be aware of the different types of control measures, as well as efficiency and effectiveness measures. Where the functions of an IS department are outsourced, the IS auditor should ensure that provision is made for independent audit reports that cover all essential areas and for full audit access by the user.

5.1.6 **Job Accounting**

Job accounting applications are designed to monitor and record IT resource usage. Information recorded by these applications, (such as the performance and utilization of the CPU, secondary storage media and terminal connect time) is used by IS management to perform activities that include:

- Matching resource utilization with associated users for billing purposes
- Optimizing hardware performance by changing or tuning system software defaults

5.1.7 **Scheduling**

Scheduling is a major function within the IS department. The schedule includes the jobs that must be run, the sequence of job-execution and the conditions that cause program execution. It also permits the scheduling of low-priority jobs, if time becomes available. Automated job scheduling software provides control over the scheduling process, since job information is set up once, reducing the possibility of errors, job dependences can be defined, and the software can provide security over access to production data.

High-priority jobs should be given optimal resource availability while maintenance functions such as backup and system reorganization, if possible, should be performed during non-peak times. Schedules provide a means of keeping customer demand at a manageable level and permit unexpected or on-request jobs to be processed without unnecessary delay.

Job scheduling procedures are necessary to ensure that IS resources are optimally utilized, based on processing requirements.

5.1.8 **Monitoring Use of Resources**

Company’s resources, like any other organization asset, should be used in a meaner that benefits the entire organization. This includes providing information when and where it is needed at a cost that is identifiable and auditable. Computer resources include hardware software telecommunications and data.

Controls over these resources are sometimes referred to as general controls. Effective control over computer resources is critical because of the reliance on computer processing in managing the business.

5.1.9 **Problem Management**

It includes detection, documentation, Control, Resolution and Reporting of Abnormal Conditions. Because of the highly complex nature of software, hardware and their interrelationships, a mechanism should exist to detect and document any abnormal conditions, which could lead to error. This documentation generally takes the form of a mechanized or manual log.

Errors that should be entered in the log include:
• Program errors
• System errors
• Operator errors
• Telecommunication errors
• Hardware errors

Examples of items that should appear in an error log entry include.

• Error date
• Error resolution description
• Error code
• Source of error
• Escalation data and time
• Initials of the individual responsible for maintaining the log
• Initials of the individual responsible for closing the log entry
• Department/center responsible for error resolution
• Status code of problem resolution (i.e., problem up in, problem closed pending some future specified date or problem irresolvable in current environment)
• Narrative of the error resolution status

For control purposes, the ability to add to the error log should not be restricted. The ability to update the error log should however, be restricted to authorized individuals. Proper segregation of duties requires that the ability to close an error log entry be assigned to a different individual than the one responsible for maintaining or initiating the error log entry. Following additional controls should be implemented:

• IS management should ensure that the problem management mechanism is properly maintained and that outstanding errors are being adequately addressed and resolved in a timely manner.
• IS management should develop operations documentation to ensure that procedures exist for the escalation unresolved problems to a higher level of IS management. The primary risk resulting from lack of resolution of problems is the interruption of business operations.
• Problem escalation procedures should be well documented. Problem escalation procedures generally include names/contact details of individuals who can deal with specific types of problem types of problem that require urgent resolution and problems that can wait until normal working hours.
• IS management should ensure that the problem evaluation procedures are being properly adhered to.
• Problem resolution should be communicated to appropriate systems, programming operations and user personnel to ensure that problems are resolved in the most timely manner. By examining a report of all our standing problems which have not been assigned for resolution and by following up on exception, the IS auditor can gain comfort as to whether problems are being communicated to the individuals most capable of resolving them.
• The departments and positions responsible for problem resolution should be a part of problem management documentation. This documentation must be properly maintained to be useful.
5.1.10 Program Change Control

Program change control (PCC) procedures, a part of the more encompassing function referred to as change managements, are established by IS management to control the movement of applications (composed of jobs or programs) from the test environment, where development and maintenance occurs, to the staging environment, where through testing occurs and finally to the production environment.

This portion of the PCC mechanism that describes the actions to be performed by IS operation personnel after a job or program has passed user acceptance testing and is to be moved from the staging environment to the production environment is usually referred to as formal job turnover procedures. The procedures associated with this turnover process ensure that:

- System, operations and program documentation are complete, up-to-date and in compliance with the established standards
- Job preparation, scheduling and operating instructions have been established
- System and program test results have been reviewed and approved by user and project management.
- Data file conversion, if necessary has occurred accurately and completely as evidenced by review and approval by user management
- System conversion has occurred accurately and completely as evidenced by review and approval by user management.
- All aspects of jobs turned over have been tested, reviewed and approved by control/operation personnel

5.1.11 Quality Assurance

Quality assurance personnel verify that system changes are authorized tested and implemented in a controlled manner, prior to being introduced into the production environment. They also, with the assistance of librarian software, oversee the proper maintenance of program versions and source code to object integrity. Specific objectives of the quality assurance function include:

- Ensuring the active and coordinated participation parties in the revision, evaluation and dissemination of standards, management guidelines and procedures
- Maintaining the agreed upon systems development methodology
- Reviewing and evaluating large system projects at significant development milestones and making appropriate accommodations for improvement.
- Establishing, enhancing and maintaining a stable, controlled environment for the implementations of changes within the production software environment.
- Defining, establishing and maintaining a standard, consistent and well-defined testing methodology for computers system.
- Reporting to management on system that are no performing as defined or designed.

5.1.12 Support/Help Desk

The responsibility of the technical support function is to provide specialist knowledge of production systems to identify and assist in system. Change/development and problem resolution. In additions, it is
technical support’s responsibility to apprise management of current technologies may benefit overall operations.

Procedure’s covering the tasks to be performed by the technical support personnel must be established in accordance with an organization’s overall strategies and policies. The support functions include:

- Determining the source of computer problems and taking appropriate corrective action
- Initiating problem reports as required and ensuring that problems are resolved in a timely manner
- Obtaining detailed knowledge of the operating system and other systems software

## 5.1.13 IS Operations Staffing

IS staffing issues are not just confined to the Operations area. However, there are increasingly technical skills required to work in this complex area. In large organizations with mainframe computers and systems operating 24 hours x 7 days, Operations staff will need to be organized to work appropriate hours to be able to support and monitor the systems needed. Shift-workers introduce another complexity to the Operations area and hand-over procedures are needed. Imagine the potential chaos that could be caused if staff on one shift leave without providing a status report to the staff on the next shift about the happenings during their shift and any outstanding problems.

Consider some of the following examples of operational issues and the skills that would be needed:

- The complexity of today’s databases in large organizations that need constant tuning and managing.
- The need for backup and recovery operations to occur seamlessly without impact on the business.
- The complexity of network protocols and telecommunications options for linking branches and external partner across local areas, across regional areas and across national boundaries.
- In many organizations, there is a move to “light out” operations that impact careers paths and jobs.
- The challenges of keeping up to date with trends, with communicating across all levels of the organization and being able to respond quickly to disaster situations are all critical skills for staff in the operations area.
- The difficult role of the Operations staff in trying to keep customers and staff informed about any operational issues while desperately trying to fix problems and restore normal systems functioning as soon as possible.
Case Example

Computer Society of Pakistan (www.csp.net.pk)

The Computer Society of Pakistan is the national organization of Information Technology professionals in the country. It was established in 1973 to promote the use of computers, increase general awareness among the public and to look after the professional interests of the IT personnel in the country.

Objective: To facilitate the professional advancement of personnel engaged in Information Technology (IT) and related occupation, To promote knowledge of the development and use of IT equipment and related techniques, To provide facilities for exchange of information and views of IT equipment and related techniques, To foster and encourage high standards of professional ethics and conduct among its members, To prescribe professional qualifications and to conduct examinations for members and others in the field of Information Technology

5.1.14 Privacy

With many countries now adopting privacy legislation, the issue is no longer a strategic one but an imperative one. Large databases are part of any corporate IT infrastructure and the personal data held in these databases needs to be protected. Privacy is an individual’s right to determine for themselves what information about them is communicated to others or held as private.

Owing to less expensive storage devices, faster processors and sophisticated databases, information is held and cross-referenced more than ever before. The proliferation of PCs, laptops and hands-held devices all potentially containing sensitive personal data and corporate secret has increased an organization’s exposure to privacy and security issue. The Operations Management needs to be included in the planning of new systems and access devices so that the privacy issues are recognized and addressed.

Physical security can restrict access but measures need to be put into place to protect the data and keep it secure. Classification of data according to its sensitivity linked with access controls can restrict the availability of data within the organization. It is a balancing act to resolve the issue of privacy versus accessibility.

Policies and procedures must be developed and widely distributed so that each staff member within the organizations knows how to handle data and how to protect it. While responsibility for this may lie outside the Operation area, it is these operational issues that can cause most problems.

Case Example

The four principles of privacy

In the US, data protection is largely based on self-regulatory initiatives which, however, fail to enforce their own rules to companies that clearly violate their guidelines. In May, following the opening of hearings on Capitol Hill, the Federal Trade Commission said that industry self-regulation was not enough. In a survey
Management of Inter-Organizational Computing

Today’s computer environment is much more complex. Business has a much closer working relationship with their external business partners and thus the movement of data and information between these organizations is more critical. Reliance on technology now extends beyond the organization- into areas over which we have no direct control.

Early users of computer processing bureau services and early adopters of Electronic Data Interchange (EDI) were the first to deal with issues arising from inter-organizational computing. There are several well-known technologies that are part of current IT strategies and which require strong management of external partners. These are described below:

5.2.1 Collaborative Computing

**Key Term**

**Collaborative computing** is the art of using computers to support groups of people as they co-operate to achieve their goals.

Collaborative computing facilitates the growth of team-based organizations through its ability to allow the geographically distributed teams to develop, edit and utilize a common database. Sometimes called workgroup computing or groupware, collaborative computing provides an opportunity for a group of individuals to share and relay information in such a way that cultivates team review and interaction in the accomplishment of duties and attainment of consensus.

The essential components of a collaborative-computing environment are

- Facilities for processing and disseminating documents and databases,
- Electronic mail,
- Information-sharing supports through communication and discussion,
Facilities for mail-authorized and
Interconnected office automation software and an application development interface.

Application of the technology in major companies, including accounting firms, seems to confirm predictions that collaborative computing will recast work patterns.

Organizations tend to become more inefficient as they grow. Increases in the number of staff means that roles change and responsibilities are devolved. With the advent of desktop systems, various departments created their own databases so that they could directly maintain information about the external parties that they dealt with and have the information required at their fingertips. This required time to enter, maintain and support the information and often resulted in costly information that was duplicated across departments. If the external party ranges to change an address then the information may only be changed in the local database and other parts of the organization may retain the previous details. Organizations ended up holding duplicated and sometime-unmatched data about a single entity.

There had to be a balance between the centralized mainframe systems that were inflexible and the desktop systems that could be readily changed but not integrated with any other parts of the organization.

Some of the questions it seeks to answer are:

- What tasks are done in-group, and why?
- How do groups co-operate to get those tasks done?
- Which tools can computer science construct to improve the process?
- How should those tools be constructed?
- How well do those tools work in the real world, and why?

The more widely used name for the core of this field is computer supported co-operative work (CSCW). While early users of collaborative computing were internal users working together, technology has widened the use and now enables geographically distinct user to work together through seamless technological links. Organizational trends to flatter structures have seen collaborative technologies flourish. Small teams can work together as one.

The creation of an intranet within organizations has enabled better use of corporate resources and enabled greater collaboration among employees.

1. Benefits and Costs involved in CSCW

Both large and small businesses can take advantage of collaborative computing, the need for which grows out of the desire to bring together diverse resources into a team. As with any technology-related decisions, the first step is to assess needs. How do we expect people will need to work together?

- Who needs to be connected?
- What security needs to be in place?
- What are the expected benefits of implementing this technology—savings, quality, and/or workplace satisfaction?

These issues should be addressed before being exposed to the "white lights" of the software sales staff. Next, a proper matching of the characteristics of the various vendor's software offerings to application needs can be made. The offerings of major vendors differ in ways that require this up-front assessment of the needs and environment of the workplace in order to choose the products that fit. For example, the present design of Windows for Workgroups may be particularly well suited to work environments involving
a small group, where stand-alone computers can be directly interconnected. Notes, Team Links, and Cooperation are capable for use as enterprise-level collaborative products.

After a candidate system is selected, pricing of all components of the installation (e.g., software, servers (if required), cables, training and on-going support and maintenance) can then lead to a business decision. Limousines can be used to pick up the groceries at the store, but are more than necessary to do the job. A firm may not need the same system as one down the street; maybe the price for the application just can't be justified. The technology is an extension of existing systems, an enhancement, and a facilitator for a collaborative work environment, not a panacea for all business problems.

5.2.2 Distributed Systems

For many years, the centralized data processing approach was widely adopted by business. Since then have been trends away from the centralized approach to a distributed model. One of the main factors I this trend has been the continued dramatic decrease in the cost of computer hardware at the same time that the software was becoming increasingly more available, feature-rich and intelligent.

**Key Term**

**Distributed System** is a system in which data processing in which some or all of the processing, storage, control functions and input/output functions are undertaken by dispersed data processing units which are themselves linked.

Depending on what parts of the IT are dispersed, there is a different focus given to distributed processing.

**i) Distributed applications or systems** Application systems may be distributed in different ways. Firstly, systems are said to be distributed by function if some parts of the system are undertaken by one department while other parts of the system are handled by other department e.g. retail industry where customer sales are usually handled by point-of-sale systems while these systems also rely on accessing the central systems for pricing information. Secondly the systems are said to be distributed if many users are connected to the system performing different functions and using different part of the system.

**ii) Distributed Data** Portions of a corporate database are dispersed among a number of computers and users thus making the directory management and tracking a key feature of these systems.

**iii) Distributed Devices.** Where one system may receive input from variety of sources, the system is said to be distributed. For example consider a manufacturing business where process controllers, robotics arms or sensors control manufacturing are changing the processes. Each of these devices is an essential part of the systems.

No matter what the type of distributed system, there are challenges for management. With the centralized model, there are lost of texts and references about IT management, but the distributed models in general mean a different Organizational structure. Responsibility for IT is quite often distributed in line with the approach to distributed processing.
5.2.3 **EDI and Electronic Commerce**

Electronic Data Interchange (EDI) has been around for many years now as a way of exchanging information between trading partners. EDI can be defined as “the direct computer-to-computer exchange of information”. EDI was originally provided for information about standard business transactions such as invoices, order, and delivery documentation. Long before the Internet provide an “open” architecture for linking systems and transferring information, organizations offered private networks for business to use to conduct EDI.

To see the further aspects of EDI and Ecommerce refer to Chapter 3 of this study text.

5.2.4 **Outsourcing**

A strategic decision has been made by many organisations over the last decade to concentrate on their ‘core activities’ and to ‘outsource’ functions which are not seen as core activities. However, organisations have reached different decisions as to what constitutes a ‘core activity’. The basis of decision-making has included:

- those seen as critical to current organisational performance;
- the ones that are seen as driving the future growth and innovation of the business;
- those that appear to offer the most scope for offering competitive advantage;
- those traditionally performed internally;
- those creating most problems of management or staffing;
- those where there is a thriving industry to provide external support.

For some organisations, all or part of their IS/IT activities have not been defined as core and have thus been candidates for outsourcing. The nomination of IS/IT for outsourcing has also been favoured in some cases because of difficulties in recruiting, retaining and fully utilising the necessary technical expertise to adequately staff the function in the competitive environment of the United Kingdom IS/IT marketplace, where there is a shortage of qualified experienced staff.

Outsourcing is a term, which embraces a number of different approaches. It involves purchasing the services required to perform business functions from outside the organisation. Management must have a strong reason to outsource and define clear objectives and goals.

- What are the **critical success factors (CSFs)**? Measures must be defined that will determine whether the outsourcing is successful or not.
- How should the **outsourcer perform the task**? Management principles to be used by the outsourced service provider need to be defined by the organization as to how they want services to be delivered (e.g. methodologies, hardware procurement, and intellectual property)
- What is the **status and condition of the current IT environment**? Understanding the current condition of the IT environment is critical before preparing any proposal or negotiating any contracts.
- Who will prepare and monitor the **Service Level Agreement (SLA)** with provider of the outsourced service? The importance of developing and monitoring the SLA cannot be underestimated.
1. **Different approaches to outsourcing**

I. **Total outsourcing**

This is where an organisation enters into a contract with a specialist company to provide all of their IS/IT operations, maintenance and development activities. This is frequently described as Facilities Management, which is defined as the contracting out of the management and operation of an organisation’s IT services to an external source, at an agreed service level, over a fixed time period, to an agreed cost formula. An example is where an organisation contracts out all of its existing IS/IT staff and facilities to be managed by an external specialist company such as EDS or SEMA for a period of three to five years. The host organisation may seek to retain a small core of internal staff to oversee the management of the contract but it is difficult to retain sufficient ‘intelligent customer capability’ to maintain true independent control.

II. **Multiple/selective sourcing**

Where an organisation enters into agreements with a range of suppliers; it may create framework contracts whereby it can purchase specialist equipment or services with a degree of competition as and when required; the host organisation will retain its main IS/IT internal staff organisation.

III. **Joint venture/strategic alliance sourcing**

Where an organisation enters into a joint venture with a supplier on a shared risk/reward basis for a specific purpose – frequently the development of a software package or piece of equipment which is seen as having widespread application across other organisations. The host organisation will usually retain its in-house IS/IT function.

IV. **Insourcing**

This is where an organisation buys in management or technical capabilities to accommodate the peaks of IS development work. The company retains its own centralised IS/IT function but buys in maintenance or development services from outside. An example of this approach is the use of ‘off-shore systems development’ whereby an organisation has a contract with a software house outside its own country borders to write (and in some cases maintain) the programs for a new application suite, with the specification of requirements being made by the host company. This has been particularly popular with UK companies entering into contracts with software houses in the Indian sub-continent and there has been some success claimed. The benefit is seen as access to lower-priced, skilled labour but frequently the difficulties in project management and communication have been under-estimated.

Overall the benefits of outsourcing have been seen as:

- **Cost reduction** – because of the economies of scale available in purchasing equipment and efficiencies in utilising specialist staff;
- **Business improvement** – by management being able to concentrate on core competencies because of expertise and specialisation available to manage and staff the IT function;
- Avoid the growing **shortage of IT and IS systems staff** and keep up with technological change;
- **Cost control** – creating a ‘customer/contractor’ relationship tends to concentrate the focus on cost control which is sometimes lost when functions are performed internally.

Difficulties with outsourcing have been seen as:

- The host organisation and the outsource organisation will have **different objectives**.
Frequently the host organisation is looking to improve information systems and facilitate organisational change or competitive advantage.

The contracting company will be seeking to minimise risk and maximise profit by maintaining stability and drive down its costs and is unlikely to suggest changes.

Outsourcing may be seen as a way of off-loading problems rather than as the result of a strategic assessment of costs and benefits.

Work that has been outsourced is difficult to switch to a new supplier if there are problems, or at the end of a contract period. This gives the external supplier significant bargaining power.

Problems of security and loss of confidentiality – particularly where an outsourcing company is also working for competitors.

Loss of flexibility – particularly when there is a need to respond to changing requirements, there may well be a competition between customers for access to the supplier's development staff.

A survey of organisations with outsourced IS/IT contracts has highlighted cost escalation, quality control, loss of independence and over-dependency upon suppliers, lack of supplier flexibility and shortage of management skills as major problems. Now that there is longer experience of outsourcing of IS/IT, the issue of maintaining and developing the host organisation’s organisational learning capability is becoming an issue.

There is always a need to nurture and develop a core of internal staff to initiate strategic thinking and development and to manage the outsourced contracts. To develop and retain these staff is difficult if all ‘action learning’ is performed outside the organisation. The knowledge and skills of internal staff tends to erode if they are not actively involved and it is difficult to develop the next generation of senior management if they are not able to get experience in key areas of the business. Any outsourcing decision needs to be treated with care; it can give apparent short-term advantages in cost-reduction but provide a hostage to fortune in the longer term.

5.2.5 Application Service Provider

The Web and the Internet began to really heat up and receive significant media exposure starting around 1994. Initially, the Web started as a great way for academics and researchers to distribute information; but as millions of consumers flocked to the Internet, it began to spawn completely new business models. Three good examples of innovative models include:

- Amazon - Amazon (which opened its doors in July, 1995) houses a database of millions of products that anyone can browse at any time. It would have been impossible to compile a list this large in any medium other than the Web.
- Ebay - Online auctions make it easy and inexpensive for millions of people to buy and sell any imaginable item. It would be impossible to do this at a reasonable cost or in a timely manner with any medium other than the Web.
- Epinions - Thousands of people contribute to a shared library of product reviews. One of the Web's greatest strengths is its worldwide view and collaborative possibilities.

These different business models are all visible to anyone surfing the Web. One of the most interesting behind-the-scenes business models that the Web has created is called the ASP, or Application Service Provider. ASPs are a completely new way to sell and distribute software and software services. Although ASPs were possible before the advent of the Web, the Web makes them so easy to create that they have proliferated hugely in the last several years. The ASP model can be extremely appealing to businesses -- especially small businesses and startups -- because it can drastically lower the costs of software and services.
1. Defining an ASP

ASPs tend to be made fairly complex and confusing in the media, but people have been using forms of the ASP for centuries. By looking at one of these existing models and seeing how simple they are, you can gain a great deal of knowledge about Internet ASPs. An airline is a classic example of a non-Internet ASP, and is extremely simple to understand. It therefore makes a great starting point into your understanding of ASPs.

Almost all Fortune 1,000 businesses, as well as many small businesses, use airlines extensively. Many individuals also fly frequently for business and pleasure. Yet the number of businesses and individuals that own their own airplanes is extremely small. Instead, we rely on airlines to provide travel services to us on a per-use basis.

The main reason for the lack of plane ownership is the extremely high cost of entry. Let's say that you would like to own and operate your own jet. Here are some of the costs involved:

- You have to purchase the jet. Jets cost millions of dollars.
- You have to maintain the jet.
- You have to hire people to staff the jet -- a pilot, for instance, is someone you will need, and pilots are extremely expensive.
- You have to hope that the jet is in the right place at the right time for the people who need it. If not, you need to move the jet around at a high cost in terms of fuel, maintenance, etc.

In almost all cases, these costs are so high that, compared to the cost of individual airline tickets, they make no economic sense. Even the most intrepid traveler who flies 52 weeks out of the year would spend at most $2,000 per week ($104,000 per year) on airline travel. That amount of money would not even cover the cost of the pilot, not to mention the cost of the plane, fuel, maintenance, support, etc. involved in owning and operating a private jet. A private jet only makes economic sense in two possible cases:

- You are moving a group of people around frequently and in unison.
- The value of the people flying is so great that it washes out the cost of operating the jet. For example, if you have a group of executives whose value to the company is $2,000 per hour (for example, a CEO making $4 million per year), then obviously you want to waste as little of this group's time as possible. You also want these people to be as relaxed as possible so they can work optimally. In cases like that, a private jet may be well worth the money.

These two cases are extremely rare, hence the rarity of private jets. Note also that people who own private jets frequently travel between the United States and Europe on the Concorde. The Concorde is an ASP for high-speed European travel. No company could justify the cost of owning and operating a supersonic jet.

Airlines are classic ASPs because they give you and/or your company a choice. You can own and operate your own jet, or you can charter a jet from an airline when you need one (see, for example, How NFL Equipment Works to find out how an NFL team uses chartered jet service), or you can pay a very low incremental cost to fly each time you need to travel (and share the cost of owning and operating the jet with hundreds of other passengers on the plane).

The "pay a low price each time you use it" versus the "buy the service outright" option is a common feature of Internet ASPs, too.
There are many other ASP-like models that most of us use every day. For example:

- Shipping companies - Instead of maintaining your own distribution network for packages, you pay a low incremental fee to ship a package with the post office, FedEx or UPS. BMW and McDonalds are examples of companies that do so much shipping that they actually own and operate their own truck fleets -- but this are a rarity.

- Telephone companies - It would be extremely difficult for a company to justify the cost of owning and operating its own nationwide fiber optic network, so we all pay an extremely low incremental cost for each minute of long distance time we use.

- Power companies - It would be possible for each homeowner and business to generate power, but not for 10 cents per kilowatt-hour. Therefore, it makes sense to purchase power from a power company that distributes the high capital cost of a power plant across all of its customers. Some companies -- especially companies that deal in forestry products -- can actually generate their own power affordably because they have a source of free fuel or waste heat from some other process within the company.

There are cases where we do not go the ASP route. For example, a huge number of Americans own and operate their own automobiles instead of using the ASP called "public transportation." Most large businesses can justify the costs of large copying machines, while smaller companies rely on the ASP called Kinkos.

The point of all this is simple -- ASPs are all around us in many different forms. We choose whether or not to use ASPs based on economic factors that are driven largely by our frequency of use and the cost of entry and maintenance.

2. **Defining an Internet ASP**

Even though airlines fit the model for an ASP, we generally do not refer to airlines as ASPs. The terms "ASP" and "Application Service Provider" are applied specifically to companies that provide services via the Internet. In most cases, the term ASP has come to denote companies that supply software applications and/or software-related services over the Internet.

Here are the most common features of an ASP:
- The ASP owns and operates a software application.
- The ASP owns, operates and maintains the servers that run the application. The ASP also employs the people needed to maintain the application.
- The ASP makes the application available to customers everywhere via the Internet, either in a browser or through some sort of "thin client."
- The ASP bills for the application either on a per-use basis or on a monthly/annual fee basis. In many cases, however, the ASP can provide the service for free or will even pay the customer.

3. **Advantages of ASPs**

The ASP model has evolved because it offers some significant advantages over traditional approaches. Here are some of the most important advantages:
- Especially for small businesses and startups, the biggest advantage is low cost of entry and, in most cases, an extremely short setup time.
- The pay-as-you-go model is often significantly less expensive for all but the most frequent users of the service.
- The ASP model, as with any outsourcing arrangement, eliminates head count. IT headcount tends to be very expensive and very specialized (like pilots in the airline example), so this is frequently advantageous.
• The ASP model also eliminates specialized IT infrastructure for the application as well as supporting applications. For example, if the application you want to use requires an Oracle or MS-SQL database, you would have to support both the application and the database.

• The ASP model can shift Internet bandwidth to the ASP, who can often provide it at lower cost.

One thing that led to the growth of ASPs is the high cost of specialized software. As the costs grow, it becomes nearly impossible for a small business to afford to purchase the software, so the ASP makes using the software possible.

Another important factor leading to the development of ASPs has been the growing complexity of software and software upgrades. Distributing huge, complex applications to the end user has become extremely expensive from a customer service standpoint, and upgrades make the problem worse. In a large company where there may be thousands of desktops, distributing software (even something as simple as a new release of Microsoft Word) can cost millions of dollars. The ASP model eliminates most of these headaches.

4. Examples of ASPs

ASPs come in all shapes and sizes. One way to understand ASPs is to look at them from several different angles using real-world examples.

I. Simple ASPs

If you were to start a small business today, you would probably begin by contacting three or four extremely common and largely unnoticed ASPs:

• A Web hosting company - Companies like Verio and WebHosting.com provide a classic ASP scenario -- virtual Web hosting. These companies provide hardware, software, bandwidth and people to host Web sites for companies and individuals. Typically, they charge something like $15 to $30 per month for the service, and may host hundreds of accounts on a single machine.

• An e-mail provider - A Web hosting company usually provides some sort of e-mail service with your Web hosting account. There are two other alternatives:
  • Free services such as Hotmail or Yahoo! Mail
  • E-mail server ASPs who run exchange servers, POP servers or IMAP4 servers and distribute them on a monthly-fee basis - For example, a company in the Raleigh area called Interpath offers a complete e-mail solution at a rate of $8 per month per account (as of 4/10/2000).

  The advantage of the second approach is that the e-mail address uses your company's domain name.

• A fax provider Efax provides a free fax service that delivers faxes to your e-mail box. This is a classic example of a free ASP.

The huge advantage of using these ASPs is the fact that you don't have to do anything to get started. Five years ago, a small business looking for these services would have needed to:

• Purchase Internet connectivity and a router
• Purchase one or more servers for the Web server software, e-mail software, etc.
• Hire a person to install and administrate the software
• In the case of a fax machine, purchase the fax machine and a separate incoming line for it
Those are tremendous hurdles. Now, all of these services can be ordered and delivered on the same day, and the monthly cost for all three is probably less than $50 per month. The latest product category to enter the list of start-up ASPs is **eCommerce Storefronts** -- a storefront might cost $200 to $400 per month. The other thing to note is that ASP versions of these services will be significantly better than anything a small business owner can afford to provide.

For example:

- In the case of Web hosting, the provider will normally have a huge amount of available bandwidth, and the bandwidth will be redundant at several levels.
- If there is a problem, trained staff on site 24 hours a day will fix it immediately.
- If you need more capacity, it is available with a phone call and a small adjustment of the monthly fee.
- The ASP will backup the data on a regular basis and is responsible for disaster recovery.

No small business could afford that level of service with a home-grown server infrastructure.

II. **Traditional ASPs**

The "traditional" ASP sells a large, expensive application to large enterprises, but also provides a pay-as-you-go model for smaller clients. A typical example might be ad-serving software or auction software for a Web site. For example:

- **Engage** offers ad-management software for Web sites. The software can be purchased on a yearly license costing tens of thousands of dollars per year. In addition, the software requires an Oracle database for the software to use. If the Oracle database is already installed and running in-house, then that is no problem, but if not it is a significant hurdle. The alternative is to let Engage manage the software as an ASP and pay Engage a CPM (cost per thousand) price for the service. Unless you are serving millions of ad impressions per month, the ASP model makes tremendous economic sense.
- **DoubleClick** (along with many similarly positioned companies) is essentially an ASP that offers advertising software plus an advertising sales force. What is so interesting about this ASP approach is that the ASP actually pays the customer!
- **OpenSite** is a leading supplier for auction software. You can purchase its software and operate it with a database, or access the software using an ASP model.

Nearly any piece of expensive software, including giant applications like SAP, PeopleSoft and Oracle, now comes in an ASP version to allow these companies to reach smaller customers affordably.

5. **Things to Ask a Prospective ASP**

ASPs today offer nearly any service a company might need. Many of these services (like e-mail, Web hosting, ad serving, invoicing and bill delivery, payroll, etc.) are mission critical. It is therefore important to make sure that the ASPs you choose will handle your information and relationship in a mission-critical way. Here are a set of questions you should ask any ASP:

- **How do customers access the software?** Is it through a browser or an application? If it is through a browser, how does the user experience feel?
- **How are customer service issues resolved?** If you (or employees) have questions and/or problems with the software, what happens? Does the ASP provide training?
• **How secure is the data?** You want to find out about internal security policies with ASP employees, passwords and access reports to protect your employees, **firewall** and other safeguards against external attack, and things like tape backups to handle hardware failures.

• **How secure is the connection between the ASP and the user?** Data flows between the ASP and the user whenever the user accesses it. Is it secured by **encryption**, a **VPN**, proprietary techniques or some other system?

• **How is the application served?** Is your data on a dedicated machine or a shared machine? Both techniques are common and you often have a choice (with dedicated service being more expensive).

• **How does the ASP handle redundancy?** If a machine fails or an Internet pipe goes down, what levels of redundancy are in place to keep your servers online?

• **How does the ASP handle hardware/software problems?** If a **hard disk** fails or the application hangs, what are the policies in place around recovery?

• **How does the ASP handle a disaster?** If the building were to burn down or a **hurricane** came through, how would the ASP handle the complete loss of the facility? How long would it be before the ASP restored service?

• **Who owns the data?** Obviously, the customer should, but this fact should be stated in the contract.

• **How can I get the data out if I choose to select a new ASP two years from now?** This is a tricky question on more complicated applications, and one that bears some thought for mission-critical applications.

• **How can I move data between existing applications and the ASP?** For example, if you have a home-grown ledger system and want to move data back and forth to a billing ASP, how would that work? Many ASPs have already thought of this and handle it very well.

### 5.3 Management of End-User Computing

#### 5.3.1 Levels of End User Computing

It is fairly straightforward to identify the consumers of a delivered computer system; these are the operators of an MIS, the sales order entry clerks for instance, whose sole or main job is to operate system. These consumers, or end-users, can be distinguished from the creators of the systems. These developers are the IS/IT professionals whose sole or main role is to develop systems. For many years this two-way split of consumer/creator served to classify the people who were involved with IS/IT. It did not preclude user involvement in systems developments, in the sense that the creators sought their requirements and preferences when making the development decisions.

1. **By Skill and Job Content**

   Of more value than a two-way switch is to catalogue those involved in systems by their technology competence and the nature of their job content. Rockart and Flannery offered a **six-level continuum** for classifying all those involved with IS/IT. Although this continuum classifies all end-users, not all levels represent end-user computing since level 1 and level 6 are our old friends the consumer/creator extremes. The six levels are:

   1. **Non-programming end-user.** The “traditional” user of IS/IT. These are the operators of the systems developed by others (those developers can be from level 3 / 4 or 6). This category is the sales order entry clerks whose support needs are much focused, specific system training and fault fixing, time efficient support. This level of end-user is still widely found since large scale
corporate systems still widely exist. These users do not program in any way and their use of systems is through a strictly defined set of procedures or menus.

2. **Command level end-users.** These are the users of a “raw” package, which they will often do along with operating pre-written systems. This level of end-user has some knowledge of the application package, perhaps enough to use it to integrate data from several sources or to write DBMS ad hoc queries. This level of end-user may delve into the operating system and is typically a knowledge worker, perhaps one who needs to generate reports drawn from the systems operated by (1). This level of user requires development support and training and is willing to learn enough to enhance the performance of their day-to-day job, be it in personnel, marketing, or whatever.

3. **Programming level end-users.** These are sometimes called “power users” since they can create systems for their own use. They develop their own applications, some of which are eventually used by other end-users. This programming is very different to the “traditional” programming of the IS/IT professional since it will be done in the high level world of application packages or 4GLs. This level of user will tend to develop systems for use by themselves or their immediate workgroup although the systems so developed may move into wider currency. This is typically the knowledge worker who has great depth of knowledge, though in a more restricted sphere than (5) or (6). This is the accountant who knows far more about the spreadsheet than the IS/IT department does. This level of user needs methodology support and training.

4. **Functional support personnel.** These are the functional project groups. They are the decentralized IS/IT groups who routinely develop systems for use in that one business area. There are similarities with (3) but tend to be familiar with a broader range of development tools. This user level provides support and training but only on the systems they develop and need specialist training and support themselves. The main difference between levels (3) and (4) is in their self-perception. A level 3 user would see themselves as an accountant using IS/IT, whereas a level 4 user would see themselves as IS/IT people developing accounting systems. This group may have another role as engineer, financial analyst, etc, and there IS/IT role may have grown informally though it is nonetheless important.

5. **End-User support personnel.** These exist solely to support others. They can be targeted at helping any/all of levels 1,2 or 3 in their IS/IT tasks and in offering training, advice, help in choosing application tools and development of problem solving to levels 2 and/or 3. This category of end-user is almost never going to develop systems for use by others though, of course, they may create systems for their own group’s use, for instance time recording and monitoring systems. When they are engaged in such activities they are acting as level 2 or 3 end-users and may themselves need end-user support and training to levels 1,2 and 3 and across the full range of operation and development tasks. They, therefore, require complex training and support themselves since there is a need to train the trainers and support the supporters. In addition, they may provide some aspects of training and support to level 4 end-users or even level 6 end-users, for instance when those levels are using tools, such as word processors, that are more normally regarded as end-user computing packages. These people are often centrally located in an Information Centre.

6. **Data processing programmers.** These are the “true” developers. They have a lot in common with levels 3 and 4 since they will need to encompass the depth of level 3 and the breadth of level 4. Whilst this category of end-user is typically less business aware than level 4, they are likely to be more concerned with, and hence more skilful at, infrastructure issues such as:
   - Capacity planning
   - Development tools and methodologies
   - Standards and connectivity
   - Network management and efficiency

This level of user is very rarely self-taught as level 3 might be. This level represents the staffing of the data centre. One of the most powerful features of classifying IS relationships in this way is that the continuum reflects movement, and so:
2. **By Control**

An alternate way of looking at the nature of end-user computing is to look, not at job content and technology skill, but at the level of end-user autonomy. Four levels of this can be defined:

1. **Level A, No discernible end-user autonomy.** This is the system operator again since the IS/IT function has responsibility for, and authority over, the system. The level A user is in a “take it or leave it” relationship with the system.

2. **Level B, End-user input but not controls.** This level of end-user may specify the required system so, in that sense, is responsible for its nature but the IS function remains responsible for developing and maintaining it.

3. **Level C, End-user selection and operation.** This level of end-user is the first of what is usually considered to be end-user computing since the measure of responsibility extends to the full selection and use of the system. This control may be through the choice and use of an application package. The operational authority and responsibility are in the end-user’s hands.

4. **Level D, End-user development.** This level of end-user holds total control over the development as well as the operation of the system.

Only levels C and D would normally be regarded as user controlled computing. There is a very useful analogy to transport types that is frequently used to explain these differences, it is:

<table>
<thead>
<tr>
<th>Transport Type</th>
<th>Level of End User</th>
</tr>
</thead>
<tbody>
<tr>
<td>Train</td>
<td>A</td>
</tr>
<tr>
<td>Taxi</td>
<td>B</td>
</tr>
<tr>
<td>Self drive car</td>
<td>C</td>
</tr>
<tr>
<td>Self build car</td>
<td>D</td>
</tr>
</tbody>
</table>

When taking a train, customers collectively have an impact, but individually must go by the route and at the time dictated by Railway Company. By taking a taxi, a customer can select the precise start and end point and time of the journey but not how the driver will achieve it, the taxi driver is free to decide upon the detail of the route and the speed of travel! When self-driving a car, one can choose when, where and how to make the journey. Building (or servicing and maintaining) the car as well gives total independence and one can go when, where, how and in what style one chooses.

3. **By Maturity**

An important development of Nolan’s stages of growth model was proposed by Huff et al when they suggested that similar stages of maturity are gone through by the “new” technology of end-user computing. Their model categorizes, not the users of user control computing, but the processes of growth in user control computing. This model is an important one since it leads to considering the differing issues in managing, both user control computing and its growth. User computing becomes more sophisticated over time, and it was also suggested that the maturity of the applications that are the tangible output of user controlled computing form the main measure of the maturity of user controlled computing. This maturity of
applications can be best judged by the nature of the integration of the applications. Unlike Nolan’s model, that of Huff et al has five stages, and these are:

1. **Isolation.** Where there is little or no exchange of data between applications. The application that result from these pockets of user control computing are best thought of as learning rather than business tools and the organizational dependence on them is low.

2. **Stand-alone.** Whilst the applications are “islands” and so there is no integration of applications, these stand-alone applications are more critical to the performance of the job. This dependence is restricted, however, to just the individual’s immediate area. The stand-alone island proliferate to the point where many businesses depend upon sequences of such applications but the data is being re-keyed at each point.

3. **Manual Integration.** During this stage the user controlled computing developments require significant exchanges of data but this needs manual intervention to happen. The links may be by physical transfer of discs or the logical transfer of files over networks or between accounts. The need for this level of integration, even though its operation is not automated, forces the issues of standards and development discipline to the attention of those managers responsible for, and engaged in, end-user computing.

4. **Automated Integration.** The focus shifts to automating the transfer of data, and integration is considered during the applications’ design. The burden of manual intervention for every download or data exchange is lifted by the automation of the connections by the data administrative function. This is the dawning of true integrated systems but ones that still require end-user knowledge of location and structure of the required data.

5. **Distributed Integration.** The distributions of location and structure disappear at this stage since the applications can be written without having to navigate to the required data. Irrespective of the physical distribution of data it can be accessed as if it was in a central warehouse store.

### 5.3.2 Risks in User Controlled Computing

There are, perhaps, not so much disadvantages as risks associated with poorly managed user controlled computing. User controlled computing is like any other emerging technology, it is associated with a number of risks. The organizational risks as associated with user controlled computing by the stage in the (user) application development cycle can be summarized as:

- **User controlled computing may solve the wrong problem.** Since users are not analysts they may incorrectly define the problem, indeed there is a tendency for UCC to alleviate symptoms rather than address root problems. Support and management structures need to deal with the issue of problem solving.

- **Waste.** User controlled computing runs the risk of wasting computer time, IS/IT resources, user time, and, in short, the organization’s resources. Waste can only be defined as such resources being used for no gain; management and support structures must ensure that gains are made.

- **Development risks.** Even when the correct problem is being addressed an incorrect solution may be used. User controlled computing is notorious for not involving error checking and testing. Management and support structures must ensure appropriate levels of accuracy.

- **Incompatibility.** When the right problem is efficiently and accurately solved there is still a risk from the potential incompatibility of different solutions created within the same problems area. Support and management structures must identify whether compatibility is critical and, if it is, ensure that it happens. The existence of these risks is not an argument for eradicating all
user controlled computing to remove all risk, that would stifle all development. It is, however an argument for being aware of, and managing, those risks.

5.3.3 Approaches to Managing User Controlled Computing

User controlled computing allows business personnel to control the satisfying their own needs. The availability of downsized technology makes end-us computing easy, it doesn’t always make it effective. Many use controlled computing applications become organizational critical and/or multi-user that fuels the drive towards appropriate levels of standardization, control, training, security, etc. Managerial approaches must be selected that make end-us computing business effective; this is generating greater benefits than the resources it consumes. Since the resource consumption is very large the benefits must be as well.

Differing management approaches to user controlled computing are required. The selection of the appropriate policy will depend upon stage growth, level of user skill and job content and organizational objectives for end-user computing. Along with categorizing stages of maturity of end-us computing, Munro et al suggest that there are two variables to be managed during the growth of end-user computing. These two management variables can be altered relatively independently of each other, and are:

- The rate of expansion of end-user computing
- The level of control over end-user computing activities.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Selection and Maintenance</td>
<td>The IS/IT staff select the types of hardware that can be purchased and maintain it</td>
</tr>
<tr>
<td>Software Selection</td>
<td>The IS/IT staff select the types of end-user tools that can be purchased and support them</td>
</tr>
<tr>
<td>Training</td>
<td>The IS/IT staff provide training for end-users on the selected software and hardware</td>
</tr>
<tr>
<td>Data Availability</td>
<td>End-users control their own data, and share it using local area networks. Corporate data can be accessed under guidance of IS/IT staff</td>
</tr>
<tr>
<td>Data Security</td>
<td>Corporate data access limited to user’s need and “read only”</td>
</tr>
<tr>
<td>Systems Development</td>
<td>IS/IT staff help end-users with analysis and design where necessary and ongoing development support through help lines</td>
</tr>
</tbody>
</table>

The rate of expansion can be managed by making information easier or harder to get; hardware and software easier or harder to get; more or less support available; or altering the costs borne by the user community. The level of control can be managed by determining the extent of the restrictions on free selection of hardware and software products; the policies on micro/mainframe use; the restrictions on free access to data; the restrictions on the acquisition process.

A fast rate of expansion is concerned with seeking most of the advantages of user controlled computing whilst strong control is concerned with getting least of the disadvantages. Munro hence suggests that high expansion and high control is the “mature” management strategy, combining as it does the best of both worlds.

Dark suggest that there are actually three strategies for managing user controlled computing. These three are:

- **User Autonomy.** Where the users are fully responsible for purchases, developments, budgets and support.
• **User Partnership.** Where some responsibilities are shared, for instance the setting of budgets, but purchases must be to corporate guidelines and support and advice is available. This definition roughly equates to Information Centre approach.

• **Central Control.** Where IS/IT controls the budgets and the purchases and developments are joint ventures that are significantly supported by IS/IT.

### 5.4 Financial Analysis and Control

Managing the increasing risks and the costs of IT needs greater control today and is subject to more pressures. Implementing IT Strategies is a balance between the direct costs, indirect costs and benefits. While tangible costs and benefits are easier to manage, there are increasingly complex intangible costs and benefits.

#### 5.4.1 Limitations of Cost Benefit Analysis

This section provides a more detailed analysis of the costs and benefits that can be obtained from Information Systems, and attempts to explain the true costs of IS systems along with the benefits such as competitive advantage, which conventional CBA has difficulty in valuing.

All firms will have some method of selecting which projects to proceed with. These methods in turn become the systems that managers use to justify their projects. At the centre of all of these systems will be the premise that the benefits should exceed the costs; in other words a cost benefit analysis. There are several inbuilt difficulties with cost benefit analysis and return on investment techniques, often these can be overcome but they present particular problems when cost benefit and return on investment are used in the evaluation of information systems.

#### 5.4.2 Checklist for IS costs

There are two classes of cost associated with the introduction of new or additional information systems. In the first are those costs that are directly associated with the new system such as hardware, software, programmers’ salaries etc. In the second category are those that occur during the implementation of the system, such as lowering of efficiency of a user department whilst staff are not fully focused on their primary tasks. The first category are called *technology costs*, the second are *organisational costs.* Cost benefit analysis also covers *intangible costs* and *opportunity costs*.

1. **Technology costs** -
   are those that can be seen as relating to the information system.

Hochstrasser and Griffiths offer a checklist that assists organisations to identify, quantify and evaluate IS costs. It covers:

- Hardware - not just the processing hardware but also all the peripherals. Although they are visible, the increasing dispersal of these items makes them difficult to locate and audit.
- Software - the cheapest solutions are off-the-shelf packages, but the specification and evaluation of the software may be significant. In-house developments can account for large and unknown costs.
- Installation - some require external expertise, which must be included in the cost. Also the data entry or data conversion costs need to be considered.
• Networking - network hardware, software and management all incur costs over and above any application using the network.
• Environmental - includes all the human and physical environment of IS e.g., safety, health, legal costs, wiring, furniture, air conditioning.
• Running costs - includes electrical power, communication costs and subscription fees for any external data services.
• Maintenance - these costs can be planned through service and maintenance contracts or provided in-house.
• Security - includes those measures, taken to reduce the danger from deliberate or accidental damage to elements of IS, that must be allowed for in the costs.
• Training costs - the real extent of training costs e.g., background education, specific training, ongoing support and updates will need to be documented and brought into the costs.

Difficulties arise because the organisation will have a variety of current information system costs, which will play a part in the new system. Furthermore, some of the costs that will accrue, as a result of the project, will relate to items that can be applied to subsequent projects. These items can be considered as additional to the organisation's information systems infrastructure. Examples of this kind of item are:
• The hardware and software required to connect the organisation’s existing personal computers together into a local area network.
• The establishment of the communication facilities between remote offices to form a wide area network.
• Database management software.
• The acquisition of skills in a new programming language.

Improvements to the information system's infrastructure will normally be proposed as an enabling improvement required by a specific information system proposal, although there will be occasions when they are proposed separately. In either case, management should separate the costs of the infrastructure and the particular information system and then evaluate the value of each separately.

2. Organisational costs -
should be assessed in monetary terms where this is possible, but more normally should be assessed in terms of the effect on competitiveness. Hochstrasser and Griffiths include incompatibility costs, new salary structures, transitional costs and management costs in this category.

3. IS Balance sheet

What can loosely be referred to as auditing the IS investment involves identifying all visible and hidden costs and valuing the past IT investments. It has been suggested that this process can be helped by creating an IS balance sheet. Even though most of the valuable elements of IS, the data and software, cannot be counted as assets for tax purposes, they still add to the value of the organisation. The following example, used by P Keen in *Shaping the Future*, shows the IS asset worth of a bank in the US.
### IS assets

<table>
<thead>
<tr>
<th>IS assets</th>
<th>Asset worth ($Million)</th>
<th>Guidance on how the figure is arrived at</th>
</tr>
</thead>
<tbody>
<tr>
<td>Centrally managed computers</td>
<td>120</td>
<td>This is the most visible element but only represents 5% of the real IS assets for this example.</td>
</tr>
<tr>
<td>Distributed computers</td>
<td>84</td>
<td>These will usually be PCs and can often account for more spending than centrally controlled equipment.</td>
</tr>
<tr>
<td>Network equipment</td>
<td>105</td>
<td>They appear across a number of budgets.</td>
</tr>
<tr>
<td>Distributed telecomms.</td>
<td>59</td>
<td>The value of the local area networks.</td>
</tr>
<tr>
<td><strong>Total hardware</strong></td>
<td><strong>368</strong></td>
<td></td>
</tr>
<tr>
<td>Application development software</td>
<td>420</td>
<td>Both software figures are little more than guesses, because the bank does little to track the value of the developments.</td>
</tr>
<tr>
<td>Other, including PC software</td>
<td>68</td>
<td>The replacement cost was estimated at three times this figure.</td>
</tr>
<tr>
<td><strong>Total software</strong></td>
<td><strong>488</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Data resources</strong></td>
<td><strong>1200</strong></td>
<td>This is the estimated cost of salaries, processing, and storage media to create the on-line resources.</td>
</tr>
<tr>
<td><strong>Total IS assets</strong></td>
<td><strong>2056</strong></td>
<td></td>
</tr>
</tbody>
</table>

Looking at IS in this asset appraisal way is part of the critical transition from computer management to information management. If the perception is that it is just a computer that is being managed then everything other than hardware becomes viewed as its operating costs, or expenditure, and this causes the business value of data and software to be hidden. The value of IS assets needs to be acknowledged so that management accord it the attention it deserves.

### 5.4.3 Value

In the previous section the concept of benefit was expanded to value. Value was defined as 'the sum of the discrete benefits and of improvements in business performance factors'. In order to help management in the selection of information projects it is helpful to break down the total value encompassed in the definition above into categories.

The first part of the definition of value includes reference to the sum of the discrete benefits. It is discrete benefits which return on investment is best suited to measure. The following are examples of changes arising from the introduction of an information system that are sufficiently tangible to have a monetary measure placed upon them:

- Increased capacity of some aspect of operations whilst holding variable costs constant
- Reduction in labour time to carry out an operation
- Reduction in skill to carry out a task
- Reduction in the cost of supervising an operation
- Ability to collect cash more quickly
- Reduction in stock levels
- Reduction of occasions when a sale is lost due to an item being out of stock
- Reduction in loss of stock by means of improved control
- Reduction in the number errors
Note how most of these tangible benefits relate to taking costs out of an organisation.

The intangible benefits that are difficult to measure could include the following:

- Gaining competitive advantage
- Avoiding competitive disadvantage
- Change through innovation
- Supporting core business functions
- Improved eg, more timely, management information
- Improved customer service
- Improved internal and external communications
- Improved product quality
- Job enhancement for employees

### 5.5 Accounting for IS Costs

#### 5.5.1 Costs incurred in delivering information system

An organisation can incur many different costs in delivering information to its directors, employees, customers and suppliers. These costs can be summarised as follows:

(a) One-off or capital costs

These will include

- Hardware purchase
- Specialist accommodation for computers
- Wiring for networks
- Installation costs such as new desks for employees

(b) One-off revenue costs

- System development costs including programmers’ salaries, system analyst fees, costs of testing the system, cost of converting files etc.
- Redundancy payments (if any)
- Hiring of new specialist staff
- Staff training

(c) Ongoing costs

- IS system staff wages
- Help desk and Information Centre salaries
- General running costs
- Subscriptions to external information providers such as news services
- Data transmission costs (telephone line rental, Internet access fees etc.)
- Consumable materials such as floppy disks, CD’s, paper etc.
- Power for computers, VDU’s etc.
• Any rental costs for hardware not initially purchased
• Hardware maintenance and support contracts
• Software maintenance and support contracts
• Standby and backup arrangements
• Regular staff training

All of these costs will have to be accounted for in some way within the organisation.

There are other reasons for re-charging costs of the IS department, apart from re-charging the tangible costs (that is the costs that result in direct expenditure compared to intangible costs such as low staff morale) incurred by that department. The charging system must also accommodate the following objectives:

- **Improved financial control for the IS and other user departments.** Actually charging for the service provides an emphasis for the IS department to give good customer service. Similarly, the fact that the user department is paying for the service will mean that the user department will be looking for value for money in the service being provided.

- **Encourage the correct use of IT.** Providing a charge enables the user department to decide whether or not to actually use specific services being provided by the IS department. If there were no charge for any service, then the use of the service, and the importance of that service to the department would not be regulated. Providing a charge limits the use of any particular service to the parts actually required.

- **Improve morale and motivation of staff.** Placing a charge on a service helps staff to appreciate the cost of either providing or obtaining that service. User departments will appreciate the cost implications of their IS choices, and hopefully recognise that unlimited service cannot be provided at effectively zero charge. Also, the staff in the IS department will be motivated because they will be earning income from providing the services and will also (hopefully) provide a better service because a charge is being made.

Given that some costs, like the tangible costs, are essentially fixed, and costs for project work such as providing services for bespoke application development, are essentially variable to the user departments, a two-tier costing structure may arise. Fixed costs are charged separately or not at all and the variable costs charged as incurred. However, before making that decision, we need to investigate the charging methods available.

### 5.5.2 Accounting for costs of an information system

Having determined what the costs of providing an information system can be, the next sections investigate the different ways in which those costs

The costs of an information system can be accounted for in three main ways:

- IS is a non-recharged cost centre.
- IS is recharged at cost.
- IS is recharged above cost, to make a profit.

The advantages and disadvantages of these methods are discussed below.
1. Non-recharged cost centre

Advantages:
- Simple and cheap. No apportionment of the IT costs is needed.
- May encourage consumer driven demand for innovation. Users demand better systems knowing that these will have no cost effects on their departments.
- Users can concentrate on the main activities of their departments, as they do not have to worry about IT costs.

Disadvantages:
- If a service is free to users, they may demand more and more even when it is not economically justifiable for the organisation to supply more.
- If not recharged fewer people are likely to complain if the service is inefficient and too expensive. The IT department will have little incentive to control costs.
- If not recharged, users can find it difficult to request changes in the service level. They fear the response 'You are getting this for free, be glad with what you get'. Ultimately user departments know what level of service they need and the IT department should be responsive to their needs.
- Performance measurement of departments is distorted if all costs involved in the operation of the department are not accounted for.

2. Recharged at cost

Advantages
- Simple as no mark-up needs to be agreed.
- Depending on how the charge-out is made, users do feel the effects of their demand on and use of IT.
- Users will complain if it appears that the IT costs imply that that department is inefficient and expensive in its supply of IT services.

Disadvantages
- If the IT department can charge out all costs, there is no incentive for it to be efficient. A better arrangement would be for it to charge out budgeted costs or standard costs only. That way, any cost overruns in the IT department would stay there and the IT department would have to explain them.
- If recharging is not related to IT usage, users will feel aggrieved. They will feel that a central cost is being arbitrarily passed on to them from a monopoly supplier.
- Even when attempts are made to charge out costs according to usage, it can be very difficult to decide on a fair basis. Some costs will be relatively easy to charge out. For example, analyst's time would be the basis for charging for development work. However, many of the costs will relate to the fixed costs of the IT department and some type of rate per hour of processing may have to be assessed.
3. Recharged at a mark-up

Under this basis, the aim would be to charge users with an amount approximating to market rates.

Advantages

- The IT department should be able to make a profit. This should be motivating for IT managers.
- Making a profit depends on being efficient with costs and offering services that users want to buy and which are competitively priced. The IT department should therefore develop a more commercial outlook.
- Users can compare the in-house cost to costs of hiring outside suppliers. This will help to keep the IT department efficient - provided users have the freedom to contract outside if that is cheaper.
- Users can buy more services if they want to. The IT department therefore becomes the mere supplier of services; the users determine what services they want. The IT department should therefore be more responsive to users’ needs.
- Performance measurement of user departments should be fairer if they have to bear the full commercial costs of services.

Disadvantages

- If there is no suitable outside supplier, it can be difficult to decide on the charge-out rates that should be used. User can be particularly aggrieved if they feel that the IT department is charging out at excessive, monopolistic profit margins.
- Buying from outside can be disadvantageous to the organisation as a whole: the IT department's fixed costs still have to be covered.
- Although a true market may exist for some services (such as specific consultancy projects), it may be impracticable for one department to subcontract to a third party if other departments do not. Most applications are integrated nowadays and it is important to be able to retrieve and use data from many departments.

4. Cross charging of costs including shared infrastructure costs

The charging systems can become more complicated where parts of the IT systems are shared between departments, as it is difficult to determine individual usage of those shared resources. To provide some estimation of usage prior to charging, some or all of the following activities can take place:

- Review of network traffic to establish either the number of messages or amount of data being transferred over the shared resource by each department.
- Checking the number of users of each shared resource and allocating charges based on number of users.
- Checking the amount of disk space used on network servers and then allocating charges based on this measure.
- Logging the number of telephone calls made to the help desk and using these as a guide to use of resources and therefore charging alternatives.

Whatever method of charging is chosen, it must be seen to be fair, and incorporate an element of actual usage rather than appear to be an arbitrary amount.
5.5.3 Establishing information systems function as a separate entity

Another alternative to providing IS support within an organisation is to establish the information systems function as a separate entity. This is taking the idea of making the IS department a separate profit centre one stage further. As well as being able to make a profit on the services being re-charged, the IS department would effectively be a separate legal entity and so would be run as a separate business. The IS support services would effectively be purchased by the main company as a separate service, in the same way that other goods and services would be purchased.

There is very little difference in this charging system compared to outsourcing the whole Information System support. The benefits to the user department include:

- Having an agreed contract with specific service standards set in advance of that service being provided.
- Agreeing a fixed price for the contract, again in advance of the service being provided
- Prices can be easily compared to other IS providers

The problems for the IS department include:

- Being able to set an appropriate price for all services in advance of provision
- The possibility of paying damages for breach of contract if the service is not provided

Before establishing the IS function as a separate entity, the organisation must ensure that the function is of a sufficient size and maturity to be able to provide this service. The company’s systems will also, normally, be established, so provision of IS support is seen more as a service than a necessity. Following the initial set-up of a system, IS support may be expected as a right, not as an additional service that needs to be paid for.

Whatever decision is taken, care is needed to ensure that the basis of making that decision is clearly stated, and that user departments are re-assured that they will be able to obtain the IS services that they require.
Chapter roundup

IS operations strategy generally addresses the following functional areas:
- Computer operations
- Controlling input/output of data
- Management of IS operations
- Control Function
- Planning and scheduling: Service level
- Job Accounting
- Scheduling
- Monitoring use of resources
- Problem management
- Program change control
- Quality assurance
- Technical support/help desk
- Librarian function
- Management of physical and environmental security

Practice Questions

**Q No.1** In your option would the IT Operations Strategy be a long-term plan or a short-term plan? Why?

**Q No.2** Within a single site, describe some of the ways that the site security can be improved.

**Q No.3** With respect to your personal and business life, identify what transactions that you participate in that may have resulted in personal data being held in a database. List at least 6 instances.

**Q No.4** Nasar & Co., a company that produces fabrics for export is restricted in its IT resources. Identify as many partners as you can with whom the IT Department might consider a partnership and describe the broad technology environment that might be adopted for each.

**Q No.5** Intranets have been heralded as a great new tool for organisations. Describe at least 4 benefits that an organisation might realise by employing an Intranet. State any assumptions that you have made about the organisation.

**Q No.6** There are many benefits of distributed data processing and many potential pitfalls. Describe at least 4 benefits and 4 potential weaknesses of using distributed systems.

**Q No.7** What do you think would be the benefits of rental or lease over outright purchase?

**Q No.8** You are an IT manager. Your mainframe computer is from a supplier, Cant Computers, who has been providing service to you for several years. You have made a decision that implies you need to upgrade and have received notification from your supplier that the cost to upgrade will be in the vicinity of Rs100,000. You immediately think – I will change suppliers and get a quote from another supplier, Butt Computing, for Rs 90,000 for similar specification.

Which supplier would you choose and why?
Q No.9) Desktop computing has introduced complexity and enormous hidden costs into the IT Manager’s budget in many companies. In your opinion, what which of the following do you think could offer the greatest cost benefits and why?

i) standardisation of desktop computers
ii) centralisation of purchasing

Suggested Solution

Answer No.1) Students should describe this Strategy as a tactical plan for implementing the IT Strategy. The Operations Strategy will cover a shorter term than the overall plan and will be a more detailed plan. It will address the priorities of IT acquisitions and installations to support the overall IT Strategic Plan and will guide the Operations Department in its activities.

Answer No.2) There are many answers to this questions and it really is a matter of appropriateness. Weighing up cost versus risk is critical. Some of the more common ways that the students might suggest include:

- Limiting physical access to the computer room
- Access codes for authorised personnel only
- Monitoring access using remote TV cameras
- Storing significant files and backup off site
- Ensuring an uninterrupted power supply and fire protection is in place
- Physical separation of development and operations staff

Answer No.3) You might wish to discuss this question in terms of the diagram on P528 of the text “Strategic Management & Information Systems”. Students could nominate many instances here including:

- Birth records
- University records and exam results
- Institute enrolment records and exam results
- Driving records
- Passport records
- Bank records, Credit cards and/or debit cards

Answer No.4) The students might identify many different partners for this example. Suggested solution might include:

- **Customers.** Using a website for reaching out to global customers might be a desired outcome so the IT Department might consider using an outsource provider for their services such as web development and hosting or could consider and ASP service.

- **Suppliers.** Adopting an online system with suppliers so that orders for raw materials, can be readily sourced when needed could help. This could be approaching suppliers to establish extranets with them or to develop an industry portal.

- **Government.** The IT department should consider forming a relationship with Government so that export, customs documents can be simply used and more effective communications forged.

- **IT Vendors.** Many IT vendors give partners direct access to their order systems which can be used without the need to develop costly systems.

Answer No.5) There are many benefits that might accrue with an Intranet. Student’s answers may include:
• Improved control over data. No replication and assigned responsibilities.
• Improved responsiveness to customers. Information may be accessed by all staff and the customer given an answer to their query immediately.
• Better staff efficiencies. Data is collected and entered only once and yet everyone can access the latest information. No need to run around trying to find out who has the latest information.
• Able to capture improved information about operations and information access and thus improve what information is being captured and how it is being used.

Answer No 6.) Students may have widely varied answers. The following is a suggested solution:

Advantages:
• User involvement. There is greater user involvement in distributed solutions.
• Availability. Confines the effects of computer breakdown to smaller segments and thus reduces the reliance on one computer.
• Flexibility and growth. Allows for phased approaches to upgrades and systems rollouts.
• More cost effective solutions able to be developed and implemented because this is normally associated with PCs.
• Responsiveness and productivity are increased. Smaller jobs, better understanding of the data.

Disadvantages.
• Maintenance and hardware problems not as easily diagnosed. Networks are more complex and there are more points for failure introduced.
• Controls. There is much less control over distributed systems. Backup and security issues in particular can be a problem.
• Integration of data and information is more complex. Data can become fragmented or not synchronised.
• Possible for costs to escalate as there are many costs that are hidden.

Answer No 7.) Student might suggest the following points:
• Capital is not tied up in IT which allows greater investment in the company’s main business
• Reduced risk of paying too much for IT. With costs decreasing for some technologies quite dramatically as it matures, there is a danger that the early adopters pay high prices and the late adopters pay far less.
• Less obsolescence. Rented or leased equipment can be quickly disposed of and there are greater opportunities for upgrading the configuration
• Improved performance. Depending on the performance clauses in the contracts, any hardware or software that is rented or leased can be disposed of or pressure put on the provider to improve service.
• Taxation advantages might exist.

Answer No 8.) Student answers should demonstrate an understanding of the associated costs with a capital purchase. Answers could be either depending on the arguments but suggested solution would be Cant Computers since a change to Butt Computing would involve not only the capital cost but also include many other flow-on costs such as:
• Reskilling the IT support staff for the new computers
• Changes to maintenance and support arrangements for computers
• Potential changes to systems and programs
• Potential changes for some users and training costs
• Need to investigate the extent of changes necessary for integration of the new computer with existing equipment
• Need for changes to disaster recovery plans

Answer No 9.) Students should demonstrate an understanding of desktop computing and the potential issues. Answers could include mention of the following:

**Standardisation** – if user departments purchase diverse computers in terms of specifications, operating systems and software then IT support becomes a major issue. In many organisations, these departments will still ring the IT department for support assuming that the skills and knowledge are there to support anything! Also software clashes can occur on different computers if the specifications are different and undermine any rollout of effective desktop tools. Standardisation means skills, tools and support can be managed more effectively.

**Centralisation of purchasing.** Many suppliers offer bulk discounts and discounts for their better customers. If each department buys from different suppliers, costs can be more overall. Also managing warranties and support becomes easier if managed centrally.
Introduction

Strategies for adopting eBusiness practices are supported by many products, technologies and types of systems. While this area is constantly changing there are some systems that are recognised by many companies as key strategies. We will look at some of those systems here but students are encouraged to research this topic further for new and emerging trends.

Study Guide

Supply Chain Management (SCM) (Study Text reference 6.3)
- Trading involves a number of partners across the supply chain. You might want to take an industry and talk about the supply chain for that industry as an example.

Enterprise Resource Planning (Study Text reference 6.4)
- Ask the students if any of them have experience with the more common ERP packages e.g. SAP, PeopleSoft and Oracle applications. Discuss how these packages are used and if there were any issues arising from the implementation.

Customer Relationship Management (CRM) (Study Text reference 6.1)
- Discuss the student’s understanding of the term. You might like to find some other examples of definitions and discuss those as well.

Sales Force Automation (SFA) (Study Text reference 6.2)
- Sales teams carry out 3 important functions – finding, acquiring and maintaining customers. You might like to talk about various ways of supporting the sales force using technology. For example, introduce the laptop, the palm pilot and mobile phone as simple examples of how technology may be applied to “automate” a mobile work force and the benefits it might bring to the organisation.

eBusiness Products (Study Text reference 6.5)
- There are literally hundreds of software and hardware products that lay claim to be eBusiness Products. Many of the products address only one specific part of the business or one particular function. Since this is a relatively new area, products emerge onto the market almost daily so the best place to research what it available is via the Internet.
6. **E BUSINESS ENABLING SOFTWARE**

6.1 **CUSTOMER RELATIONSHIP MANAGEMENT**

6.1.1 **Definition**

There are as many definitions for CRM as there are opinions as to what is going to happen in the stock market the next day. At its basic core, CRM entails initiatives that surround the customer side of the business. An example is initiatives wrapped around the customers in an effort to increase sales, improve customer service, add market share, enhance customer loyalty and reduce operating costs of sales and service.

**Key Term**

CRM is a business strategy comprised of process, organizational and technical change whereby a company seeks to better manage its enterprise around its customer behaviors.

It entails acquiring and deploying knowledge about customers and using this information across the various customer touch points to increase revenue and achieve cost reduction through operational efficiencies.

CRM is a corporate philosophy because it is a fundamental approach to doing business. That approach is to be customer-focused and customer-driven, running all aspects of your business to satisfy your customers by addressing their requirements for products and by providing high-quality, responsive service. The philosophy extends to support customer managed relationships (CMR) where the customer is in the driver’s seat, determining the rules of the relationship. Companies that adopt this customer-focused and customer-driven approach are, thus, customer-centric.

The inverse of customer-centric is product-centric. Can you think of any products that your company could never effectively sell? Innovative though these products may have been, they probably didn’t solve any customer problems or address any customer requirements.

6.1.2 **CRM Objectives**

The objectives of CRM are straightforward:

- Acquire new customers
- Retain the right existing customers
- Grow the relationships with existing customers

These are probably corporate business objectives, too, or at least corporate marketing objectives; but the way they are state and strategies to achieve them may not be sufficiently customer-focused. As a philosophy, customer-centricity drives to view the entire business from the perspective of customers. CRM implements the marketing, sales, and service business processes—the customer-facing and customer-touching business processes through which an entity interacts with its customers.
All of the business processes, and many business processes of suppliers and partners should provide critical support for CRM processes. This support is achieved through business process automation and application integration.

For example, the fulfillment system (or the supplier’s fulfillment system) must be integrated with the CRM system so that customers can find out when their orders are going to be shipped. Usually customers interact with direct sales representatives, contact center representatives, and Web applications. These interactions occur through a variety of touchpoints—the phone, face-to-face, a Web site, etc. CRM business processes have to support all these touchpoints, supporting a single and consistent view of your customers as well as a single and consistent view of the company.

A single and consistent view of your company is achieved by providing the same marketing, sales, product, support, and order information to the customers across all the touchpoints through which they interact with the entity. This consistent “customer experience” can be accomplished in the same manner as single and consistent customer information. It’s also a critical success factor for customer-centricity and difficult to achieve.

6.1.3 Impacts of CRM on Organizations

Risk management is either a very important or moderately important aspect of CRM projects. Why it so important? some of the impacts that a CRM initiative may have on an organization:

- Increased expectations from senior management to increase revenues, reduce costs, increase market share and increase business flexibility may put tremendous pressure on the organization and may potentially compromise the internal control structure
- Increased complexity of managing multiple channels, technologies, customer relationships and customer definitions
- Vital and confidential customer information may be transmitted and shared across new networks, systems and platforms
- Significant changes to the organization, attitudes and beliefs, placing heavy reliance on the organization’s employees for the successful adoption of the solution

These factors introduce many risks to the organization, for instance, the potential disruption of vital operations; violations to customer privacy and confidentiality; ineffective, inconsistent or inefficient processes; lack of internal business controls; poor customer service; incorrectly targeted sales and marketing efforts, non acceptance of new systems and processes; and security breaches.

6.1.4 CRM Applications

CRM is implemented by a wide range of applications that implement the three direct CRM processes—sales, marketing, and service—and the many business processes that support them. The applications that implement these business processes are considered “operational” applications. They are the applications that “do” the business, delivering offers, generating orders, and responding to customer requests.

CRM also has an analytic or decision support dimension. We call these applications customer-centric intelligence applications.

Illustration I shows these applications and how customers interact with them.
1. **Customer-Facing Applications**

The key, customer-facing CRM applications are **contact center**, **sales force automation**, and **field service**, described briefly in Table A.

We call these “customer facing” because your sales, fields service, and contact center representatives actually interact with your customers. Customer-facing CRM applications support those staff members.

<table>
<thead>
<tr>
<th>Customer-Facing CRM Applications</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact Center</td>
<td>Contact center applications are telephony applications that support marketing, sales, and service—all the CRM business processes. These applications implement telemarketing, telesales, and teleservice functions. Telemarketing is usually an outbound activity—the telemarketing reps contact the customers. Teleservice is typically an inbound activity—customers contact the support centre and speak with customer support reps. Telesales may be either an inbound or outbound activity. It presents product information and quotes to prospects and customers or responds to customer requests with product information and quotes.</td>
</tr>
<tr>
<td>Sales Force Automation</td>
<td>Sales force automation (SFA) applications support the selling efforts of the sales force, managing leads, prospects, and customers through the sales pipeline or sales funnel</td>
</tr>
</tbody>
</table>
Field Service Automation

Field service automation applications support the customer service efforts of field service representatives and service managers. These applications manage customer service requests, service orders, service contracts, service schedules, and service calls. They provide planning, scheduling, dispatching, and reporting of field service representatives for service calls.

Table A. The three key customer-facing CRM applications are described in this table.

2. Customer-Touching Applications

The key customer-touching CRM applications are campaign management, e-commerce, and self-service customer support, described briefly in Table B. We say “customer touching” because your customers interact directly with the applications rather than through a company representative.

<table>
<thead>
<tr>
<th>Customer-Touching CRM Applications</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Campaign Management</td>
<td>Campaign management applications automate marketing campaigns. They present offers to targeted leads, prospects, and customers on demand, on a schedule, or in response to business events through direct mail, e-mail, contact center, field sales, and Web touchpoints. Ideally, these applications should be able to record responses to offers.</td>
</tr>
<tr>
<td>Electronic Commerce</td>
<td>Electronic commerce applications implement marketing, sales, and service functions through online touchpoints, most typically the Web. These applications let sellers market products through online catalogs and associated Web content. They let customers shop for products through a virtual shopping cart metaphor and purchase the products in their shopping carts through a virtual check-out metaphor. Customers may also perform self-service support tasks such as order status and history inquiry, returns processing, and customer information management.</td>
</tr>
<tr>
<td>Self-Service Customer Support</td>
<td>Self-service customer support applications let customers help themselves to product support information, create service requests, manage information about themselves, and manage their orders.</td>
</tr>
</tbody>
</table>

Table B. The three key customer-touching CRM applications are described in this table.

3. Customer-Centric Intelligence Applications

Customer-centric intelligence applications are analytic applications that analyze the results of operational processing. Their results can be used to improve the efficiency and effectiveness of operational CRM applications.

Customer-centric intelligence (what we have, in the past, called Customer Intelligence) is the term we use to describe customer-focused analytic functions, but you might be calling these same applications business intelligence, decision support systems (DSS), or analytic CRM applications. The name is less important than their capabilities. These capabilities, described in Table C, should include these high-level functions:

- Data warehousing
- Reporting
- Analytic applications

<table>
<thead>
<tr>
<th>Customer-Centric Intelligence CRM Applications</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Description</td>
</tr>
</tbody>
</table>

CUSTOMER RELATIONSHIP MANAGEMENT
### Data Warehousing

Data warehouses provide the input to customer-centric intelligence applications. Data warehouses that support these applications must contain:

- Customer information used by all operational CRM applications
- Customer information used by analytic applications such as customer values and customer scores
- Information about your products and services
- Information about the channels and touchpoints through which you offer products and services
- Information about your marketing, sales, and service initiatives
- Information about customer behavior in response to those initiatives
- Information about customer requests
- Information about your responses to customer requests
- Information about customer transactions.

### Reporting

Reporting presents the information that you have loaded into the data warehouse in order for managers and analysts to view and analyze it. Reports provide a range of tabular and graphical presentation formats and optionally allow analysts to interact with the report presentation, changing its visual format, drilling up into summary information and/or drilling down into detail. Reports support manual analysis.

### Analytic Applications

Analytic applications automate both the analyses that managers and analysts perform manually on reports and analyses based on statistical and pattern recognition algorithms. Analytic applications process data warehouse data, whereas reports merely present that information. Analytic applications are your tools for analyzing the performance, efficiency, and effectiveness of your operational CRM applications. Their output should enable you to improve the operational applications that deliver your customer experience in order to achieve the CRM objectives of acquisition, retention, and growth. For example, analytic applications may be designed to provide insight into customer behavior, requests, and transactions as well as into customer responses to your marketing, sales, and service initiatives. Analytic applications also create statistical models of customer behavior, values of customer relationships over time, and forecasts of customer acquisition, retention, and desertion.

### 6.1.5 The CRM Application Supplier

Implementing CRM applications with the goal of becoming a customer-centric company will likely involve purchasing application software packages. Building your own applications is not a viable nor practical option given the breadth, depth, and quality of available packages.

There are three types of CRM software suppliers:

- CRM suite suppliers
- CRM point solution suppliers
- E-commerce suppliers
1. **CRM Suite Suppliers**

CRM suite suppliers offer a suite of CRM products that implements all the key customer-facing, customer-touching, and customer-centric intelligence applications. While application functionality varies across the suite, some products offering richer functionality than others. Suites usually have the advantages of providing a single and consistent view of the customer, integration across touchpoints, a single architecture, and support from a single vendor.

The leading CRM suite suppliers are (alphabetically) Oracle, PeopleSoft, Siebel, and SAP. E.piphany also provides a CRM suite that implements all the CRM applications except e-commerce as do a number of smaller players such as Talisma.

Oracle, PeopleSoft, and SAP have the additional advantage of tight integration between CRM applications and their ERP and supply chain applications, facilitating the automation of the business processes that support marketing, sales, and service.

2. **CRM Point Solution Suppliers**

CRM point solution suppliers offer products that implement one or two CRM applications. The advantages of a point solution approach are the ability to implement best-in-breed functionality and the ease of adding incremental applications to existing CRM environments.

There are dozens of CRM point solution suppliers. For example, NCR and Unica offer products that implement customer-centric intelligence applications. MarketFirst and Revenio specialize in marketing automation solutions, and companies such as SalesLogix focus on SFA tools.

3. **E-Commerce Suppliers**

E-commerce suppliers provide, obviously, the customer-touching e-commerce application, and their offerings are far richer in e-commerce functionality than the e-commerce offerings of CRM suite vendors. In addition, the latest versions of their products package campaign management, contact center, and customer-centric intelligence capabilities—everything except sales force and field service automation, and the product support aspects of contact center. They also all do an excellent job of integrating external applications and automating supporting business processes. We’ve been following e-commerce since 1996.

The leading suppliers and products are (alphabetically) ATG Dynamo, Blue Martini 4, BroadVision Business Commerce and Retail Commerce, IBM WebSphere Commerce Suite, and Microsoft Commerce Server.

6.1.6 **Selecting CRM Products**

Given the array of supplier types, the very large number of available products, and the strategic nature of the applications that they implement, selection of CRM products is a critical and potentially complex decision. These are the critical decision factors to consider when making your product choices:

- **Functionality.** What the products do should closely reflect the way that you do business.
- **Single and consistent customer view.** The products should minimize entity’s efforts to integrate and synchronize customer information.
- **Integration across touchpoints.** You’ve got to provide a consistent customer experience. You don’t want to code it yourself.
• **Automation of supporting business processes.** The tighter the integration with back office and supply chain systems, the better the customer experience. This integration is about the most complex task in CRM implementation. The more that’s “in the box,” the better.

### 6.1.7 How to Succeed with CRM

Implementing the CRM products that you select, and becoming customer centric through their integration and usage, are complex and strategic efforts that should touch every aspect of your organization. CRM projects require careful planning and meticulous execution. Here are a few key points to remember:

- Adopting a customer-centric philosophy and implementing CRM products will involve major cultural and organization change. You will meet a lot of resistance.
- CRM products automate business processes and tasks that you might never before have automated. They introduce additional organizational change and, perhaps, technological change.
- CRM should be enterprise-wide in scale and scope. Few organizations have the staff, skill, and budget to do it all at once. Take an incremental approach, one CRM application at a time, following a CRM pilot that you know will succeed.
- Many CRM products are new. You might be a pioneer for technology, products, and/or suppliers. There are significant rewards for pioneering, but there are significant risks, too.
- Supplier claims and user expectations for CRM can be unreasonable. Be skeptical of vendor claims. Have vendors prove their claims with references. Take small steps toward customer-centricity and have reasonable and demonstrable expectations for those steps.

### 6.1.8 Conclusion

“Improved Satisfaction, Increased Business”

And finally, here’s the bottom line reason for “doing” CRM truly is a way to improve customer satisfaction and increase business. If you offer products and services that customers need (at a fair price), then they’ll do business with you. If you make them doing business with you, an easy, efficient, responsive, and quality experience, then those customers do business with you over and over again. They become loyal customers, and you have profitable relationships with them. Remember that you must continuously earn their loyalty, never taking these customer relationships for granted. The continuous effort to earn loyalty will help maintain your customer focus and will grow those relationships. That’s CRM.
6.2 Sales Force Automation (SFA)

Key Term
Sales Force Automation is the use of technology to help automate, organize, and track the selling process. Sales managers, sales teams, and sales reps have embraced SFA as a means of increasing their sales efficiency and effectiveness.

Sales Force Automation has rapidly evolved in the last several years to a "must have" requirement for competing in today's competitive sales environment. Today's sales managers are no longer asking: "Does my competitor have SFA technology?" Instead, they're asking: "How effectively are my competitors using their SFA technology to compete with me?"

Key Term
Sales Process Management is the collaborative evaluation that identifies a company's best business practices, and then integrates them into a customizable technology application, which is then delivered seamlessly to all members of a sales team. The goal of effective SPM is to enhance sales productivity and help generate increased revenues.

1. Stages of SFA

Stage 1 -- Transaction-Centric, the basic level of SFA --. The software allows you to know who your customers and prospects are, view and manage the sales pipeline, review sales cycle activities, perform trend analysis and begin sales forecasting.

Stage 2 -- sales connectivity -- Connecting SFA with marketing, customer service, installation and service (for companies selling goods), promotions, and of course accounting, inventory management and manufacturing can go a long way in improving the profitability of any business

Stage 3 -- knowledge-empowerment -- the most advanced step of SFA, serves not only as a means of benefiting the organization by institutionalizing all selling and selling-channel-related knowledge, but also benefits individual salespeople by helping them achieve their highest potential. This Stage will require not only your commitment, but that of your best salespeople.

2. Data Mapping

Data mapping refers to tracing the path of information flow within an organization. In a customer-centered system, the customer is the initial source of data and the path is traced inward from there. In many ways, SFA is the automation of data flow. Data maps are useful tools to optimize data flow and, hence, improve communications in a company.
To track sales leads more effectively, one draws out

1. How this information (the name of a lead) moves through all the stages within a company.
2. How did the company get the lead?
3. Who does that information go to?
4. How is that information entered into the system?
5. Who assigns a lead to someone?
6. How does that someone get the information?
7. If the lead becomes a customer, what happens?

3. **Mobile devices and SFA**

One of the enterprise’s most critical and expensive assets is its sales force and associated SFA system. For each day the sales force is not operating at peak efficiency, the company suffers from lost revenue, lower customer satisfaction and higher operating costs. While there are many tangible and intangible benefits to getting more from SFA with a mobile sales solution, the four that will have the greatest impact on a company's bottom line are:

- Greater effectiveness and productivity of the sales force,
- Improved customer interactions,
- Streamlined business processes, and
- Increased return on existing SFA investments.

**Case Example**

**AvantGo Mobile Sales**

AvantGo Mobile Sales is a flexible, proven application built on AvantGo’s best-of-breed mobile software platform. AvantGo Mobile Sales puts at their fingertips all the information sales professionals need to do their job more productively and effectively.

The solution works with all major SFA applications, including Siebel, PeopleSoft, Amdocs, Oracle, Dendrite, SAP and others. And unlike SFA vendors’ mobile extensions, which only mobilize one application, AvantGo Mobile Sales collects and combines information from many other critical enterprise applications, such as enterprise resource planning (ERP), supply chain management (SCM) and knowledge management systems, into a single mobile sales application that sales professionals can easily access at any time to be better informed and prepared.

AvantGo enterprise solutions ensure instant access to important information, messaging and applications—even outside of wireless coverage areas. Patent-pending message and transaction queuing techniques, combined with advanced compression, caching, encryption and optimization of wireless data transmission, deliver the fastest, most reliable, interactive mobile experience available.

4. **Benefits of Sales Force Automation include**

1. Improved customer management;
2. Rapid, accurate and inexpensive communication among field reps, sales managers and the corporate office;
3. Easier database access;
4. Reduced errors and cycle time;
5. Improved sales call planning, reporting, and scheduling; and superior growth – both at the corporate level and in the sales force.

Case Example

Salesnet

Salesnet allows you to painlessly track your leads, wirelessly maintain your customer/prospect database, capture and automatically route Web site leads, generate emails and letters, create comprehensive sales reports, and access your important sales documents, all without the complexity and cost associated with typical SFA/CRM applications.

Salesnet is an application service provider (ASP) that offers a robust Web-based Sales Process Management (SPM) and Sales Force Automation (SFA) service. Salesnet's online Sales Process Management (SPM) solution offers the fastest CRM/SFA deployment in the industry, with a 100 percent successful track record.

Salesnet's Professional Services team guarantees that your best sales business practices will be automated within weeks, from pilot to rollout, and at one-fifth the cost of traditional client/server CRM/SFA deployments. Salesnet's ASP model eliminates the need for a huge up-front capital investment in software and hardware. And, sales professionals get real-time access to critical sales team activities, sales reports, forecasts, and customer information -- via their desktop computer, laptop, or preferred wireless device -- regardless of their geographic dispersement.

Advantages of this sort of product are improved quality of information, faster responses to customers, improved communication with workers who are mainly out of the office and greater efficiency in mobile workforce operations.

Disadvantages is increased security risks, need for improved controls over remote operations, greater investment in technology and more complex networks.
6.3 Supply Chain Management

6.3.1 Introduction

Key Term

A supply chain is a network of facilities and distribution options that performs the functions of procurement of materials, transformation of these materials into intermediate and finished products, and the distribution of these finished products to customers.

Supply chains exist in both service and manufacturing organizations, although the complexity of the chain may vary greatly from industry to industry and firm to firm.

Below is an example of a very simple supply chain for a single product, where raw material is procured from vendors, transformed into finished goods in a single step, and then transported to distribution centers, and ultimately, customers. Realistic supply chains have multiple end products with shared components, facilities and capacities. The flow of materials is not always along an arborescent network, various modes of transportation may be considered, and the bill of materials for the end items may be both deep and large.

Traditionally, marketing, distribution, planning, manufacturing, and the purchasing organizations along the supply chain operated independently. These organizations have their own objectives and these are often conflicting.

Marketing's objective of high customer service and maximum sales dollars conflict with manufacturing and distribution goals. Many manufacturing operations are designed to maximize throughput and lower costs with little consideration for the impact on inventory levels and distribution capabilities.

Purchasing contracts are often negotiated with very little information beyond historical buying patterns. The result of these factors is that there is not a single, integrated plan for the organization—there were as many plans as businesses.

Clearly, there is a need for a mechanism through which these different functions can be integrated together. Supply chain management is a strategy through which such an integration can be achieved.

Supply chain management is typically viewed to lie between fully vertically integrated firms, where the entire material flow is owned by a single firm, and those where each channel member operates independently.

Therefore coordination between the various players in the chain is key in its effective management. Cooper and Ellram [1993] compare supply chain management to a well-balanced and well-practiced relay team. Such a team is more competitive when each player knows how to be positioned for the hand-off. The relationships are the strongest between players who directly pass the baton, but the entire team needs to make a coordinated effort to win the race.
6.3.2 Supply Chain Management Software

Supply chain management software is possibly the most fractured group of software applications on the planet. Each of the major supply chain decisions previously outlined composes dozens of specific tasks, many of which have their own specific software. There are some large vendors that have attempted to assemble many of these different chunks of software together under a single roof, but no one has a complete package.

Integrating the different software pieces together can be a nightmare. Perhaps the best way to think about supply chain software is to separate it into software that helps you plan the supply chain and software that helps you execute the supply chain steps themselves.

1. Supply chain planning (SCP) software

Supply chain planning (SCP) software uses fancy math algorithms to help you improve the flow and efficiency of the supply chain and reduce inventory. SCP is entirely dependent upon information for its accuracy. If you're a manufacturer of consumer packaged goods for example, don't expect your planning applications to be very accurate if you can't feed them accurate, up-to-date information about customer orders from your retail customers, sales data from your retailer customers' stores, manufacturing capacity and delivery capability.

There are planning applications available for all of the major supply chain steps previously listed. Arguably the most valuable (and complex and prone to error) is demand planning, which determines how much product you will make to satisfy your different customers' demands. SCP comprises demand management or forecasting, network or multi-facility planning, production planning, distribution or replenishment planning, and transportation planning.

2. Supply chain execution (SCE) software

Supply chain execution (SCE) software is intended to automate the different steps of the supply chain. This could be as simple as electronically routing orders from your manufacturing plants to your suppliers for the stuff you need to make your products.

SCE comprises order management, availability or capability to promise, warehouse and transportation management, and international trade. International trade covers tariffs, landed cost calculations, and export documentation.

3. Supply chain process management (SCPM) software

Supply chain process management (SCPM) software is the glue that binds together these two very different suites. It provides global, real-time visibility into events, Key Performance Indicators (KPIs), and decision support around exception situations.

The following figure shows the market share of each kind of Supply chain management (SCM) software:
Complete supply chain management solutions support supply chain activities across all time horizons. However, every industry views time horizons differently. Two quarters might be a strategic timeframe for the fashion industry, yet managers in the defense industry may view such a timeframe as operational. The key distinction between each timeframe is the degree of flexibility managers have to change what occurs. SCM software supports activities across the following timeframes:

- **Executional** timeframe: the frequency of order updates to operators on the shop floor. Typically a day, but can be shorter. For instance, the period of a picking wave in a warehouse.
- **Operational** timeframe: the time taken to receive and fulfill an order or the life of a customer contract. Typically a few days to a few weeks.
- **Tactical** timeframe: roughly the length of supplier contracts, or a supplier’s lead-time. Typically a week to a few months.
- **Strategic** timeframe: Some view strategy as determining what products will sell into what markets. Then the strategic timeframe is the time required to change key assets i.e., to erect a new plant, close a distribution center, launch a new product. Typically a few months to a few years.

Often SCM suites unlock value by compressing the above time-periods. For instance, instead of running a weekly transportation plan, best practice would include running a transportation plan every day. Fixed transport routes and schedules are inefficient, and dynamic, optimized routing generates considerably savings. Reducing planning and execution cycles enables supply chains to respond rapidly, which in turn, improves order fulfillment metrics in the face of unexpected problems.

### 6.3.3 Features of a SCM software

A few years ago, operational excellence in supply chain management just meant exploiting appropriate optimization and forecasting technologies. Nowadays, software supplier(s) master, integrate, and have references for the following seven technologies:

1. **Forecast**

   If the time from order to customer delivery is shorter than your total manufacturing lead-time, you have no option but to forecast, using statistical analysis of historical data.

2. **Collaborate**
This is sharing information with sister companies and business partners, which requires both portal technology and Enterprise Application Integration (EAI) technologies. Portal technology is key. It provides a standard user interface to multiple systems. It not only allows access to different systems in multiple regions that are geographically remote, but also lets users learn quickly to drive multiple systems, because it also provides a standard user interface. Greater benefits emerge through automating data transfer and processes across systems. Enterprise Application Integration provides connectors to multiple systems, a means of translating messages from one format into another and also directing messages to the appropriate application.

3. **Optimize**

This includes mixed integer linear programming, heuristics approaches such as Theory of Constraints, and genetic algorithms. The supplier also requires the technical skills to exploit the hardware to rapidly find the optimum.

4. **Execute**

This is the ability to process transactions in real-time, with guaranteed performance. For instance, a warehouse picker firing his scanner at a bar code label requires rapid confirmation in order to pick efficiently.

5. **Process Management**

Supply Chain process management technology at its simplest combines data base triggers and stored procedures with e-mail. It should also include workflow, especially in the order management modules, which is a weakness in some systems.

6. **Document Transactions**

SCM requires a system of record, to track costs, invoice customers, and pay suppliers. There is little benefit, if you don’t get paid on time and in-full.

7. **Analyze Performance**

Usually this requires OLAP and data warehouse technology.
6.4 Enterprise Resource Planning

6.4.1 Introduction

Enterprise resource planning software, or ERP, doesn’t live up to its acronym. Forget about planning it doesn’t do that and forget about resource, a throwaway term. But remember the enterprise part. This is ERP’s true ambition. It attempts to integrate all departments and functions across a company onto a single computer system that can serve all those different departments’ particular needs.

That is a tall order, building a single software program that serves the needs of people in finance as well as it does the people in human resources and in the warehouse. Each of those departments typically has its own computer system, each optimized for the particular ways that the department does its work. But ERP combines them all together into a single, integrated software program that runs off a single database so that the various departments can more easily share information and communicate with each other.

6.4.2 Information Systems Software

In a company there are usually different types of information systems. These can be divided into three areas:

- Standard application packages
- Systems developed in-house
- “Joint-venture” systems

A “Joint-venture” system is a system that is a combination of a standard application package and an in-house-developed system. An in-house-developed system is a system that is customised to your own company. A standard application package system has been developed by a vendor to satisfy many users’ (clients’) business requirements. This means that users purchase a system on the market instead of developing a system on their own. An ERP system is a standard application package that is fully integrated.

This means that the different systems, financial, manufacturing, etc., use the same database.

6.4.3 The History of ERP

ERP’s roots can be traced back to the ISVs, Independent Software Vendors, of the 1970s, who developed small-scale integrated financial and manufacturing packages, initially for minicomputers such as the IBM 3X range. In the 1980s, the concept was introduced to the mainframe market, but it still took some time before mainframe users started to take notice.

The standard application package is the opposite of the in-house developed information system, which has dominated the mainframe world. The cost of permanent employees, programmers and technical support to create and maintain the home-grown applications is one of the reasons for the dramatic fall of the in-house-developed applications.

The idea behind the standard applications packages is that several companies can use the same software. With several users, the costs of development, support and maintenance are shared. In addition, each client does not have to “reinvent the wheel”.
The standard application packages are made for handling specific tasks. Financial systems are created for treating the financial information flow, and MPS systems for treating the logistic information flows in manufacturing. After these standard application packages came the ERP system, which also is a standard application package. The difference is that ERP is a system where the financial, manufacturing, distribution systems, etc., are integrated.

ERP is a concept developed by GartnerGroup. The term ERP has only been widely used for three or four years, but these systems and their predecessors, MRP (Material Requirements Planning) and MRP II (Manufacturing Resource Planning), have been actively sold for nearly 25 years. They are the primary business systems installed in tens of thousands of manufacturing companies around the world.

ERP vendors, as well as ERP “experts”, come from two major different origins: MRP systems and financial systems. The ERP vendors were vendors of one of the two systems above and became ERP vendors by building in the other part into the system. This is not that simple in reality, but broadly it can be seen this way. The company’s origin is often reflected in its system. If the vendor’s best module is its financial module, the company usually has an origin of being a vendor of financial systems. Today there are of course new vendors that started their business

6.4.4 The ERP system

The ERP system is an attempt to create an integrated product that manages all operations in a company. Before, the systems were not integrated and companies had (and many still have) several different systems for managing finance, storage, purchasing, etc., which were running separately. This caused large problems when trying to get the systems to work together. If you have many different systems you have to enter the same data into several systems. A couple of different “program islands” have been floating around in the companies and ERP is one attempt to link them into one unit. If you enter data into the module for manufacturing, the data is entered in the central database and obtained in the financial module simultaneously.

6.4.5 The system’s influence on a company

In order to understand the function of ERP systems you need to understand the problems they are designed to solve. Every big company collects, generates, and stores vast quantities of data. In most companies, however, the data are not kept in a single database. Instead, the information is spread across a large number of computer systems. Maintaining these different systems leads to large costs – for storing and rationalising redundant data as well as reformattting data from one system for use in another. But even more important than the direct costs are the indirect ones. If a company’s sales and ordering systems cannot communicate with its production system then its manufacturing productivity and customer responsiveness will suffer. If its sales and marketing systems are incompatible with its financial systems then management is left to make important decisions based on instinct rather than according to a detailed understanding of product and customer profitability.

When developing systems in the past, companies would first decide how they wanted to do business and then choose a software package that would support their processes. They often rewrote large portions of the software code to ensure a tight fit. With ERP systems, however, the sequence is reversed. The business often has to be modified to fit the system. Some degree of customisation is possible. Since the systems are modular, companies are able to install only those modules that are most appropriate to their business. However, the complexity of the system makes major modifications impracticable.
As a result, most companies installing an ERP system need to adapt or completely even rework their processes to fit the requirements of the system. For some companies the ERP system can be the catalyst for reworking their processes but for others it might cause large problems.

Configuring an ERP system is largely a matter of compromises, of balancing the way you want to work with the way the system lets you work. ERP vendors try to structure the systems to reflect best practices, but it is the vendor, not the client, that is defining what “best” means. In many cases the system will enable a company to operate more efficiently than it did before. In some cases, however, the system’s assumptions will run contrary to a company’s best interests.

ERP systems may not be suitable for all companies. For a fast growing company with an organisation that is quickly changing, it may be difficult to benefit from an ERP system. The problem is that the company has a different organisational structure when the system is implemented compared to when the project started, according to Philip Ekstrand, Data Webhouse. Some parts of the organisation may have been sold and new parts may have been acquired. Hence, the company will have to modify its ERP system again to make it suitable for the new organisation. When that job is finished, the organisation has changed again, and so on.

6.4.6 The structure of the ERP system

ERP systems consist of different modules. A company can therefore decide which modules they need and only acquire them, not needing to purchase them all.
Traditionally a system must integrate three of the following core modules to belong to the ERP group: manufacturing, distribution, finance and human resources. At the heart of an ERP system is a central database that draws data from and feeds it into a series of applications supporting diverse company functions. Using a single database streamlines the flow of information throughout a business.

6.4.7 Why do companies acquire an ERP system?

Companies name the following advantages with having acquired an ERP system:

- The opportunity to see the whole company as one unit, since the system is integrated.
- The strategic possibility to rationalise and gain better control of the company’s information flow.
- The old systems could not be developed, or it would be too expensive to develop them further, in order to support the company’s processes.
- To reduce the maintenance cost of the information system environment by replacing several old systems with a single new one. This replacement also reduces the dependency on a few key users.

There are two major starting points for investing in an ERP system. Either the company sees it as a strategic solution, or it sees it as a technical solution.

1. Strategic solution

A strategic solution means that a company acquires an ERP system because it is a part of its future strategies. For large enterprises it is very difficult to get a general overview of its organisation. This can be simplified with a uniform system where everybody works according to the same routines. This concerns especially today’s more and more globalised companies. “ERP wakes up the dream of seeing the whole company as one unit”, says Bobby Cameron, analyst at Forrester Research. An integrated ERP system gives opportunities to rationalise and develop an organisation. An ERP system may be seen as a tool to obtain information that can be important when forming the company’s future strategies. Information Technology to an increasing degree concerns the management, and the decision to buy an ERP system is almost always taken by the top management.

2. Technical solution

If the company sees ERP as a technical solution the main reason for changing systems is that its present information systems are too old. Two important factors have further caused this changing system process to boom, the year 2000 problem and the Euro.

3. Technical and/or strategic solution - discussion

There are, as mentioned, two starting points when acquiring an ERP system. Either you see it as a technical solution or you see it as a strategic solution. However, it is impossible to separate them since they affect each other.

There are three levels affected when implementing an ERP system:

- Operational development. Development of the company’s functional strategies and their relationship with concerned functions within the organisation.
• **System development.** Development and administration of necessary IT strategy, where the ERP system is an important part.

The top level touches the work with the company’s business strategy. Business strategies indicate how we can strengthen the company’s relations to different operators in the surroundings, for example clients, vendors, competitors and business partners.

The second level focuses on the development of internal operations in the company. Companies today analyse their business processes to find ways to become a more efficient company. Business processes define the workflow within the company’s organisation.

The third level focuses on the company’s need of IT services. The infrastructure of the company’s activity consists of the use of IT. Appropriate IT is often a question for the company management, in order to estimate the technological level of the company.

### 6.4.8 Effects from implementing an ERP system

To decide whether or not to implement an ERP system you have to look for its positive and negative effects. It is also easier to accomplish a successful implementation if you are aware of these effects.

1. **Positive effects**

   • **Standardised (fast?)** implementations. It is much easier to buy an existing system than developing your own system. There have been a lot of complaints over the years that ERP systems take too long to implement, especially the implementation time of SAP R/3. By now the vendors have developed methods and other means to shorten the time of the implementation, AcceleratedSAP, for example.

   • **Cheap development.** The ERP vendors put in between 5-15 percent of their revenues in their Research & Development department. To develop your own systems that are equally good is very costly.

   • **Safe cost estimation.** To invest in an existing system makes it easier to estimate the total cost of the system and implementation. If you develop your own system it is difficult to know how much you finally will spend on the system.

   • **“Know-how”** built-in the system. The system has been implemented and tested in other companies and therefore you know it is in working order. When you develop your own system, it is hard to anticipate the problems that you may run into and how these problems will affect the functionality.

   • **Flexible systems.** The systems consist of modules, which make adaptations at a later time easier.

2. **Negative effects**

   • **External vendor without company knowledge.** To acquire an ERP system means buying a system that is not specifically adapted to the company. But systems adapted to specific industries are coming and will be improved in the years ahead.

   • **Increased need of external competence.** Since the market has grown so quickly, there is a lack of skilled people. It is difficult to keep the internal competence and you therefore need much help from consulting firms.

   • **New routines for the staff.** An ERP system is hard to adapt completely to the organisation. This means new routines for the staff, which make the work more difficult in a period of transition.
• *Freezes system development to the vendor.* The company follows the vendor’s development with little possibility to influence. The programs can be hard to support for the company itself. The client will also have to purchase future releases of the system.

• *Underestimates the importance of the pre-study.* The company may after the implementation have a system that it cannot handle.

### 6.4.9 The implementation process

The implementation process is as mentioned earlier an important part of acquiring an ERP system. If the process is not handled right it will cost much money and in the worst case the implementation will not work out at all, so the company will have spent money on a product that does no good.

Those services that are indirectly related to an implementation of an ERP system are the following:

• *Procurement.* Comprise inquiries on client’s needs and goals.

• *Project management.* The clients often do not have the resources to carry out the necessary activities for a successful implementation. In some cases they therefore need someone to take total responsibility for the implementation and the related services. However, according to our interviews with ERP clients, the best implementation processes have been those where the client itself is highly involved in the management of the project.

• *Routine consultants help.* Comprises help in changing routines when implementing an ERP system and transferring of information from previous systems.

• *The implementation process:* Provides the client’s physical installation of the system and modifications and adjustments for the client’s requirements.

• *Training.* Has the aim to give the client knowledge in how the system could best be used. Training should occur when implementing the system, when buying new releases, when changing staff, and when the client buy new modules. According to our interviews, the user training should occur as close to the going live point as possible.

• *Support.* Involves assistance when errors occur, which are caused by bad handling or product failure. Some ERP vendors have support systems, which their clients can connect themselves to.

• *Service and new releases.* The vendors offer contracts, which give the client a possibility to, on pre-set conditions, upgrade their systems to new releases. Some vendors also have agreements concerning service.

SAP, as well as the other ERP vendors, has worked hard on reducing the implementation time; one example is their implementation method AcceleratedSAP.

### 1. Critical success factors of ERP implementation

Critical success factors can be viewed as situated exemplars that help extend the boundaries of process improvement, and whose effect is much richer if viewed within the context of their importance in each stage of the implementation process. A number of factors that may affect the ERP implementation process and the probability of conversion success have been identified in the IT implementation, IT failures, and business process reengineering literatures. Among the more important factors are:

• Top management support and involvement,

• The need for a project champion,

• User training on software,

• Technological competence,

• Process delineation,
• Project planning,
• Change management, and
• project management

In the context of ERP implementation, additional issues include the need to reengineer business processes prior to implementation, the need to communicate effectively and set appropriate expectations, the use of a balanced IS and business team, and the avoidance of customization. Some other factors that are also critical to the successful implementation are:

• Project team competence
• Interdepartmental cooperation
• Clear goals and objectives
• Interdepartmental communication
• Management of expectations
• Vendor support
• Careful package selection
• Data analysis & conversion
• Dedicated resources
• Use of steering committee
• Education on new business processes
• Business Process Reengineering
• Minimal customization
• Architecture choices
• Partnership with vendor
• Use of vendors’ tools
• Use of consultants

6.4.10 ERP Software Vendors

When it comes to ERP vendors, one company is dominating the world market totally: SAP. The others have more or less given up the first place and are fighting for the second one. The German vendor SAP occupies approximately 30 percent of the world market. In the table below, the eight largest ERP vendors are listed.

<table>
<thead>
<tr>
<th>Company</th>
<th>Product</th>
<th>Growth % 1998</th>
<th>Growth % 1997</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP</td>
<td>R/3</td>
<td>41</td>
<td>58</td>
</tr>
<tr>
<td>Oracle</td>
<td>Oracle Applications</td>
<td>42</td>
<td>83</td>
</tr>
<tr>
<td>Peoplesoft</td>
<td>Peoplesoft</td>
<td>69</td>
<td>108</td>
</tr>
<tr>
<td>JD Edwards</td>
<td>One World</td>
<td>52</td>
<td>57</td>
</tr>
<tr>
<td>Baan</td>
<td>Baan IV</td>
<td>15</td>
<td>100</td>
</tr>
<tr>
<td>SSA</td>
<td>BPCS</td>
<td>2</td>
<td>43</td>
</tr>
<tr>
<td>JBA</td>
<td>Business 400</td>
<td>-</td>
<td>58</td>
</tr>
<tr>
<td>Intentia</td>
<td>Movex</td>
<td>52</td>
<td>50</td>
</tr>
</tbody>
</table>
1. **SAP AG**

The leading ERP package vendor, with a 32% market share in 1999, is SAP AG (SAP stands for “Systeme, Anwendungen, und Produkte in Datenverarbeitung” or Systems, Applications and Products in Data Processing). SAP AG was founded in Germany in 1972 by five engineers who wanted to produce integrated business application software for the manufacturing enterprise. Seven years later, the company launched its first enterprise software, R/2, which was designed around a centralized, mainframe-based database. SAP’s client/software product, R/3, was introduced in 1992 and quickly came to dominate the ERP software market. In 1999, SAP AG was the third-largest independent software vendor in the world, serving over 11,000 customers (with more than 20,000 installations) in over 100 countries. Leveraging its leading position in the ERP market, SAP developed vertical, industry-specific business solutions for 19 industries. These industry “solution maps” provide functionality from SAP and its partners for complete, end-to-end industry-specific processes. SAP followed the lead of focused niche players, and in 1999 it extended its ERP offering to include customer relationship management, data warehousing and supply chain management modules. SAP recast its entire set of offerings around the Internet, borrowing the “business portal” concept (called mySAP.com Workplace in SAP parlance) to organize all information around the user’s role in the enterprise, and adding functionality for business-to-business and business-to-consumer electronic commerce. SAP started the mySAP.com Marketplace, an electronic inter-company trading community for buying, selling and collaborating within and across industries.

2. **Oracle**

The heavyweight of the database software market, Silicon-Valley-based Oracle is the world’s second largest software company. It has built a solid enterprise applications business, which accounted for $2.5 billion of the firm’s $9.3 billion 1999 revenues. Second to SAP in the enterprise software market, Oracle applications serve over 5,000 customers in 140 countries. Oracle has been a leader in refocusing its ERP solutions around the Internet, and it launched a barrage of electronic-commerce and Internet-based business-to-business software applications while the other JBOPS companies were slow to react to the changing marketplace. Further, Oracle was the first JBOPS company to integrate front office applications with its ERP offering.

3. **PeopleSoft**

Started as a software firm for human resource management in 1987, Pleasanton-based PeopleSoft gradually expanded its software to cater to other corporate functions. The company’s revenues grew to $1.3 billion in 1998 up forty-fold from $32 million in 1992 (sales are expected to remain flat in 1999). PeopleSoft’s ERP system provides enterprise solutions for finance, materials management, distribution, supply chain planning, manufacturing and human resources. In 1996, PeopleSoft acquired Red Pepper, a producer of supply chain management software, and in 1999 it acquired Vantive for its customer relationship management offering.

4. **J.D. Edwards**

Founded in 1977 by three partners from an accounting firm, Denver-based J.D. Edwards addresses business processes in finance, manufacturing, distribution/logistics and human resources, and encompasses the entire supply chain from planning and scheduling through execution. Growing from $120 million in revenues in 1992 to $944 million in 1999, the software maker has served over 5,000 customers in over 100 countries. Its OneWorld system is considered to be more flexible than its competitors’, and the company made headway in smaller enterprises. And, rather than build its own customer relationship management system, J.D. Edwards developed tight integration with Siebel’s leading offering.
5. Baan

The Baan Company was founded in The Netherlands in 1978 making financial software. Baan’s products have been simpler to use than SAP’s, leading to the company’s growth in the early nineties. Today, the company operates in 80 countries, serving more than 2,800 customers. Baan’s net revenues have increased from $47 million in 1992 to $736 million in 1998. The Baan Series is its primary enterprise system, which incorporates a variety of functionalities from sale order management and manufacturing to supply chain management. Since October of 1998, Baan suffered a series of setbacks including management turmoil, accounting irregularities, multiple-quarter losses and CEO turnover.

6.4.11 Choosing the right ERP package

The selection process starts with an identification of system scope, business objectives and business processes. Some ERP packages provide better solutions in certain functional areas. For example, SAP began as manufacturing software and still excels along that dimension. Moreover, different ERP vendors have experience in different industries, and offer solutions that are geared to those industries. A major consideration in choosing a package involves the management style of the firm. Even the most flexible ERP packages are based on a model of doing business that may not align with the firm’s desired business model. For example, Dell Computer found that the SAP R/3 system it had licensed would not fit its highly decentralized management style.

Time-to-implementation is another issue that might be critical. Technical issues ranging from the hardware platform that the ERP package will run on to the set of currencies and tax rules supported by the package need to be considered carefully, and the stability and future viability of the ERP vendor are becoming important considerations as well.

In addition, a number of basic design issues can have a tremendous impact on the likely cost picture. The major cost categories include:

- Hardware
- Storage
- Software
- Networking
- Services
- Facilities
- Personnel
- Downtime
- Support and Maintenance

1. The Hidden Costs of ERP

Although different companies will find different land mines in the budgeting process, those who have implemented ERP packages agree that certain costs are more commonly overlooked or underestimated than others. Armed with insights from across the business, ERP pros vote the following areas as most likely to result in budget overrun.
I. Training
Training is the near-unanimous choice of experienced ERP implementers as the most elusive budget item. It’s not so much that this cost is completely overlooked as it is consistently underestimated. Training expenses are high because workers almost invariably have to learn a new set of processes, not just a new software interface.

II. Integration and Testing
Testing the links between ERP packages and other corporate software links that have to be built on a case-by-case basis is another often underestimated cost. A typical manufacturing company may have add-on applications for logistics, tax, production planning and bar coding. If this laundry list also includes customization of the core ERP package, expect the cost of integrating, testing and maintaining the system to skyrocket.

III. Data conversion
It costs money to move corporate information, such as customer and supplier records, product design data and the like, from old systems to new ERP homes. Although few CIOs will admit it, most data in most legacy systems is of little use. Companies often deny their data is dirty until they actually have to move it to the new client/server setups that popular ERP packages require. Consequently, those companies are more likely to underestimate the cost of the move. But even clean data may demand some overhaul to match process modifications necessitated or inspired by the ERP implementation.

IV. Data analysis
Often, the data from the ERP system must be combined with data from external systems for analysis purposes. Users with heavy analysis needs should include the cost of a data warehouse in the ERP budget and they should expect to do quite a bit of work to make it run smoothly. Users are in a pickle here: Refreshing all the ERP data in a big corporate data warehouse daily is difficult, and ERP systems do a poor job of indicating which information has changed from day to day, making selective warehouse updates tough. One expensive solution is custom programming. The upshot is that the wise will check all their data analysis needs before signing off on the budget.

V. Consultants Ad Infinitum
When users fail to plan for disengagement, consulting fees run wild. To avoid this, companies should identify objectives for which its consulting partners must aim when training internal staff. Include metrics in the consultants’ contract; for example, a specific number of the user company’s staff should be able to pass a project-management leadership test similar to what Big Five consultants have to pass to lead an ERP engagement.

VI. Replacing Your Best and Brightest
It is accepted wisdom that ERP success depends on staffing the project with the best and brightest from the business and IS. The software is too complex and the business changes too dramatic to trust the project to just anyone. The bad news is, a company must be prepared to replace many of those people when the project is over. Though the ERP market is not as hot as it once was, consulting firms and other companies that have lost their best people will be hounding yours with higher salaries and bonus offers than you can afford or that your HR policies permit. If you let them go, you’ll wind up hiring them or someone like them back as consultants for twice what you paid them in salaries.
VII. Implementation Teams Can Never Stop

Most companies intend to treat their ERP implementations as they would any other software project. Once the software is installed, they figure, the team will be scuttled and everyone will go back to his or her day job. But after ERP, you can’t go home again. You’re too valuable. Because they have worked intimately with ERR, they know more about the sales process than the salespeople do and more about the manufacturing process than the manufacturing people do. Companies can’t afford to send their project people back into the business because there’s so much to do after the ERP software is installed. Just writing reports to pull information out of the new ERP system will keep the project team busy for a year at least. And it is in analysis and, one hopes, insight that companies make their money back on an ERP implementation.

VIII. Waiting for ROI

One of the most misleading legacies of traditional software project management is that the company expects to gain value from the application as soon as it is installed; the project team expects a break, and maybe a pat on the back. Neither expectation applies to ERP. Most don’t reveal their value until after companies have had them running for some time and can concentrate on making improvements in the business processes that are affected by the system. And the project team is not going to be rewarded until their efforts pay off.

IX. Post-ERP Depression

ERP systems often wreak cause havoc in the companies that install them. In a recent Deloitte Consulting survey of 64 Fortune 500 companies, one in four admitted that they suffered a drop in performance when their ERP systems went live. The true percentage is undoubtedly much higher. The most common reason for the performance problems is that everything looks and works differently from the way it did before. When people can’t do their jobs in the familiar way and haven’t yet mastered the new way, they panic, and the business goes into spasms.

6.4.12 Trends on the ERP market

We will start by giving a short definition of the word “trend” according to Kotler (1997): “A trend is a direction or sequence of events that have some momentum and durability”. Successful companies recognise and respond profitably to unmet needs and trends in the macroenvironment. Unmet needs always exist, Kotler (1997)

The trends that we have described are the following:

1. ERP for small and middle-sized companies
2. Componentisation
3. Industry solutions
4. Supply Chain Management
5. E-business and E-commerce
6. Outsourcing

1. ERP for middle-sized and small companies

Most ERP vendors have historically had large companies as their primary target. The market situation is now changing; the market growth among large companies is stagnating. The ERP vendors are therefore searching for new clients, preferably middle-sized, but also small companies.
One possible success factor for the ERP vendors in their attempt to sell to smaller companies is that smaller companies may follow their larger business partners, which already have an ERP system. Many companies are vendors to larger ones that can make requirements on which system architecture that their vendors use. This to make it easier to transfer information and work closer to each other. “Small companies are drawn into using an application like R/3 because larger business partners are using it”
2. **Componentisation**

The ERP vendors are making their systems more open in the form of components. Instead of an integrated system based on about ten modules, the ERP systems are now divided further into smaller components, which can be integrated if wanted. The idea behind componentisation is to take advantage of the benefits of the large systems in terms of fast access to information and combine it with the small systems’ flexibility. Because of the complexity of the modules, the companies have been forced to adapt the ERP system and/or the organisation. The advantage of the smaller components is that they can be made more suitable for each company and changes will be easier and cheaper.

3. **Industry solutions**

Industry solutions can be seen as part of a larger effort by the ERP vendors to ease the implementation of their products. Everyone has heard stories of ERP implementations that took two or three years. That happens, in part, because the ERP packages arrive needing to be configured for the business and the industry. By configuring parts of the package in advance for a given industry and cutting out functions not required in that industry, vendors can shorten and ease the implementation process. Many of the leading ERP vendors have begun to organise their companies, both sales forces and development, around industry orientation. There is a wealth of industry-focused software on the market today that can complement the basic ERP systems. All ERP vendors have rich complementary software programs that encourage the connection of third-party software with their systems to solve industry-specific issues. The ERP consulting partners are also aligning themselves to different industries. SAP wants all their partners to concentrate on a limited number of industries in order to gain more business expertise, compared to their focus of today that are in many different areas.

4. **Supply Chain Management**

A company’s supply chain is comprised of geographically dispersed facilities, such as plants, distribution centers, sources of raw materials, customer warehouses, and transportation links carrying raw materials. The facilities include physical entities operated by the company’s vendors and clients as well as those operated by the company itself. In managing its supply chain, the company is concerned not only with cost but also with service, quality and time factors that can strongly influence its success in the marketplace. Traditionally, companies have employed a variety of methods to solve unpredictable supply and demands problems. Some have built excess inventory, stored finished products or sub-products in company warehouses, or moved them out to distributors or customers. Some have added capacity through plant and personnel expansions, while others have outsourced jobs when production demands ran higher than expected. The disadvantages of these solutions – higher expense, lower profit margins and reduced flexibility – have made them increasingly unacceptable.

I. **ERP’s role in Supply Chain Management**

Practical developments in Supply Chain Management have grown in the 1990’s due to advances in IT support. Gains in computing speed, communications, and the power and flexibility of data management software have promoted a range of applications. Furthermore, widespread implementation of ERP promotes integration of supply chain activities. In many companies, however, the scope and flexibility of installed ERP systems have been less than desired or expected, and their contribution to Supply Chain Management has yet to be fully achieved. Software tools are letting companies link their enterprise resource planning systems with those of their business partners to speed the delivery of goods and services.
Hence, the role of the ERP system in the supply chain is to deliver the right information. In an internal Supply Chain Management the ERP system is available for use within the company. The ERP system covers the whole supply chain information flow from purchasing of raw material to product delivery. Here, the goal is to obtain an optimised supply chain within the organisation. If we look at it further, it is possible to make the supply chain even more efficient if we exchange information with our external vendors and customers, see figure 5.8.1.

![Diagram of supply chain management with ERP system at the center, connecting internal suppliers and customers on one side and external suppliers and customers on the other side.]

**Figure 5.8.1: ERP’s role in Supply Chain Management, Forrester Research**

If we give our vendors access to some information of our ERP system they can, for example, see how much of a certain product that we have in stock and what we plan to manufacture. With this information it is easier for our vendors to estimate our needs. The same relationship applies between our company and our clients. If we have information about their stock, it is easier to make forecasts. To go even further we can connect our vendors and clients. If our vendors know the needs of our clients in the last distribution chain, their forecasts can be even more efficient.

### 6.4.13 E-business and e-commerce

E-business can be described as the business transformation that occurs by exploiting the benefits of enterprise integration and global network connectivity. E-commerce is the transactional business process of selling and buying via the Net. The ERP vendors provide back-office accounting, supply chain, payroll, and manufacturing systems that interact with e-commerce systems to process orders, ship goods, and generate payments. There are two fundamental ways you can use the Web to support e-commerce:

- Using the Internet as a router for e-commerce transactions and transaction-related notifications and documents between two parties.
- Using workflow to connect internal systems and external Internet service provider systems to create new types of e-commerce “value-chains” between business partners.
Connecting clients and vendors more closely to the organisation can be achieved by giving them access to the organisation’s information system, in some cases the ERP system. By receiving more information in real-time that is easier to maintain than manual variants, you will create gains for all parties. If the external clients can perform some work on their own, like ordering goods, the organisation’s administrative function is relieved and business communications go faster. The external parties can also integrate these functions in their own systems. The most common form for this kind of information flow is EDI, Electronic Data Interchange. But, align with the widespread of Internet lately the need for Internet based solutions for this has increased. Such solutions are often cheaper, since the initial cost for EDI is high.

Electronic Data Interchange (EDI) and Electronic Funds Transfer (EFT) software service providers were delivering e-commerce long before the business world discovered the Web. The Internet has not significantly changed what either EDI or EFT software does, only how it does it. In the past, users of EDI and EFT software typically transmitted transactions between a buyer and a seller or a remitter and a bank via a privately run, value-added network (VAN). This locked people to a particular communications infrastructure and service pricing structure. Today people increasingly use the Internet as the router for EDI and EFT transactions. Some companies have begun moving some of their EDI transactions processing onto the Internet and many banks are rolling out Internet-based online banking services, which indicates that EDI and EFT on the Web are considered safe.

Web e-commerce has a long way to go before it becomes an integral part of the functionality that is expected from ERP suites. An important first step for all vendors is to ensure that they can seamlessly integrate Web-based services within current application process workflows. In this way, the vendors can extend the reach of their applications beyond the boundaries of conventional functional modules to make the vision of an extended-enterprise extranet a reality for their customers.

1. E-supply chain

E-supply chain refers to the management of the supply chain using Internet technologies. Eighty percent of businesses use the Web today, although less than seven percent use it in support of Supply Chain Management.

An Intranet is an internal net that is normally used within the boundaries of a company, and are protected from outside access by a "firewall". Companies are linking their ERP systems, or at least making information available from their ERP systems, to the Intranet.

Extranet is an external Intranet shared by two or more companies. Each participating company moves certain data outside of its private intranet to the Extranet, making the data available only to the companies sharing the Extranet. An example of this use would be providing inventory data to your supplier to help support an automatic replenishment process.

Last but not least is the Internet with which we are most familiar. This form is open to the general public. The Internet tends to be used more for e-commerce today, but has some emerging uses in Supply Chain Management, such as advertising surplus inventory to outside brokers.

So just how does e-supply chain benefit us? The objectives of any company are to reduce costs, reduce cycle time and grow revenue. E-supply chain supports these objectives by doing everything from improving the effectiveness of customer-supplier relationships to enabling faster customer response. World-class competitiveness demands a closer relationship with our supply chain partners and the building of “value-based” relationships. The quicker we can move data through the pipeline, the quicker we can react and hence, deliver the end product to our customer.
2. **From ERP to E Business**

With the advent of E-Business, companies are using the Internet to make connections with their suppliers, customers and trading partners. This shifts the emphasis from the traditional internal focus of the ERP vendors to an external orientation, increasing the importance of both Business-to-Business and front-office applications, which have been traditionally “bolted on” to companies’ ERP backbones. The fortunes of the leading ERP vendors changed along with the changing marketplace, and ERP package sales significantly slowed down in 1999. The ERP package vendors promise to broaden their offerings to fulfill the promise of E-Business, but only time will tell whether they will manage to extend their architectures to satisfy the new demands or whether today’s ERP systems will become tomorrow’s legacy systems.

### 6.4.14 Outsourcing

Outsourcing is a term describing when a business, or part of it, is sold or contracted to an outsider. Companies are nowadays finding it much more cost-effective to focus on their core business and leave other businesses to experts.

The idea of IT outsourcing is that an outside company – like a consulting firm – runs the software system on servers at a central location, taking on all the implementation and maintenance responsibilities itself.

1. **Outsourcing - pros and cons**

What are the advantages and disadvantages of outsourcing the ERP environment.

<table>
<thead>
<tr>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Scale economics by the vendor can reduce operation costs for the client, and minimise the client’s investments.</td>
<td>• The client loses control of its IT service.</td>
</tr>
<tr>
<td>• A reduction of the client’s responsibility concerning development and the running of the IT service.</td>
<td>• It is difficult to turn back from outsourcing. This is a risk when having signed an agreement with a consulting firm, since the consulting firm has its own interests to protect.</td>
</tr>
<tr>
<td>• The client can devote itself to its core business and focus on maximising its competitive advantages on the market.</td>
<td>• The IT service needs steering and follow-up of the consulting firm.</td>
</tr>
</tbody>
</table>

2. **Why outsource the ERP system?**

A reoccurring problem for all companies in the ERP business is the lack of skilled people. Especially the ERP clients suffer from this problem. It is hard for them to keep the employees that achieve good knowledge of the system, the so-called super users. They often leave the company for a job at a consulting firm. It is also difficult to hire people with good knowledge of ERP systems.

Therefore, it is difficult for ERP clients to build up enough competence to be able to run the system by themselves. To run the whole ERP environment you need to cover several different competencies, which requires about one employee per module.
For small and middle-sized clients it is even more difficult than for large ones to build up an ERP organisation. One way for the ERP vendors to reach these companies is outsourcing, which can be an attractive alternative for smaller companies with lean IT budgets. The price of an ERP system, implementation included, may be as high as the company’s normal IT budget. It can also be very expensive and time-consuming to find employees with high ERP expertise.

On the other hand, some organisations see their ERP system as a strategic resource. What is strategic you do not outsource is a common theory, and ERP systems can be seen as a strategic because it is closely intertwined with what the company do. Outsourcing the management of ERP systems helps businesses free IT resources to focus on the next set of technology and business challenges.

6.5 E-BUSINESS PRODUCTS

There are literally hundreds of software and hardware products that lay claim to be eBusiness Products. Many of the products address only one specific part of the business or one particular function. Since this is a relatively new area, products emerge onto the market almost daily so the best place to research what is available is via the Internet.

Some of the different types of products that you might find are described below.

1. **Infrastructure**
   This includes network products, ISP and hosting services, development services, databases management products, development products, specific computer languages and even ASP services providing a total approach.

2. **Online Shopping Carts**
   There are many companies that have developed online shopping cart products. These products tend to service the needs of smaller businesses with little resources to develop their own solutions. They enable the visitor to the web site to utilize a simple concept of the shopping cart to “collect” online purchases from those offered into the shopping cart and then proceed to a “Checkout” just like using a supermarket.

**Case Example**

**Merchant Order Form** [http://www.merchantorderform.com/](http://www.merchantorderform.com/)

MOF is a Perl based shopping cart program. Its features are:

- It can be installed on any server
- It is industry standard CGI program that is stand alone program
- Web based shopping cart with flexible payment methods, design and layout options.
- MOFcart can accept *unlimited* product input and options for size, colour, text, and price.
- MOFcart can accept *unlimited* product input and options for size, colour, text, and price.
3. **Online Payments**

Products for offering online secure payment systems also abound. These products vary from direct online verification of credit card details with either banks, or branded cards through to smart card developments to handle micro-payments for goods.

Most online shoppers use credit cards to pay for their online purchases. But other options such as debit cards – which authorize merchants to debit your bank account electronically – are increasing in use. Other developments in recent years looked at systems to emulate money. “Electronic money” or “e-money” aim to make purchasing simpler. These sorts of products can include “stored-value” cards that let you transfer cash value to a card. Some cards can be “reloaded” with additional value at a cash machine while others are “disposable. The equivalent Internet-based payment systems called “e-wallets aim to allow “micropayments”- very small payments. Most e-wallet by decreases the sales amount from the online balance.

---

**Case Examples**

**FlexeGate**

The FlexeGate Package is a complete online business solution, which comes with the high-end online store system - FlexeGate Store. FlexeGate Store is designed to work for Australian small businesses, and allows easy management for users with no existing online store.

**Some Features of FlexeGate - for, the Merchants**

**Store creation:**

- Build a complete web site including your online shop: Home, About Us, Contact Us, Shop/Products.
- Build just an online shop to integrate with your existing web site.
- Select your choice of colours and use your logo to customize the shop for your corporate image.
- Wizard to help you set up your site/store.
- Unlimited categories.
- Unlimited products.
- Ability to customise stores for international locations.
- Multiple GST/tax rates.
- GST calculated by product to enable some products to be tax exempt.
- Allows Affiliate login - for resellers or important customers.
- Allows for separate billing and shipping addresses.
- Publish your site/store immediately.
PayPal
PayPal lets any business or consumer with an email address to securely, conveniently, and cost-effectively send and receive payments online. Their network builds on the existing financial infrastructure of bank accounts and credit cards to create a global, real-time payment solution. They deliver a product ideally suited for small businesses, online merchants, individuals and others currently underserved by traditional payment mechanisms.

PayPal offers three types of accounts: Personal, Premier, and Business

ALL accounts include these basic features:

- Send and receive money online from a PayPal or checking account
- Earn money market returns on your PayPal balance
- FDIC pass-through insurance up to $100,000
- Email-based customer service

Personal Accounts
- Send money for FREE
- Receive money for FREE (non-credit card payments only)
- Can upgrade to a Premier account at any time

Premier Accounts
- Send money for FREE
- Low fees for receiving money
- No limit on receiving credit card payments
- Exclusive customer service hotline 7 days a week
- Special tools for sellers
- ATM debit card for select users

Business Accounts
- Include all the features Premier accounts
- Can do business under a corporate or group name
- Access to Multiple Logins

4. Online Forms

While online forms can be developed simply using one of the CGI script or Java script language, several products are available that allow the user without these skills to develop their own forms. Online forms can then be used to capture information from visitors to the business’s website such as an order, a request or feedback that can be collated.
Case Example

MycGIScripts.com

They specialize in software solutions which can help a website grow and prosper. They currently offer solutions for website tracking, web promotion, e-commerce and scripts which allow a user to add dynamic content to your website.

Some examples from list of our CGI scripts are:

- **Password protect**: Allow you to very easy protect any directory on unix server
- **Account manager Lite**: Solution for easy management multiply .htaccess files from one admin menu.
- **CSV manager**: This script allows you to add records or to search one or several csv databases.
- **Formmail Pro**: This script allows you to use email forms at your website.
- **File Uploader**: This script is combination of FormMail Pro and file uploader. It can upload unlimited num of files in your server, process forms, have included autoresponder and more.

5. **Knowledge Management Systems**

Many software products are available that enable the knowledge of an organizations to be captured. Products to capture the formal knowledge within an organization are a mixture of packaged software (databases) and tailor-made systems. But the knowledge of an organization is so much more that the formal knowledge. Consider a corporate email application. How many questions and answers are held contained in those emails.? How much “knowledge” is contained in those emails between departments and between customers and staff? But these electronic records are not so easy to analyse or share or maintain.

There is an emerging range of products that serve to improve the ability of organizations to manage both informal as well as formal knowledge.

**Case examples:**

**Wincite.**

Wincite software is a database application that can be accessed from a web browser. While the primary use of the product has been in the areas of competitive/business intelligence for business units of large companies, more recently the product is also being used in connection with knowledge management initiatives, strategic planning, and field sales management. URL: [http://www.wincite.com/index.htm](http://www.wincite.com/index.htm)

**Hummingbird**

Hummingbird Document and Content Management Solutions operate in desktop, Web, and enterprise information portal environment to give organizations the ability to create centralized repositories, or libraries, containing all of the unstructured data they generate. URL: [http://www.hummingbird.com/products/dkm/](http://www.hummingbird.com/products/dkm/)

**4i editions**

Documentum has developed a number of products serving the information needs of organizations within the 4i family of products e.g. 4i eBusiness Platform is an enterprise-wide content management solution that allows organizations to create, manage, personalize, and deliver trusted content on a global scale. URL: [http://www.documentum.com/products/content-management-products.html](http://www.documentum.com/products/content-management-products.html)
Revelation Knowledge management.

Right Now has developed a knowledge base that structures “unstructured” data by clustering and classifying knowledge into information buckets based on historical relatedness. This view of the information allows customers to easily step through groups of related information to find their answers. Staff, customers and whatever partners the organization wants can have. URL: [http://www.rightnow.com/products/response.html](http://www.rightnow.com/products/response.html)
Practice Questions

Q no 1) While the direct costs of an ERP project can be significant there are many indirect costs that also need to be considered. Describe at least 4 cost categories, apart from the cost of the software that need to be considered in an ERP project.

Q no 2) You are the IT Manager and have been asked to provide advice to the Sales Manager about SFA systems. They want to buy a package and have asked what might be available and what it might do for them. Research the web and identify a product that might help them. Describe the product, its advantages and disadvantages. (For answer please refer to Case example SALESNET)

Q no 3) Consider options for online payments. Compare and contrast the following products in terms of what sort of businesses might be interested in each of the solutions.

ii) http://www.paypal.com/
iii) http://www.billpoint.com/

Describe what sort of features businesses should look for in online payments systems. (For answer please refer to case example)

Answer to Q no 1)

Students should recognise that many costs in an ERP project are hidden but can include:

Planning and project management

It takes time and effort to properly prepare for an ERP deployment. The company's IT staff and the appropriate business managers must be given the time and clear responsibility to conceive and evaluate the project's scope, costs, and timeline. It's important to assign the planning responsibilities to staff members who not only have a good grasp of the technology, but who also understand the company's business requirements and processes.

Integration

Companies almost always underestimate the time and cost necessary for enterprise software integration. ERP systems rarely exist in a vacuum and they usually need to be tied into software and complex business processes that predate the ERP system. In addition to software from a primary ERP vendor, the enterprise may also want to use applications provided by other software vendors. For example, a company may want to tie its core ERP suite from SAP into a CRM application from Siebel and global trading management software from Vastera. Mergers and acquisitions also create difficult integration challenges because the merged companies may use different ERP packages and other different applications with which they've already integrated. Dick Kuiper, a vice president with Meta Group, says that a large enterprise typically operates five or more ERP systems and some companies are known to have more than 20 ERP systems.

Dirty data

A number of problems and hidden costs crop up when handling real-world data. When an enterprise converts its legacy systems to ERP, it must convert large amounts of data for use in the new system. Much of the old data is difficult—if not impossible—to convert, which means a lot of time and money will be spent re-entering it into the system or putting it through complex conversion processes. Even after a system is fully deployed, you can't take the data for granted because it ages. For instance, every month some of the company's customers, employees, and business partners change their address or other parts of their profile. Gartner Group analyst Beth Eisenfeld estimates that 2 percent of a company's customer data goes bad every
month. She recommends an ongoing effort to clean up obsolete data. Finally, when data is combined from multiple systems for analysis or as a result of integration projects, more work can be involved to clean it up and convert it.

Testing
Given the mission-critical nature of a company's ERP system, it should be thoroughly tested before it's fully deployed. Don't just test the system with dummy data. Use actual data from different real-world scenarios. For example, a manufacturing company should pull up historic orders from customers and route the orders through the entire process of creating the product, shipping it, and billing for it. Ideally, employees who actually operate the specific business processes on a day-to-day basis should perform these tests. Of course, all of this costs money, but the investment will significantly reduce other costs that result from the downtime and poor implementations that occur when systems aren't properly tested.

Documentation
ERP systems take a long time to deploy and are used for many years within a company. That means they usually outlast the IT employees and business-process managers who conceptualise, deploy, and modify the systems. Documenting the system is crucial so that future employees can make sense of the software and business-process logic the system encompasses. Documentation is also needed to help future workers deal with the inevitable updates, extensions, and integration projects that occur as a company evolves. In addition, documentation can save consultants time and help them map out the scope of projects properly to improve cost accountability.

Training
One of the biggest mistakes enterprises make is forgetting that employees must adapt to a new ERP system. Employees must be trained on how to operate the system and how to apply it to familiar business tasks such as looking up and entering data. Furthermore, a new ERP system almost always means changes to business processes. That requires change management to teach employees about new business practices and manage staff reorganization. Employees often resent change and resist it when it means they have to let go of established work habits and take up new reporting relationships. Despite all the money a company spends, an ERP deployment can fall flat on its face or simply operate at vastly reduced efficiency if the company fails to adequately train the staff and manage the change effectively.

Consulting fees
Since few IT departments are staffed to handle the extra work required to implement each phase of a big ERP project, many of the items mentioned earlier require consultants. Without proper management, though, consulting fees can eat through your budget faster than a pack of mice through a chunk of cheese. It's important to make sure that in-house staff is capable of managing consultants. Consulting contracts should carefully define key deliverables, schedules, skill levels of available staff, and objectives for training internal staff. The contract should also be accompanied by a detailed specification that clearly points out the desired business objective and technical requirements. Proper planning and project management (as mentioned earlier) are important for managing consultants and holding them accountable.

The bottom line on ERP
Although ERP projects are complex and expensive, properly implemented, they are nonetheless worthwhile. Meta Group found that once fully deployed, the median annual savings from a new ERP system was $1.6 million per year. But every ERP system must be continually maintained and upgraded to take advantage of new applications, technologies, and features. ERP software is hardly static, and there are major new developments as the software grows to embrace the Internet and as companies open up their data and business processes to partners.
7 IFAC Guidelines and Discussion Papers

<table>
<thead>
<tr>
<th>Topic List</th>
<th>Syllabus Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.1 Managing Security of Information</td>
<td>1.4</td>
</tr>
<tr>
<td>7.2 Managing IT Planning for Business Impact</td>
<td>1.4</td>
</tr>
<tr>
<td>7.3 Acquisition of Information Technology</td>
<td>1.4</td>
</tr>
<tr>
<td>7.4 The Implementation of IT Solutions</td>
<td>1.4</td>
</tr>
<tr>
<td>7.5 IT Service Delivery and Support Summary</td>
<td>1.4</td>
</tr>
<tr>
<td>7.6 IT Monitoring (Exposure Draft)</td>
<td>1.4</td>
</tr>
<tr>
<td>7.7 Project Executive Checklist</td>
<td>1.4</td>
</tr>
<tr>
<td>7.8 IFAC Discussion Paper - E Business and The Accountant</td>
<td>-</td>
</tr>
</tbody>
</table>

Introduction

Many organizations recognize the potential benefits that technology can yield. Successful organizations, however, understand and manage the risks associated with implementing new technologies. Executive management needs to have an appreciation for and a basic understanding of the risks and constraints of information technology in order to provide effective direction and adequate controls.

Study Guide

Managing Security of Information (Study text reference 7.1)
- You might want to lead a discussion about the core principles and relate it to the students’ experience.

Managing IT Planning for Business Impact (Study text reference 7.2)
- Discuss how this guidelines relates to the work the students’ have already done on IT planning.

Acquisition of Information Technology (Study text reference 7.3)
- Discuss the definitions of this guideline and how it might be adopted by a small business.

Implementation of Information Technology Solutions (Study text reference 7.4)
- This guideline covers a lot of potential scenarios or routes. Lead a discussion to ensure that the students understand the options for implementation.

IT Service Delivery and Support (Study text reference 7.5)
- You might like to lead a discussion to link the work done previously with IT Management and Operations Management to this guideline. Highlight that there are various approached adopted by organisations in terms of the methodologies and standards that they adopt

IT Executive Checklist (Study text reference 7.7)
- Lead a discussion about the problems with IT Projects that have received a lot of press and how this checklist might be applied.

Managing IT Monitoring (Exposure Draft) (Study text reference 7.6)
- IT Monitoring is essential and has an impact on IT governance. This guideline emphasizes the main principles on which IT monitoring should be based as well as provides a generic approach for implementing effective monitoring.
7. IFAC GUIDELINES AND DISCUSSION PAPERS

IFAC IT Committee (ITC) was formed in 1994 to address global IT issues impacting the accounting profession. With many countries already addressing IT issues at a national level, the IFAC ITC agreed that it would promote best practice, encourage sharing of information developed in individual countries and take a leadership role in preparing IT guidance in key business areas.

During the term of the IFAC ITC, several guidelines were developed and have since been published by IFAC. Each title is discussed below and students are encouraged to obtain and read copies of each guideline.

These guidelines can be obtained from the IFAC web site at:
http://www.ifac.org/Store/Category.tmpl?Category=Information%20Technology

7.1 MANAGING SECURITY OF INFORMATION

7.1.1 Introduction

Written in 1998, this guideline provides information about the importance of security to an organization and provides a framework for designing, implementing and managing effective security over information.

In a global information society, where information travels through cyberspace on a routine basis, the significance of information is widely accepted. In addition, information and the information systems and communications that deliver the information are truly pervasive throughout organizations — from the user’s platform to local and wide area networks to servers to mainframe computers. Accordingly, executive management has a responsibility to ensure that the organization provides all users with a secure information systems environment. Sound security is fundamental to achieving this assurance.

Furthermore, there is a need for organizations to protect themselves against the risks inherent with the use of information systems while simultaneously recognizing the benefits that can accrue from having secure information systems. Thus, as dependence on information systems increases, security is universally recognized as a pervasive, critically needed, quality.

The data or information must be protected against harm from threats that will lead to its loss, inaccessibility, alteration or wrongful disclosure. The protection is through a layered series of technological and non-technological safeguards such as physical security measures, background checks, user identifiers, passwords, smart cards, biometrics, firewalls, etc. Security applies to all information.

The objective of information security is “the protection of the interests of those relying on information, and the information systems and communications that deliver the information, from harm resulting from failures of availability, confidentiality, and integrity.”
7.1.2 CORE PRINCIPLES

- **Accountability**: Responsibility and accountability must be explicit.
- **Awareness**: Awareness of risks and security initiatives must be disseminated.
- **Multidisciplinary**: Security must be addressed taking into consideration both technological and non-technological issues.
- **Cost Effectiveness**: Security must be cost-effective.
- **Integration**: Security must be coordinated and integrated.
- **Reassessment**: Security must be reassessed periodically.
- **Timeliness**: Security procedures must provide for monitoring and timely response.
- **Societal Factors**: Ethics must be promoted by respecting the rights and interests of others.

The above principles and security objectives should be implemented by following procedures:

- **Policy Development**: The security objective and core principles provide a framework for the first critical step for any organization — developing a security policy.
- **Roles and Responsibilities**: For security to be effective, it is imperative that individual roles, responsibilities, and authority are clearly communicated and understood by all.
- **Design**: Once a policy has been approved by the governing body of the organization and related roles and responsibilities assigned, it is necessary to develop a security and control framework that consists of standards, measures, practices, and procedures.
- **Implementation**: Once the design of the security standards, measures, practices, and procedures has been approved, the solution should be implemented on a timely basis, and then maintained.
- **Monitoring**: Monitoring measures need to be established to detect and ensure correction of security breaches, such that all actual and suspected breaches are promptly identified, investigated, and acted upon, and to ensure ongoing compliance with policy, standards, and minimum acceptable security practices.
- **Awareness, Training, and Education**: Awareness of the need to protect information, training in the skills needed to operate information systems securely, and education in security measures and practices are of critical importance for the success of an organization’s security program.

Executive management, information systems security professionals, data owners, process owners, technology providers, users, and information systems auditors all have roles and responsibilities in ensuring the effectiveness of information security. Due diligence must be exercised by all individuals involved in the management, use, design, development, maintenance, operation, or monitoring of information systems.

7.2 MANAGING IT PLANNING FOR BUSINESS IMPACT

7.2.1 Introduction

For most organizations, the rapid developments in information technology provide management with an opportunity to develop and implement new or improved products and services. To take advantage of this opportunity, management must first recognize the potential represented by information technologies, and, next, identify and implement information systems which assist in better meeting the organization’s business objectives. Information technology planning, as described in these guidelines, is an effective approach to assist management in this process since it provides:
• a structured basis for evaluating the impact of technologies in the broader context of business objectives and comparative assessment with similar organizations;
• a framework for scheduling necessary information system projects in an integrated manner while recognizing available resources and constraints; and
• assurance that investments in the information system projects are justified in terms of realizable benefits and represent the most appropriate option to the organization.

The objective of the information technology plan is to provide a road-map of the information technology required to support the business direction of an organization, outlining the resources that are required and the benefits that will be realized on implementation of the plan.

7.2.2 **Core Principles**

• Alignment — the plan should support and complement the business direction of an organization.
• Relevant scope — the scope of the plan should be established to facilitate formulation of effective strategies.
• Relevant timeframe — a planning horizon should be formulated that provides long-term direction and short-to-medium term deliverables in a manner consistent with the business strategy.
• Benefits realization — costs of implementation should be justified through tangible and intangible benefits that can be realized.
• Achievability — the planning process should recognize the capability and capacity of the organization to deliver solutions within the stated planning timeframe.
• Measurable performance — the plan should provide a basis for measuring and monitoring performance.
• Reassessment — the plan should be reassessed periodically.
• Awareness — the plan should be disseminated widely.
• Accountability — responsibility for implementing the plan should be explicit.
• Commitment — management commitment in implementing the plan should be exhibited.

Although information technology plans are unique, the planning process and the underlying activities are similar. Usually, the plan will be developed in four phases:

**Phase I: Orientation**

This start-up phase is required to establish the scope of the plan and the methodology and techniques to be applied. In this phase the resources that are required for developing the plan are mobilized. Following steps are involved:

• Establish scope
• Establish methodology/techniques and mobilize resources

**Phase II: Assessment**

The focus of this phase is to establish the broad information technology requirements of the organization and compare these with the current information technology usage. Also, this phase provides an opportunity to identify other potential uses of technologies which may assist in meeting business objectives. Major steps in this phase are: confirm business direction and drivers; review technology trends; outline future requirements; inventory existing information systems; and develop an assessment of what is needed. In the
concluding step of this phase there should be a well-developed assessment of the current and future business needs, the benefits available from implementing technologies, the gap between what is desired and what is required by the organization, and a list of the key issues to be considered in the formulation of the information technology strategies.

**Phase III: Strategic Plan**

This phase commences with developing the vision and desired future positioning of information technology within the organization. This is followed by an analysis of the options that are available with respect to information, applications, technology infrastructure, communications, business process re-engineering, and organizational resources. The option analysis culminates in the selection of appropriate, justified and compatible strategies which, collectively, form the strategic plan.

**Phase IV: Tactical Plan**

In this phase, the selected strategies are divided into a series of projects which are scheduled for implementation depending upon relative priorities and resource availability. The planning process is concluded by recommending a monitoring and control mechanism that will ensure that the plan is implemented in a timely, efficient and effective manner.

The information technology plan is usually prepared under the direction of a steering committee that is headed by the Chief Executive Officer, Chief Information Officer, or another senior business executive.

### 7.3 Acquisition of Information Technology

#### 7.3.1 Introduction

Guided by the IT plan, organizations seek to acquire “the right solution at the right price and at the right time”. The type of acquisition and organization size can influences the acquisition approach and this guideline addresses the various types of acquisition.

The importance of IT related acquisitions is usually directly proportional to their cost, scale and complexity. In general, the larger and more complex the acquisition, the higher will be its impact on, and importance to, the business. In addition, the acquisition may be important to the business due to its interrelationships with other IT projects. Finally, a structured acquisition process, as is described in this guideline, provides a framework for ensuring that:

- there are no major omissions from a business, technical or legal standpoint;
- the costs and resources for the acquisition process are appropriate and are efficiently deployed;
- the validity of the business case in support of the acquisition is reaffirmed prior to selecting a solution; and
- there is progressive buy-in to the new system as a result of user group involvement throughout the acquisition process.

The objective of the IT acquisition process is to *acquire the right solution, at the right price and at the right time*.

#### 7.3.2 Core Principles

- **Alignment** — the acquisition should be consistent with the business and it plans.
• **Relevant requirements** — the objectives, scope and requirements of the acquisition should be clearly defined and documented, including any integration issues that need to be addressed.

• **Obsolescence** — the impact of new and emerging technologies on the acquisition must be considered.

• **Accountability** — responsibilities and accountability for the acquisition must be explicit.

• **Option analysis** — the available options must be identified and assessed.

• **Evaluation** — selection criteria must be established and consistently applied across the alternatives available.

• **Negotiation** — effective negotiation must be conducted before any decision is made.

• **Transparency** — good governance dictates that the IT acquisition process be fair, open and consistent.

The approach to the acquisition process will vary with the nature of the acquisition.

• Where the acquisition is of low value, easy to define and supported by a range of supplier alternatives, a fast-track commodity procurement process can be used.

• Where the acquisition is of high value, but is easy to define and has a range of alternatives, the Request for Proposal-based acquisition process is recommended. Where such acquisitions are not easy to define or the available alternatives are not known, this may be preceded by a Request for Information.

The Request for Proposal-based approach has two phases. In the **first phase**, the acquisition process is initiated. Major steps include start-up and orientation, describing requirements, determining evaluation criteria, documenting the contractual conditions and issuing the Request for Proposal. In the **second phase**, the solution is selected. Major steps include accepting the proposals, establishing the short list, validating the responses, conducting negotiations and selecting the solution.

### 7.4 The Implementation of IT Solutions

#### 7.4.1 Introduction

This guideline provides an overview of various routes for implementing a software solution including systems development and package tailoring.

To take advantage of the great strides being made in the information technology arena, most organizations have now aligned their IT planning with their business objectives and have followed a structured approach to acquiring IT solutions. The approach to implementing IT described in this guideline builds on the previous guidelines and provides:

• an understanding of the critical success factors pertaining to IT implementation; and

• a structured basis for implementing IT solutions.

The following summary explains the basic principles involved and provides a brief outline of how IT implementation projects are to be managed.

IT projects are launched to implement the decisions made in the strategic IT planning phase. An IT project may cover the acquisition and implementation of IT resources such as data, application systems, technical components, facilities and, eventually, the relevant people.
7.4.2 CORE PRINCIPLES

- **Aligned scope** — the scope of the implementation of an IT solution should be aligned with the objectives first developed during the acquisition phase, including any issues of integration and implementation timing.

- **Project management and commitment** — an IT project must be properly managed. To achieve this goal, the human resources allocated to the project need to have experience in project management, technical competence and knowledge of the organization’s business processes.

- **Managing changes, awareness and communication** — when preparing an organization for the implementation of new systems, the issue of change management must be specifically addressed and a communication plan must be established to ensure that all relevant parties are kept informed about the progress of the project.

- **Selection of the relevant implementation methods** — there are several methods for implementing a new IT system. The method chosen will depend on the type of IT development selected. To ensure the successful implementation of the solution developed, it may be necessary to follow elements of several different methods.

- **Implementation phasing** — depending on the method chosen, the phasing of an IT project may either be strict and detailed or more iterative. It is essential, however, to include the following five major project phases: general design, specifications, development, completion (migration and tests) and deployment.

- **Integration** — the final product of the IT project will generally either be a new application system or new technical facilities, which must then be integrated into the existing information system.

- **Risk management and monitoring** — the project risks must be continuously evaluated during the project and alternative contingency solutions identified. To ensure effective project management, performance indicators must be established and reviewed regularly. Regular management reporting is also essential.

Although projects involving IT implementation vary depending on the context and IT resources involved, the major underlying phases remain similar. Following are the general phases in an implementation process.

**Project level**

General design and mapping — this phase includes the integration of the project with the overall existing information system and the definition of the method or methods to be followed.

**Methodological level**

Detailed specifications — this phase includes translating user requirements into detailed specifications. Depending on the method or methods chosen, this may be included in the prototyping exercise.

Development — this is mainly the coding or the customization of the system with relevant documentation (technical and user). Testing is also performed at a technical level.

**Project level**

Completion — this refers to the tests the users perform on the completed system after it has been integrated into the overall information system.

Deployment — this is the final phase where the system is implemented. All users are trained and any final changes are made.

The organization’s process owner(s) should have the prime responsibility for making overall decisions, as long as the sponsor agrees. All project steering committees report to the IT strategic committee, which is in charge of all IT planning and overall management.
7.5 IT SERVICE DELIVERY AND SUPPORT SUMMARY

7.5.1 Introduction

The IT Management Series provides Statements of Best Practices associated with the management of information technology (IT). While there are many methodologies and approaches to IT management, this series addresses the topic under the broad headings:

- Planning and Organization
- Acquisition and Implementation
- Delivery and Support
- Monitoring

This series also includes the actual processing of data by applications in line with the COBIT approach. This guideline should, therefore, be read in conjunction with the other titles in the series for an overall appreciation of the issues associated with IT management.

7.5.2 Core Principles

- **Accuracy** — information delivered to the business must be accurate and timely.
- **Awareness** — training, education and support services are provided to all IT staff and IT customers.
- **Cost effectiveness** — systems and facilities should be aligned with business needs and not put undue financial burdens on the organization.
- **Customer-focused** — the organization's systems should be easy to operate and supportive of its business operations.
- **Disciplined approach** — information technology should have adequate controls, a well-defined structure and consistent policies and procedures.
- **Flexibility** — systems and facilities should exhibit a degree of flexibility to cater for fluctuations in business volumes and staffing levels and, wherever possible, be capable of being easily modified to handle changes in business practices.
- **Meeting performance expectations** — the delivery of, and support for, IT services must meet the expectations of IT customers, be available at agreed-on times and be measurable and measured.
- **Protected environment** — business data and the facilities and information systems used to process them should be safe and secure. The environment should also offer a safe working environment for IT customers and staff.
- **Relevance** — the systems and facilities should be appropriate and aligned with the organization's business needs. They should also be fit for purpose and conform to the user requirements.
- **Reliability** — information systems should be robust and reliable.

Delivery and support infrastructure for information technology must be available when the organization is about to deploy information technology. Such delivery and support mechanisms need to cover service level management, management of third-party services, performance and capacity, business continuity, security, budgets and cost allocation, training, customer service, configuration management, problem reporting, data
management, facilities management and operations management. The majority of processes will, however, be performed almost daily and will require regular monitoring and review.

The delivery and support of an organization’s IT services is normally the responsibility of the Chief Information Officer and senior IT management.

To manage the delivery and support of IT services, we need to understand the expectations of the organization, its IT customers and, in particular, its senior management. These needs will vary according to how the organization uses technology but may include:

- availability of services and facilities as and when required;
- accessibility to information as and when required;
- confidentiality and security of data;
- good performance of systems and facilities;
- timely training;
- appropriate tools and facilities;
- help and support when required;
- problems and requests for enhancements resolved promptly.

Managing the IT services and processes to ensure that IT customers are satisfied involves delivering effective services, providing support and maintaining a reliable IT infrastructure.

7.6 IT MONITORING (EXPOSURE DRAFT)

7.6.1 Why monitor IT?

Information, and the systems and communications that deliver the information, are truly pervasive throughout today’s organizations. Executive management has a responsibility to ensure that the organization monitors its use of information and information technology (IT). IT monitoring is fundamental to IT governance and part of management’s stewardship responsibility to make certain that what was agreed to be done is being done and is being done in line with directions and policies set by the board. Monitoring is needed to make sure that those to whom responsibility has been delegated are doing the right things, are doing them right and can be held accountable if they do not.

7.6.2 What is IT monitoring?

Those responsible for IT governance need first to set measurable goals, then delegate the execution to executive management and, finally, regularly verify that performance matches the goals. If goals and measures are not in line, the governance body needs to take corrective action, provide redirection or, possibly, reconsider the original goals. Monitoring of IT is enabled by the definition of relevant performance indicators, the systematic and timely reporting of performance and prompt acting on any deviations identified. IT monitoring is especially important because of the complexity and risk involved in IT activities. It has the business goals of ensuring the delivery of information to help the organization achieve its objectives and ensuring the achievement of performance objectives for the IT function.
IT monitoring covers:

- how IT sustains the business with operational processes and risk and control systems;
- whether IT complies with business strategy, standards and policy;
- how IT improves the business with technology, process and organizational changes; and
- how IT supports enterprise growth through process knowledge and service capability.

### 7.6.3 **Key/Core Principles**

While IT monitoring processes are unique to the needs and circumstances of each organization, they are generally developed using seven core principles.

- **Comprehensiveness** — any monitoring activity has to be comprehensive, based on simple and consolidated measures focusing on exceptions.
- **Relevance** — any monitoring activity has to be relevant to the mission, vision, goals and strategy of the enterprise.
- **Acceptability** — an effective monitoring approach has to be acceptable to those being monitored, this means not invading their privacy and not intruding into their day-to-day responsibilities.
- **Timeliness** — to make correct and expedient decisions, monitoring data must be available to detect deviations that need to be reported immediately.
- **Verifiability** — information obtained by the monitoring process should be verifiable by other means – thus, it should be accurate and, whenever possible, it should be based on fact.
- **Action-oriented** — any form of monitoring must enable expedient corrective action.
- **Flexibility/adaptability** — the monitoring system should be easily adaptable to provide accurate, relevant and timely information in a changing environment.

### 7.6.4 **What tools are available?**

While many IT monitoring tools are available, management is effectively using seven key tools in performing IT governance responsibilities:

1. traffic light reports to follow up on projects and strategic initiatives;
2. performance management through balanced scorecards (and dashboards);
3. benchmarking for decision making relative to IT investments for risk and control;
4. active monitoring of the IT infrastructure;
5. brainstorming for risk management and improvements;
6. internal and external audit for independent assurance;
7. management reporting for executive management review.

1. **Traffic light reports to follow up on projects and strategic initiatives**
Traffic light reports have become a preferred reporting mechanism for executives and boards. They exemplify the principle of comprehensiveness and the practice of exception reporting. They provide a “green” condition when the committed action is on schedule and on budget. When issues are known that suggest that the commitment might go over budget or schedule, or might not achieve all of its objectives in the future, an “orange” condition is reported. When budgets or schedules are exceeded, or when it is clear that goals will not be achieved without major changes or investments, then a condition “red” is provided. These commitments can be of different types, such as:

- a project,
- an improvement initiative, or
- the closure of an audit recommendation.

2. **Performance management through balanced scorecards (and dashboards)**

IT management is increasingly applying the balanced scorecard method (Kaplan, Norton) and performance dashboards to the measurement of the value and overall contribution delivered by IT. In this method, alignment is achieved between business and IT plans through visible alignment of IT goal (outcome) measures of IT processes and the business goals they support. They also identify the key performance indicators (drivers) of success for each process.

Management implements a set of measurement and monitoring activities to collect information on the achievement of the outcomes using the goal measures and on the performance of IT processes using the key performance indicators. This information, and the correlation of results over time, enable IT management to determine whether its IT strategies and approaches are effective and to decide on corrective or adjusting actions as appropriate.

3. **Benchmarking for decision making relative to IT investments for risk and control**

Maturity modeling and benchmarking are other management practices for monitoring the return of investment and risk mitigation of IT. Maturity models provide for measurable, recognizable levels of maturity, for example, in control maturity, risk management, operational proficiency, etc. On these scales, an enterprise can define where it is (As-Is) and where it wants to be (To-Be). This can then drive strategy and help decision making on improvement projects. Monitoring these improvements and regularly reassessing the enterprise’s maturity level through benchmarking (i.e., comparing it to where others are) are becoming best practice in management monitoring in the domain of IT.

4. **Active monitoring of the IT infrastructure**

Concern for IT infrastructure risks at enterprise and national/international levels has changed how IT security and risk are being managed. Awareness that the traditional approach of defining policy, selecting safeguards and implementing them is too static for a highly volatile environment has pushed organizations into a more fluid continuous approach of actively monitoring the IT infrastructure. This consists of continuously monitoring and performing self-assessments to detect and then fix the problems identified. Results of this monitoring activity need to be brought to top management’s attention when appropriate, and management needs to give guidance on when notifying management is appropriate and when not.
5. **Brainstorming for risk management and improvements**

Apart from the above techniques, for the most part, only high-risk enterprises will implement processes and assign responsibilities to monitor enterprise risks on a continuous basis. A cost-effective alternative exists in well-prepared and facilitated risk brainstorming sessions between top management and those responsible for IT, security, risk and audit. These brainstorming sessions might be performed, for example, on an annual basis and the professionals involved should prepare and document a list of the most important vulnerabilities and threats for consideration.

6. **Internal and external audit for independent assurance**

Internal and external audit reports are key monitoring tools for executive management. These reports should include a statement of the audit objectives, a description of the audit scope and methodology, the period of coverage and the nature and extent of the audit work performed. The report should include a full discussion of the audit findings and conclusions, the cause of the problem areas noted in the audit and recommendations for actions to correct the problem areas and improve operations. The report should include a statement that the audit was made in accordance with generally accepted auditing standards and disclose, when applicable, standards that were not followed.

7. **Management reporting for executive management review.**

Management reporting is an essential element of IT governance. Executive management should receive, for review, reports on the organization’s progress toward identified goals. It should also receive status reports on the extent to which planned objectives have been achieved, deliverables obtained, performance targets met and risks mitigated. Once the reports have been reviewed, management should ensure that any required remedial actions are taken in a timely manner.

7.6.5 **What is the best approach?**

Although monitoring of IT is unique to the organizational environment, the monitoring process and the underlying activities are similar. Usually, the process consists of the following six phases:

I. **Phase I: Orientation.**
   This start-up phase is required to determine the scope of monitoring and the methodology and techniques to be applied. In this phase, the resources required for monitoring IT are mobilized.

II. **Phase II: Criteria Definition.**
   This phase is regularly covered in the planning/design phase of each IT and business process. Goals or performance measurement indicators are set up for monitoring.

III. **Phase III: Ongoing Monitoring.**
   Ongoing monitoring is a continuous supervisory function over key IT activities and control processes. Exceptional events have to be identified and tracked. Performance measures need to be established, involving both IT and the stakeholders, aligned with the strategy and reviewed on an ongoing basis.

IV. **Phase IV: Separate Periodic and Ad Hoc Monitoring.**
   Besides ongoing monitoring, separate periodic and ad hoc monitoring is vital to ensure the ongoing monitoring and other control functions operate properly, to periodically review IT-related risks and
opportunities and to obtain comfort relative to major IT decisions. Periodic monitoring includes internal audit procedures, external assurance, self-assessments and brainstorming sessions.

V. Phase V: Subsequent Actions.
Subsequent actions include corrective actions to redirect IT activities and processes and bring them back in line with goals, strategy and policy; minimization of adverse effects; refinement of goals and measures; changes to strategy, policy and standards; and initiation of reassessment activities.

VI. Phase VI: Reporting.
For monitoring to be able to support effective IT governance, management reporting about all phases of the monitoring process, including subsequent actions and escalation procedures, is an essential element of the recurring/iterative control cycles.

Everyone who has a specific role and/or responsibility for achieving IT goals and processes must be involved in monitoring IT. Effective monitoring involves the entire organization, as information is captured, consolidated and reported up the various management levels.

7.7 Project Executive Checklist

7.7.1 Introduction

There are many well-known cases of significant failures of information technology and communications infrastructure projects, of major IT investments having to be abandoned before completion and of IT projects which have been completed, but then found to be inappropriate to the needs of the business.

In the US, a survey of IS auditors found that, of completed projects, some 30–40 per cent exceed their budget and overrun time schedules by two or three times. In the UK, the IT Skills Forum found that 70 per cent of users believe that they obtain inadequate return on their IT investment.

Analysis of the problems with IT projects suggest that better estimation of time, scope and resources coupled with improved planning, monitoring and control could greatly increase the success rate of such projects.

An important element in ensuring that projects achieve their desired results is for senior management to take a more proactive involvement during the key project stages.

These key stages can be defined as:

- proposal approval
- selection of product and supplier
- analysis and planning
- implementation
- post-completion review

This checklist covers the first stage, proposal approval, and provides some of the questions which senior managers should ask and seek adequate answers to before authorising any investment in an information technology project and the related communications support.
The questions in this checklist have been grouped under the following headings.

1. The strategic dimension
2. Checking the benefits
3. Appraising the project
4. Managing the change
5. Managing the risk
6. Legal compliance
7. Security issues

1. **The strategic dimension**

They are designed to ensure that such strategies exist, are relevant to the business and that all relevant parties are fully involved and committed

1. Do you review the information and communication needs and flows through the business?
2. Are you reviewing your information and communication strategy and systems as frequently and as rigorously as you should?
3. Do you periodically benchmark your business and information systems against peers and competitors?
4. Are you kept regularly informed of new business opportunities which developments in technology are bringing?
5. Are the business and information managers fully aware of the plans and strategy of the organisation?

2. **Checking the benefits**

They are designed to ensure that benefits have been clearly defined and identified and that, on completion, they can be realised

1. These questions focus on the expected benefits of the project. They are designed to ensure that benefits have been clearly defined and identified and that, on completion, they can be realised
2. Does the project help achieve the strategic objectives of the business?
3. What benefits and improvements can be expected from this project and how will they be measured?
   - Have the qualitative benefits been identified?
   - What are the quantitative benefits and how will their realisation be evidenced?
   - Do the realised benefits justify the project life cycle costs?
4. Which business processes will be improved and how will customers benefit?
5. Does the technical functionality of the proposed business solution adequately meet the needs of all the cross-functional groups affected?
6. Will the proposed system be used by external organisations e.g. suppliers, customers? If so, what benefits will accrue to them?
7. Does the proposed system provide user access to all those who need it and when they need it?
8. Have satisfactory controls to protect the business been incorporated in the system design? Are they auditable?

3. **Appraising the project**

They are designed to ensure that all aspects of the project have been thoroughly evaluated and that the optimal solution has been selected.

1. These questions focus on the appraisal mechanisms used to establish the viability of the project. They are designed to ensure that all aspects of the project have been thoroughly evaluated and that the optimal solution has been selected.
2. Has a detailed business case, supported by resource and technical plans, been prepared?
3. Has a proper project proposal been prepared?
4. What is the anticipated life cycle of the technology being proposed?
5. What is the life cycle of the technology and what are the life cycle costs of the project?
6. Has a feasibility study been carried out evaluating alternative solutions in terms of cost/benefit and other operational criteria?
7. Can the operational management of the proposed system be handled by the users themselves with minimal IT department support?
8. Is the data capture for the system done once and once only?
9. Are there any connectivity issues if interface is required from more than one operating division or business partner?

4. **Managing the change**

They are designed to ensure that all aspects of the transition to the new system are delivered with the full involvement of all interested parties and with minimal disruption to the business process undergoing the change.

1. Are the people involved in the project development and implementation capable and reliable?
2. Have effective means of communicating developments and progress to all staff been put in place?
3. Have the role, responsibilities and time commitment of the people involved been clearly set out and accepted by them?
4. Is there a procedure for issues management?
5. Are there sufficient resources to implement the new project and concurrently support the old system adequately?
6. Are there any staff development (e.g. training/ retraining/redeployment) issues which need to be addressed?
7. What are the training costs, including on-the-job training?
8. Can the in-house MIS function deliver the system in its entirety? Otherwise have satisfactory arrangements been made for third-party resources?

9. Have appropriate agreements and arrangements been put in place for all aspects of user support?

10. Have users been notified of the support arrangements and do they understand them?

5. **Managing the risk**

They are designed to ensure that risks are clearly identified and the impact of any potential failure has been evaluated and suitable strategies established for its resolution

1. What can go wrong with the project, and why, i.e.:
   - proven technology?
   - capable and experienced supplier?
   - in-house product methodology experience?
   - resource constraints?
   - robustness of cost estimates?
   - mission critical process?
   - time deadlines?

2. What would happen if it does go wrong, and how disruptive would it be?

3. What can be done about it and is it enough?

4. Has an action plan been prepared detailing the ‘who, when and what’?

6. **Legal compliance**

It is designed to ensure that all relevant statutory matters have been identified and compliance mechanisms defined.

1. Have the legal and regulatory aspects of the system been appraised (e.g. data protection, health and safety requirements?)

7. **Security issues**

They are designed to ensure that the system is available when required and that data and information are protected against unauthorised access or modification.

1. Will the proposed system be available and ready for full use whenever required? How will the business cope with any prolonged systems failure?

2. Will the data and information in the proposed system be disclosed only to those who have a right to know it?

3. How will the data and information be protected against unauthorised modification?

4. What facility will there be to identify unauthorised access, abuse or misuse by staff or third parties?
7.8 IFAC DISCUSSION PAPER - E BUSINESS AND THE ACCOUNTANT

7.8.1 Introduction

This document presents certain risk management aspects of e-business relevant to accounting and financial reporting from a managerial perspective. Although it includes a short description of the major risks and opportunities associated with e-business, it focuses particularly on the management of IT risks in relation to accounting information. Furthermore, this document envisages a useful framework of concepts with which accountants and others can analyze e-business from an accounting point of view. Based on this framework of concepts, the document provides guidance to accountants on principles and criteria for accounting systems in an e-business environment.

7.8.2 E-Business Risks and Opportunities

1. E-Business Opportunities

E-business through the Internet offers significant opportunities. Because these opportunities are similarly available to the competition, they also represent concomitant risks. Examples of such opportunities (and concomitant risks) include:

I. Competition:

Through the creation of a website, a business can compete locally in traditional industries, as well as regionally, nationally and globally. The Internet permits an entity to effectively target niche markets or areas of specialty and to service broad markets in a cost-effective manner. The Internet also permits both economies of scale (to become a high-volume global supplier with low costs) and economies of scope (through product specialization).

II. Marketing:

With the exception of certain national and international retailers and suppliers, traditional marketing has been concentrated locally or regionally. And, until recently, marketing efforts have been focused on traditional media, such as television and newspapers for consumer products and trade magazines or trade shows for industrial products. Through the Internet, marketing can be targeted to selected customers based on customer registration information, past purchase history or other criteria.

III. Cost Reduction:

E-business facilitates implementation of new business models, including supply chains, service and support arrangements and the creation of cost-effective alliances. It also offers profit-enhancing changes through cost reduction, such as:

- Virtual warehousing.
- Vertical integration.
- Electronic delivery of goods and services.
- Automated order processing.

Classic business approaches generally do not fit well with the new e-business models described in the third section of this paper. These new models are increasingly centered on the customer or consumer. For
example, many customers now expect goods and services to be delivered 24 hours a day from anywhere in
the world. The ability to meet customers, discuss their needs with them, demonstrate products and perform
other activities that traditional businesses use to differentiate their services may no longer be available to
the same degree.

2. E-Business IT Risks

Since e-business invariably involves the use of the Internet through IT, the most important risks associated
with e-business are IT risks. It should be recognized, however, that IT risks are inextricably related to the
risks associated with the opportunities mentioned. The following IT risks can be distinguished: IT
infrastructure, IT application and IT business process risks.

IT infrastructure risks relate to the adequacy of the IT infrastructure for information processing. For
example, hardware may be susceptible to malfunction. IT infrastructure risks are addressed by a security
concept geared to the needs of the entity and by technical and organizational controls defined on this basis.

Typical IT infrastructure risks include:

- Inappropriate physical security measures that do not prevent theft, unauthorized access or
improper disclosure of information;
- Vulnerability to overheating, water, fire and other physical risks;
- Inadequate or improper emergency plans and procedures;
- Absence of adequate back-up procedures;
- Inadequate configuration and monitoring of firewalls against intrusion attempts; and
- Inadequate encryption.

IT application risks result from:

- Bugs and errors in IT applications;
- Uncoordinated or undocumented program changes;
- Inadequately designed input, processing and output controls in IT applications; or
- Inadequate procedures to ensure software security in connection with the security
infrastructure (inadequate access authorization concepts and data back-up and restart
procedures).

Typical IT business process risks in an e-business environment include:

- Transaction data are not transmitted efficiently, completely or accurately from the e-business
subsystem to the accounting application;
- Safeguards protect only a certain subsystem from unauthorized or unapproved transactions
and, thereby, allow transaction data to be modified by one of the downstream IT subsystems;
- Improper or inadequate access control mechanisms may make it difficult or impossible to
effectively manage access controls for all IT subsystems integrated into the e-business process;
- Access protection that responds to a single IT application integrated into the business process
could be bypassed deliberately by manipulating the upstream or downstream IT subsystems;
- Back-up measures are effective for only the e-business subsystem and, hence, for the
subprocess, but not for the entire IT business process; and
- The design and implementation of interfaces between the e-business subsystem and
downstream IT subsystems may not be appropriate.
3. **E-Business Legal Risks**

Management is responsible for ensuring that e-business operations are conducted in compliance with applicable laws and regulations. Some of the relevant legal issues include:

- Protection of intellectual property, including patent, copyright and trademark laws;
- Enforceability of contracts with Internet service providers; and
- Ownership of software by a software vendor or the right of a software vendor to sell software licenses.

Commercial legal risks also arise in connection with contract law and the purchase and sale of goods and services through the Internet across national boundaries. Management is also responsible for ensuring the privacy of personal information obtained as part of the enterprise’s e-business activities. To help ensure privacy of personal information, management can establish controls to limit the risk of breaches of web security.

### 7.8.3 E-Business Systems and the Use of E-Business Systems in Enterprises

The use of the term *e-commerce* has already been superseded by the term *e-business*. E-commerce can be described as the procurement and distribution of goods and services over the Internet using digital technology. The more encompassing term e-business can be defined as including all activities carried on by a business via the Internet. This definition for e-business extends beyond the definition of e-commerce by encompassing a digital approach to the whole enterprise, including other parts of the IT system and other non-transactional activities, such as recruiting employees via the Internet. Because the mere definition of e-business does not fully convey the complexity of e-business reality, it may be useful to explain e-business in terms of the phases of an evolutionary process.

Business models such as B2C and B2B have been widely referred to in the business media. Several new models have emerged; a summary of the current models is:

<table>
<thead>
<tr>
<th></th>
<th>Government</th>
<th>Business</th>
<th>Consumer</th>
<th>Employee</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Government</strong></td>
<td>G2G</td>
<td>G2B</td>
<td>G2C</td>
<td>G2E</td>
</tr>
<tr>
<td><strong>Consumer</strong></td>
<td>C2G</td>
<td>C2B</td>
<td>C2C</td>
<td>X</td>
</tr>
</tbody>
</table>

The key models can be described as follows:

- **B2C** (Business to Consumer) — typically a retailer selling directly to the consumer; at present, this is the sector that has shown the fastest growth (lately B2B has shown the most growth potential — the B2C growth rate now appears to be decelerating).
- **B2B** (Business to Business) — typically a business selling up, down or across the supply chain, involving business partners or business consortia.
- **B2E** (Business to Employee) — typically a system enabling intercompany (intragroup) e-mails over the Internet to be directed to the correct department.

Examples for two of the other models would be:

- **B2G** — Electronic submission of corporate tax returns.
E-business requires modern IT, which in turn necessitates an integrated consideration of the organization of business processes and IT implemented for this purpose. Hence, it is useful to analyze and describe the IT system from the perspective of the business processes using IT (IT business processes). An IT system includes the following basic elements:

- IT business processes;
- IT applications; and
- IT infrastructure.

The IT control system controls how these elements operate together to achieve their objectives while reducing risk to a tolerable level.

### 7.8.4 E-Business Accounting Principles and Criteria

Management is responsible for the attainment of the enterprise’s objectives in accordance with the business strategy it has defined.

It is important that management implements IT controls that operate effectively to help ensure that an IT system performs reliably. Information generated by an IT system will be reliable where that system is capable of operating without material error, fault or failure during a specified period. This also applies to accounting information. The following principles may be used to evaluate whether processed accounting information is reliable:

- Principles for accounting information security; and
- Principles for appropriate accounting information processing.

#### 1. Principles for Reliable Accounting Information

**I. Principles for accounting information security**

IT systems are more likely to yield reliable accounting information when they meet the following security requirements.

- Integrity.
- Availability.
- Confidentiality.
- Authenticity.
- Authorization.
- Non-repudiation.

The preceding security requirements also help serve to meet the need for the privacy of information. In an e-business environment, securing privacy of information has become a necessity.

**II. Principles for appropriate accounting information processing**

The principles for appropriate accounting information processing are fulfilled where the e-business system and the entire IT system safeguards comply with the following general criteria for the input, processing, output and storage of information and data about e-business transactions:

- Completeness;
• Accuracy;
• Timeliness;
• Assessability;
• Order; and
• Inalterability (logging of alterations).

The completeness criterion refers to the extent and scope of processed e-business transactions, i.e., the recipient of transactions determines that all transactions are input completely into the e-business system.

In accordance with the accuracy criterion, processed information should accurately reflect e-business transactions, i.e., recorded transactions should reflect the actual events and circumstances in conformity with the applicable financial reporting framework.

Under the timeliness criterion, e-business transactions should be recorded on a timely basis, i.e., as soon as possible after the transaction has occurred.

Under the criterion of assessability, each item and disclosure in the financial statements should be verifiable in that it can be traced back to individual entries in the books and records and to the original source documents that support that entry.

In accordance with the criterion of inalterability, no entry or record may be changed after the posting date so that its original content can no longer be identified, unless the change to the original content can be identified by means of a log of such alterations.

Before accepting a transaction for processing, it would be useful to verify the following:

• That all transaction details have been entered by the customer;
• The authenticity of the customer;
• The availability of the products or services to be supplied;
• The reasonableness of the order, for example, to identify an unusually large quantity resulting from an input error, or to identify erroneous duplicate orders;
• The pricing structure applied, including delivery costs, where appropriate;
• The method of payment or credit worthiness of the customer; and
• The non-repudiability of the transaction in that its author cannot later deny having entered into it.

2. The Criteria for a Functioning Accounting System

I. Source document entry function

For automatically generated e-business transactions, the source document entry function may also be satisfied by demonstrating that the accounting process itself links the specific transaction with its entry. Process evidence can usually be furnished by the following:

• Documentation of the program’s internal entry generation rules;
• Evidence that these generation rules have been subject to an authorized modification procedure (including access protection, application control, testing and release procedures); and
• Evidence that entries have actually been made in accordance with these rules.

How the source document entry function is actually implemented depends on the structure of e-business processes. When a transaction is recorded, the entry of at least the following information is important:

• A sufficient description of the transaction (a description of the transaction or a key representing such a description);
• The amount entered or details of quantity and value which determine the amount entered;
• The date of the transaction (voucher date, accounting period); and
• Confirmation (authorization) by the person responsible for keeping books of account.

II. Journal function

The journal function provides that all transactions posted into the books are recorded completely and in an understandable manner in chronological order as soon as possible after they have occurred (usually in a journal).

III. Ledger function

The ledger function provides that transactions recorded in chronological order in the journal are also organized by type of asset, liability, revenue or expense in accounts. In accounting systems, the journal and ledger functions are usually combined. In integrated software, these functions may be supported by automatic account assignment processes. The ledger function presents transactions separately for the general ledger and subledgers, generally with the following information:

• Name of account;
• Entry identifier;
• Credit and debit totals and balances;
• Entry date;
• Voucher date;
• The account representing the other side of the accounting entry;
• Voucher reference; and
• Entry description or code.

Furthermore, it may be useful if the following information is presented by the ledger function:

• Credit card approval number;
• Packet information to substantiate receipt, etc.; and
• Digital signature information to enforce the contract.

3. Documentation

A prerequisite for the transparency of the e-business and IT system is adequate procedural documentation that contains a description of all of the system elements needed to understand the e-business process. An expert third party is able to assess the appropriateness of complex procedures only if he or she has access to informative documentation to supplement input data and processing results.

For example, technical system documentation contains information about the following:

• The purpose of a software module in connection with other modules;
• Data organization and structures (structure of data records or tables in databases);
• Modifiable elements of tables that are used to generate entries;
• Programmed processing procedures, including the input and processing controls in place;
• Programmed error routines;
• Keys;
• Interfaces to other systems and the specific data exchanged; and
• Edit routines and the actions initiated (e.g., halt processing, create an error message, etc.).

Technical system documentation is generally supplemented by documentation of the proper application of the system. This relates to:
• Back-up processes;
• Business continuity processes, including ISP processes;
• Processing verification (processing and reconciliation logs);
• Description of the procedures for releasing new and modified programs; and
• List of available programs with evidence of the program version.

4. **Retention Requirements for E-Business Transactions**

Typical storage techniques are optical storage (microfilm), electronic storage (storing data in digital form on magnetic data carriers) and digital optical storage (storing an optical image on electronic media).

The related technical and organizational requirements include:
• Inalterability of a digitalized document;
• Back-up copies of files;
• Organizational arrangements for the digitalization procedure to monitor completeness and reproduction quality; and
• Indexing processes that allow the digital document to be matched to the transaction.

**7.8.5 Conclusion**

Management sets the enterprise’s e-business objectives to help meet the overall business objectives. To attain the enterprise’s e-business objectives and manage the risks and opportunities identified, management brings its IT strategy in line with its e-business strategy and establishes an appropriate IT control system. The IT strategy also depends on the complexity and diversification of the enterprise’s e-business activities and organizational structure and would include an evaluation of IT risks resulting from e-business activities that may affect the accounting system and the financial statements.

The risk-driven approach to managing IT risks in an e-business environment can be depicted as follows:

IT risks may also endanger the continuing existence of enterprises (the going concern problem) whose business activities are highly dependent on IT. Such risks should be identified, analyzed and assessed by the risk management system.

IT business processes, applications and infrastructure can be regarded as an integral part of the IT system. Consequently, IT business processes may directly affect the accounting system and, hence, the reliability of any information or data that it produces. This means it is important that information security and processing requirements be considered when designing IT business processes. These considerations naturally lead to an IT business process-driven perspective of IT risk management.
## Information Technology Security Control and Management

8. IT Control Frameworks

9. IS Risk Management

10. IS Organizational Issues

11. Control Activities I

12. Control Activities II

# IT Control Frameworks and Objectives

## Introduction

There was some information about controls and security in Module D. This module builds on the knowledge gained there and students must ensure that they don’t have any outstanding questions or issues.

In recent years, increased attention has been devoted to internal control by auditors, managers, accountants, and legislators. Five recently issued documents are the result of continuing efforts to define, assess, report on, and improve internal control. They are:

- The Information Systems Audit and Control Foundation's **COBIT** (Control Objectives for Information and related Technology),
- The Institute of Internal Auditors Research Foundation's Systems Auditability and Control (**SAC**),
- The Committee of Sponsoring Organizations of the Treadway Commission's Internal Control - Integrated Framework (**COSO**), and
- The American Institute of Certified Public Accountants' Consideration of the Internal Control Structure in a Financial Statement Audit (**SAS 55**), as amended by Consideration of Internal Control in a Financial Statement Audit: An Amendment to SAS 55 (**SAS 78**).

We have discussed only COBIT and COSO as being more relevant and widely used.

## Topic List

<table>
<thead>
<tr>
<th>Topic</th>
<th>Syllabus Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1 Internal Controls Frameworks: COBIT® and COSO</td>
<td>1.2</td>
</tr>
<tr>
<td>8.2 Summaries of the Documents</td>
<td>2.2</td>
</tr>
<tr>
<td>8.3 SAS 80</td>
<td>2.2</td>
</tr>
<tr>
<td>8.4 COBIT</td>
<td>2.2</td>
</tr>
<tr>
<td>8.5 The COBIT framework</td>
<td>2.2</td>
</tr>
<tr>
<td>8.6 Control Objectives</td>
<td>2.2</td>
</tr>
<tr>
<td>8.8 COBIT Management Guidelines</td>
<td>2.2</td>
</tr>
<tr>
<td>8.8 COBIT Audit Guidelines</td>
<td>2.2</td>
</tr>
<tr>
<td>8.9 WEBTRUST</td>
<td>2.2</td>
</tr>
<tr>
<td>8.10 Control Objectives</td>
<td>2.2</td>
</tr>
</tbody>
</table>
IT Control Objectives (Study Text Reference 8.3 & 8.10)

- Discuss the need for controls to assist IT Management meet their responsibilities.
- Students should be able to provide a definition based on the one supplied in the COBIT guidelines but not word for word.
- This section should explain why we have controls. It is important to stress that even controls should have objectives.

Control frameworks (Study Text Reference 8.2, 8.3, 8.4, 8.9 & 8.10)

- Discuss why controls are needed. Ensure that students do not start focusing on particular IT control procedures until they have identified the “big picture”, organisational requirements for control, which stem from the need to safeguard the business.
- You should discuss the importance of the associations mentioned and the reason why students may want to consider joining them after qualifying.
- You may want to set groups of students the task of visiting a site and then giving a preparation to the rest of the group on a particular topic such as WebTrust or COBIT.
- Explain what “auditing around the computer” (that is, only auditing the input and output and ignoring what the computer does) means and why this may not be suitable in today’s environment.
8. **IT CONTROL FRAMEWORKS**

As the use of IT grew so did the need for standards in the IT audit area. Also IT auditing recognized as requiring specialist knowledge and services for practitioners. In the late 60’s the EDP Auditors association (EDPAA) was founded. EDP stands for Electronic Data Processing and was then the common term for computer systems.

In 1994 to reflect the change in emphasis in the computer industry from just processing data to the management of information the EDPAA changed its name to the Information Systems Audit and Control Association (ISACA) Check Objectives for information and Related Technology. This focuses on ensuring that control processes are related to business objectives and support these. Elements of COBIT can be downloaded from the ISACA web-site.

As the public and organizations start relying on other people’s systems there is a need to fell confident about these systems. There are assurance services that an organization can subject its systems to so as to demonstrate their commitment to secure systems.

8.1 **INTERNAL CONTROLS FRAMEWORKS: COBIT® AND COSO**

In recent years, increased attention has been devoted to internal control by auditors, managers, accountants, and legislators. Five recently issued documents are the result of continuing efforts to define, assess, report on, and improve internal control. They are:

- The Information Systems Audit and Control Foundation’s **COBIT** (Control Objectives for Information and related Technology),
- The Institute of Internal Auditors Research Foundation's Systems Auditability and Control (SAC),
- The Committee of Sponsoring Organizations of the Treadway Commission's Internal Control - Integrated Framework (**COSO**), and
- The American Institute of Certified Public Accountants' Consideration of the Internal Control Structure in a Financial Statement Audit (*SAS 55*), as amended by Consideration of Internal Control in a Financial Statement Audit: An Amendment to SAS 55 (*SAS 78*).

COBIT (1996) is a framework providing a tool for business process owners to efficiently and effectively discharge their IS control responsibilities.

A comparison of the five documents reveals that each builds on the contributions of the previous documents. COBIT incorporates as part of its source documents both COSO and SAC. It takes its definition of control from COSO and its definition of IT Control Objectives from SAC. SAC embodies the internal control concepts developed in SAS 55, COSO uses the internal control concepts in both SAS 55 and SAC, and SAS 78 amends SAS 55 to reflect the contributions to internal control concepts made by COSO. In particular, SAS 78 responds to the Winters and Guy (1992) call for a reconciliation of the internal control concepts presented in the COSO report and SAS 55.

This chapter summarizes the two documents and compares the internal control concepts presented in each. The following Table notes the major issues presented.
<table>
<thead>
<tr>
<th><strong>Primary Audience</strong></th>
<th>COBIT</th>
<th>COSO</th>
<th>SAS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management, users, information system auditors</td>
<td>Management</td>
<td>Process</td>
<td>External Auditors</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>IC viewed as a</strong></th>
<th>COBIT</th>
<th>COSO</th>
<th>SAS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set of processes including policies, procedures, practices, and organizational structures</td>
<td>Effective &amp; efficient operations</td>
<td>Effective &amp; efficient operations</td>
<td>Process</td>
</tr>
<tr>
<td>Confidentiality, Integrity and availability of information</td>
<td>Reliable financial reporting</td>
<td>Reliable financial reporting</td>
<td>Reliable financial reporting</td>
</tr>
<tr>
<td>Reliable financial reporting</td>
<td>Compliance with laws &amp; regs</td>
<td>Compliance with laws &amp; regs</td>
<td>Compliance with laws &amp; regs</td>
</tr>
<tr>
<td>Compliance with laws &amp; regs</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>IC Objectives</strong></th>
<th>COBIT</th>
<th>COSO</th>
<th>SAS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organizational</td>
<td>Effective &amp; efficient operations</td>
<td>Effective &amp; efficient operations</td>
<td>Reliable financial reporting</td>
</tr>
<tr>
<td></td>
<td>Confidentiality, Integrity and availability of information</td>
<td>Reliable financial reporting</td>
<td>Effective &amp; efficient operations</td>
</tr>
<tr>
<td></td>
<td>Reliable financial reporting</td>
<td>Compliance with laws &amp; regs</td>
<td>Compliance with laws &amp; regs</td>
</tr>
<tr>
<td></td>
<td>Compliance with laws &amp; regs</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Components or Domains</strong></th>
<th>COBIT</th>
<th>COSO</th>
<th>SAS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domains:</td>
<td>Control Environment</td>
<td>Control Environment Risk Assessment</td>
<td>Control Environment Risk Assessment</td>
</tr>
<tr>
<td>Planning and organization</td>
<td>Risk Management</td>
<td>Control Activities</td>
<td>Control Activities</td>
</tr>
<tr>
<td>Acquisition and implementation</td>
<td>Control Activities</td>
<td>Information &amp; Communication</td>
<td>Information &amp; Communication</td>
</tr>
<tr>
<td>Delivery and support</td>
<td>Information &amp; Communication</td>
<td>Monitoring</td>
<td>Monitoring</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Monitoring</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Focus</strong></th>
<th>COBIT</th>
<th>COSO</th>
<th>SAS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring</td>
<td>Overall Entity</td>
<td>Overall Entity</td>
<td>Overall Entity</td>
</tr>
<tr>
<td>Information Technology</td>
<td>At a point in time</td>
<td>At a point in time</td>
<td>At a point in time</td>
</tr>
<tr>
<td>For a period of time</td>
<td>Management</td>
<td>Management</td>
<td>Management</td>
</tr>
<tr>
<td>Management</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>IC Effectiveness Evaluated</strong></th>
<th>COBIT</th>
<th>COSO</th>
<th>SAS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Responsibility for IC System</td>
<td>187 pages in four documents</td>
<td>353 pages in four volumes</td>
<td>63 pages in two documents</td>
</tr>
<tr>
<td>Size</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 8.2 Summaries of the Documents

#### 8.2.1 COBIT: Control Objectives for Information and related Technology

The Information Systems Audit and Control Foundation (ISACF) recently developed the Control Objectives for Information and related Technology (COBIT) to serve as a framework of generally applicable and IS security and control practices for information technology control. (The report can be ordered from ISACA by phone or mail.) This COBIT framework allows management to benchmark the
security and control practices of IT environments, allows users of IT services to be assured that adequate security and control exists, and allows auditors to substantiate their opinions on internal control and to advise on IT security and control matters. The primary motivation for providing this framework was to enable the development of clear policy and good practices for IT control throughout industry worldwide.

The completed phase of the COBIT project provides an

- Executive Summary, a
- Framework for control of IT,
- A list of Control Objectives, and
- A set of Audit Guidelines. (The control objectives and audit guidelines are referenced to the framework.)

Future phases of the project will provide self-assessment guidelines for management and identify new or updated control objectives through incorporations of other identified global control standards. Plus, add control guidelines and identify key performance indicators.

1. **Definition:**

COBIT adapted its definition of control from COSO: The policies, procedures, practices, and organizational structures are designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected.

COBIT adapts its definition of an IT control objective from SAC: A statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity.

COBIT emphasizes the role and impact of IT control as they relate to business processes. The document outlines platform and application independent IT control objectives.

2. **IT Resources:**

COBIT classifies IT resources as data, application systems, technology, facilities, and people. Data is defined in its widest sense and includes not only numbers, text, and dates but objects such as graphics and sound. Application systems are understood to be the sum of manual and programmed procedures. Technology refers to hardware, operating systems, networking equipment, and the like. Facilities are the resources used to house and support information systems. People addresses individuals' skills and abilities to plan, organize, acquire, deliver, support, and monitor information systems and services.

3. **Requirements:**

To satisfy business objectives, information needs to conform to certain criteria which COBIT refers to as business requirements for information. COBIT combines the principles embedded in existing reference models in three broad categories: quality, fiduciary responsibility and security. From these broad requirements, the report extracts seven overlapping categories of criteria for evaluating how well IT resources are meeting business requirements for information. These criteria are effectiveness, efficiency, confidentiality, integrity, availability, compliance, and reliability of information.

4. **Process and Domains:**

Based on analysis of the information technology infrastructure library (ITIL) IT management practices, a UK document, COBIT classifies IT processes into four domains. These four domains are (1) planning and organization, (2) acquisition and implementation, (3) delivery and support and (4) monitoring. The natural
grouping of processes into domains is often confirmed as responsibility domains in an organizational
structure and follows the management cycle or life cycle applicable to IT processes in any IT environment.
The Exhibit illustrates the relationship between IT resources and the four IT process domains and lists 32
individual IT processes within the four domains.
COBIT presents a framework of control for business process owners. Increasingly, management is fully
empowered with complete responsibility and authority for business processes. COBIT includes definitions
of both internal control and IT control objectives, four domains of processes and 32 high level control
statements for those processes, 271 control objectives referenced to those 32 processes and audit guidelines
linked to the control objectives.

6. Framework:

The COBIT framework provides high-level control statements for particular IT processes. The framework
identifies the business need satisfied by the control statement, identifies the IT resources managed by the
processes, states the enabling controls and lists the major applicable control objectives.

8.2.2 COSO Report

The COSO report defines internal control, describes its components, and provides criteria against which
control systems can be evaluated. The report offers guidance for public reporting on internal control and
provides materials that management, auditors, and others can use to evaluate an internal control system.
Two major goals of the report are to (1) establish a common definition of internal control that serves many
different parties, and (2) provide a standard against which organizations can assess their control systems
and determine how to improve them.

1. Definition:

The COSO report defines internal control as: a process, effected by an entity's board of directors,
management, and other personnel, designed to provide reasonable assurance regarding the achievement of
objectives in the following categories:
• Effectiveness and efficiency of operations
• Reliability of financial reporting
• Compliance with applicable laws and regulations.

The report emphasizes that the internal control system is a tool of, but not a substitute for, management and
that controls should be built into, rather than built onto, operating activities. Although the report defines
internal control as a process, it recommends evaluating the effectiveness of internal control as of a point in
time.

2. Components:

The internal control system consists of five interrelated components:
• Control environment,
• Risk assessment,
• Control activities,
• Information and communication, and
• Monitoring.
The control environment provides the foundation for the other components. It encompasses such factors as management's philosophy and operating style, human resource policies and practices, the integrity and ethical values of employees, the organizational structure, and the attention and direction of the board of directors. The COSO report provides guidance for evaluating each of these factors. For example, management's philosophy and operating style can be assessed by examining the nature of the business risks management accepts, the frequency of their interaction with subordinates, and their attitudes toward financial reporting.

Risk assessment consists of risk identification and risk analysis. Risk identification includes examining external factors such as technological developments, competition, and economic changes, and internal factors such as personnel quality, the nature of the entity's activities, and the characteristics of information system processing. Risk analysis involves estimating the significance of the risk, assessing the likelihood of the risk occurring, and considering how to manage the risk.

3. Control activities

Consist of the policies and procedures that ensure employees carry out management directives. Control activities include reviews of the control system, physical controls, segregation of duties, and information system controls. Controls over information systems include general controls and application controls. General controls are those covering access, software, and system development. Application controls are those which prevent errors from entering the system or detect and correct errors present in the system.

The entity obtains pertinent information and communicates it throughout the organization. The information system identifies, captures, and reports financial and operating information that is useful to control the organization's activities. Within the organization, personnel must receive the message that they must understand their roles in the internal control system, take their internal control responsibilities seriously, and, if necessary, report problems to higher levels of management. Outside the entity, individuals and organizations supplying or receiving goods or services must receive the message that the entity will not tolerate improper actions.

Management monitors the control system by reviewing the output generated by regular control activities and by conducting special evaluations. Regular control activities include comparing physical assets with recorded data, training seminars, and examinations by internal and external auditors. Special evaluations can be of varying scope and frequency. Deficiencies found during regular control activities are usually reported to the supervisor in charge; deficiencies located during special evaluations are normally communicated to higher levels of the organization.

4. Other Concepts:

The COSO report addresses the limitations of an internal control system and the roles and responsibilities of the parties that affect a system. Limitations include faulty human judgment, misunderstanding of instructions, errors, management override, collusion, and cost versus benefit considerations.

The COSO report defines deficiencies as "conditions within an internal control system worthy of attention." Deficiencies should be reported to the person responsible for the activity and to management at least one level above the individual responsible.

An internal control system is judged to be effective if the five components are present and functioning effectively for operations, financial reporting, and compliance.
8.2.3 Conclusion

Internal and external pressures motivate the accounting and management professions to continue to develop and refine internal control concepts. This article summarizes and compares important documents resulting from these efforts: COBIT and COSO.

COBIT is a globally validated collection of control objectives, organized into processes and domains and linked to business requirements for information. COSO presents a common definition of internal control and emphasizes that internal controls help organizations achieve effective and efficient operations, reliable financial reporting, and compliance with applicable laws and regulations. The document provides guidance on assessing control systems, reporting publicly on internal control, and conducting evaluations of control systems.

COBIT and COSO contain many of the same internal control concepts; indeed, later documents build on internal control concepts developed in earlier ones. The documents differ in the audience addressed, the purpose of the document, and level of detail of guidance provided. Although other parties will find each of the documents useful, COBIT is directed to three distinct audiences: management, users and information systems auditors and COSO to managers and boards of directors. COBIT is focused exclusively on controls over information technology in support of business objectives whereas COSO provides a broad, entity-level view.

8.3 Statement on Auditing Standards (SAS) No. 70

Statement on Auditing Standards (SAS) No. 70, Service Organizations, is an internationally recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). SAS 70 is the authoritative guidance that allows service organizations to disclose their control activities and processes to their customers and their customer’s auditors in a uniform reporting format. A SAS 70 examination signifies that a service organization has had its control objectives and control activities examined by an independent accounting and auditing firm. A formal report including the auditor’s opinion (“Service Auditor’s Report”) is issued to the service organization at the conclusion of a SAS 70 examination.

SAS 70 provides guidance to enable and independent auditor ("service auditor") to issue an opinion on a service organization’s description of controls through a Service Auditor’s Report (see below). SAS 70 is not a pre-determined set of control objectives or control activities that service organizations must achieve. Service auditors are required to follow the AICPA’s standards for fieldwork, quality control, and reporting. A SAS 70 examination is not a "checklist" audit.

SAS 70 is generally applicable when an auditor ("user auditor") is auditing the financial statements of an entity ("user organization") that obtains services from another organization ("service organization"). Service organizations that provide such services could be application service providers, bank trust departments, claims processing centers, Internet data centers, or other data processing service bureaus.

In an audit of a user organization’s financial statements, the user auditor obtains an understanding of the entity’s internal control sufficient to plan the audit as required in SAS No. 55, Consideration of Internal Control in a Financial Statement Audit. Identifying and evaluating relevant controls is generally an important step in the user auditor’s overall approach. If a service organization provides transaction processing or other data processing services to the user organization, the user auditor may be required to gain an understanding of the controls at the service organization.
**8.3.1 Service Auditor’s Reports**

One of the most effective ways a service organization can communicate information about its controls is through a Service Auditor’s Report. There are two types of Service Auditor’s Reports: Type I and Type II.

A Type I report describes the service organization’s description of controls at a specific point in time (e.g., June 30, 2000).

A Type II report not only includes the service organization’s description of controls, but also includes detailed testing of the service organization’s controls over a minimum six month period (e.g., January 1, 2000 to June 30, 2000).

The contents of each type of report is described in the following table:

<table>
<thead>
<tr>
<th>Report Contents</th>
<th>Type I Report</th>
<th>Type II Report</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Independent service auditor’s report (i.e. opinion).</td>
<td>Included</td>
<td>Included</td>
</tr>
<tr>
<td>2. Service organization’s description of controls.</td>
<td>Included</td>
<td>Included</td>
</tr>
<tr>
<td>3. Information provided by the independent service auditor; includes a description of the service auditor’s tests of operating effectiveness and the results of those tests.</td>
<td>Optional</td>
<td>Included</td>
</tr>
<tr>
<td>4. Other information provided by the service organization (e.g. glossary of terms).</td>
<td>Optional</td>
<td>Optional</td>
</tr>
</tbody>
</table>

**8.3.2 Benefits to the Service Organization**

Service organizations receive significant value from having a SAS 70 engagement performed. A Service Auditor’s Report with an unqualified opinion that is issued by an Independent Accounting Firm differentiates the service organization from its peers by demonstrating the establishment of effectively designed control objectives and control activities. The Service Auditor’s Report also helps a service organization build trust with its user organizations (i.e. customers).

Without a current Service Auditor’s Report, a service organization may have to entertain multiple audit requests from its customers and their respective auditors. Multiple visits from user auditors can place a strain on the service organization’s resources. A Service Auditor’s Report ensures that all user organizations and their auditors have access to the same information and in many cases this will satisfy the user Auditor’s requirements.

SAS 70 engagements are generally performed by control oriented professionals who have experience in accounting, auditing, and information security. A SAS 70 engagement allows a service organization to have its control policies and procedures evaluated and tested (in the case of a Type II engagement) by an independent party. Very often this process results in the identification of opportunities for improvements in many operational areas.
8.4 COBIT

8.4.1 Components of COBIT Framework:

COBIT framework comprises six documents:
- Executive Summary
- The COBIT Framework
- Control Objectives
- Audit Guidelines
- Management Guidelines
- Implementation Toolset

1. COBIT Framework

The COBIT Framework provides a tool for the business process owner that facilitates the discharge of this responsibility. The Framework continues with a set of 34 high-level Control Objectives, one for each of the IT processes, grouped into four domains: planning and organisation, acquisition and implementation, delivery and support, and monitoring. This structure covers all aspects of information and the technology that supports it. By addressing these 34 high-level control objectives, the business process owner can ensure that an adequate control system is provided for the IT environment. IT Framework governance guidance is also provided in the COBIT Framework.

2. COBIT Control Objectives

318 Detailed controls objectives are defined in COBIT Control Objectives

3. Audit Guideline

In addition, corresponding to each of the 34 high-level control objectives is an Audit Guideline to enable the review of IT processes against COBIT’s 318 recommended detailed control objectives to provide management assurance and/or advice for improvement.

4. Management Guidelines

The IT Governance Institute has further built, in cooperation with world-wide industry experts, analysts and academics. Management Guidelines for COBIT, which consist of Maturity Models, Critical Success Factors (CSFs), Key Goal Indicators (KGIs) and Key Performance Indicators (KPIs). This delivers a significantly improved framework responding to management’s need for control and measurability of IT by providing management with tools to assess and measure their organisation’s IT environment against the 34 IT processes COBIT identifies.
In order to ensure that management reaches its business objectives, it must direct and manage IT activities to reach an effective balance between managing risks and realising benefits. To accomplish this, management needs to identify the most important activities to be performed, measure progress towards achieving goals and determine how well the IT processes are performing. In addition, it needs the ability to evaluate the organisation’s maturity level against industry best practices and international standards.

Hence, the main objective of the COBIT project is the **development of clear policies and good practices** for **security** and **control** in IT for worldwide endorsement by commercial, governmental and professional organisations. It is the goal of the project to develop these control objectives primarily from the business...
objectives and needs perspective. (This is compliant with the COSO perspective, which is first and foremost a management framework for internal controls.) Subsequently, control objectives have been developed from the audit objectives (certification of financial information, certification of internal control measures, efficiency and effectiveness, etc.) perspective.

8.4.2 Audience

COBIT is designed to be used by three distinct audiences.

- **MANAGEMENT:** to help them balance risk and control investment in an often unpredictable IT environment.
- **USERS:** to obtain assurance on the security and controls of IT services provided by internal or third parties.
- **AUDIT ORS:** to substantiate their opinions and/or provide advice to management on internal controls.

8.4.3 General Definitions

For the purpose of this project, the following definitions are provided.

*Control is defined as* and organisational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected.

*IT Control Objective is defined as* a statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity.

*IT Governance is defined as* a structure of relationships and processes to direct and control the enterprise in order to achieve the enterprise’s goals by adding value while balancing risk versus return over IT and its processes.

Starting the analysis from the broader Quality, Fiduciary and Security requirements, seven distinct, certainly overlapping, categories were extracted. COBIT’s working definitions are as follows:
Another way of looking at the relationship of IT resources to the delivery of services is depicted below.

The COBIT Framework consists of high-level control objectives and an overall structure for their classification. The underlying theory for the classification is that there are, in essence, three levels of IT efforts when considering the management of IT resources.

Starting at the bottom, there are the **activities and tasks** needed to achieve a measurable result. Activities have a life-cycle concept while tasks are more discrete. The life-cycle concept has typical control requirements different from discrete activities.

**Processes** are then defined one layer up as a series of joined activities or tasks with natural (control) breaks. At the highest level, processes are naturally grouped together into domains. Their natural grouping is often confirmed as responsibility domains in an organisational structure and is in line with the management cycle or life cycle applicable to IT processes.

The IT resources identified in COBIT can be explained/defined as follows:

- **Data** are objects in their widest sense (i.e., external and internal), structured and non-structured, graphics, sound, etc.
- **Application Systems** are understood to be the sum of manual and programmed procedures.
- **Quality Requirements** covers hardware, operating systems, Quality, Cost, Delivery
- **Secure Requirements (COSO Report)**: Effectiveness and Efficiency of operations, Reliability of Information, Compliance with laws and regulations
- **Security Requirements**: Confidentiality, Integrity, Availability

**Control objectives and an overall structure for their identification is that there are, in essence, three levels of IT resources.**
Thus, the conceptual framework can be approached from three vantage points:

- Information criteria,
- IT resources and
- IT processes.

These three vantage points are depicted in the above COBIT Cube.

With the preceding as the framework, the domains are identified using wording that management would use in the day-to-day activities of the organization—not auditor jargon.

Thus, four broad domains are identified: **planning and organization, acquisition and implementation, delivery and support, and monitoring**.

### Planning and organization

This domain covers strategy and tactics, and concerns the identification of the way IT can best contribute to the achievement of the business objectives. Furthermore, the realisation of the strategic vision needs to be planned, communicated and managed for different perspectives. Finally, a proper organisation as well as technological infrastructure must be put in place.

### Acquisition & Implementation

To realise the IT strategy, IT solutions need to be identified, developed or acquired, as well as implemented and integrated into the business process. In addition, changes in and maintenance of existing systems are covered by this domain to make sure that the life cycle is continued for these systems.

### Delivery & Support

This domain is concerned with the actual delivery of required services, which range from traditional operations over security and continuity aspects to training. In order to deliver services, the necessary support processes must be set up. *This domain includes the actual processing of data by application and application controls.*

### Monitoring

All IT processes need to be regularly assessed over time for their quality and compliance with control requirements. This domain thus addresses management’s oversight of the organisation’s control process and independent assurance provided by internal and external audit or obtained from alternative sources.

It should be noted that these IT processes can be applied at different levels within an organization. For example, some of these processes will be applied at the enterprise level, others at the IT function level, others at the business process owner level, etc. It should also be noted that the **Effectiveness** criterion of processes that plan or deliver solutions for business requirements will sometimes cover the criteria for **Availability, Integrity** and **Confidentiality**—in practice, they have become business requirements.

For example, the process of “identify solutions” has to be effective in providing the Availability, Integrity and Confidentiality requirements. It is clear that all control measures will not necessarily satisfy the different business requirements for information to the same degree.
• **Primary** is the degree to which the defined control objective directly impacts the information criterion concerned.

• **Secondary** is the degree to which the defined control objective satisfies only to a lesser extent or indirectly the information criterion concerned.

• **Blank** could be applicable; however, requirements are more appropriately satisfied by another criterion in this process and/or by another process.

Similarly, all control measures will not necessarily impact the different IT resources to the same degree. Therefore, the COBIT Framework specifically indicates the applicability of the IT resources that are specifically managed by the process under consideration (not those that merely take part in the process).

In summary, in order to provide the information that the organization needs to achieve its objectives, IT governance must be exercised by the organization to ensure that IT resources are managed by a set of naturally grouped IT processes. The following diagram illustrates this concept.
COBIT IT PROCESSES DEFINED WITHIN THE FOUR DOMAINS

Business Objectives

IT Governance

Information

Monitoring

IT Resources

Planning & Organisation

Delivery & Support

Acquisition & Implementation

M1 monitor the processes
M2 assess internal control adequacy
M3 obtain independent assurance
M4 provide for independent audit

PO1 define a strategic IT plan
PO2 define the information architecture
PO3 determine the technology direction
PO4 define the IT organisation and relationships
PO5 manage the IT investment
PO6 communicate management aims and direction
PO7 manage human resources
PO8 ensure compliance with external requirements
PO9 assess risks
PO10 manage projects
PO11 manage quality

DS1 define and manage service levels
DS2 manage third-party services
DS3 manage performance and capacity
DS4 ensure continuous service
DS5 ensure systems security
DS6 identify and allocate costs
DS7 educate and train users
DS8 assist and advise customers
DS9 manage the configuration
DS10 manage problems and incidents
DS11 manage data
DS12 manage facilities
DS13 manage operations

AI1 identify automated solutions
AI2 acquire and maintain application software
AI3 acquire and maintain technology infrastructure
AI4 develop and maintain procedures
AI5 install and operate systems
AI6 manage changes
8.6 Control Objectives

COBIT Framework focuses on high-level controls for each process, Control Objectives focuses on specific, detailed control objectives associated with each IT process. For each of the 34 IT processes of the Framework, there are from three to 30 detailed control objectives, for a total of 318.

The following chart provides an indication, by IT process and domain, of which information criteria are impacted by the high-level control objectives, as well as an indication of which IT resources are applicable.

<table>
<thead>
<tr>
<th>Domain</th>
<th>Process</th>
<th>Information Criteria</th>
<th>IT Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Planning &amp;</td>
<td>Define a strategic IT plan</td>
<td>P S</td>
<td></td>
</tr>
<tr>
<td>Organisation</td>
<td>Define the information architecture</td>
<td>P S S S S</td>
<td></td>
</tr>
<tr>
<td>PO1</td>
<td>Determine technological direction</td>
<td>P S</td>
<td></td>
</tr>
<tr>
<td>PO2</td>
<td>Define the IT organisation and relationships</td>
<td>P S</td>
<td></td>
</tr>
<tr>
<td>PO3</td>
<td>Manage the IT investment</td>
<td>P P S</td>
<td></td>
</tr>
<tr>
<td>PO4</td>
<td>Communicate management plans and direction</td>
<td>P S S</td>
<td></td>
</tr>
<tr>
<td>PO5</td>
<td>Manage human resources</td>
<td>P S S</td>
<td></td>
</tr>
<tr>
<td>PO6</td>
<td>Ensure compliance with external requirements</td>
<td>P S S P P P S S</td>
<td></td>
</tr>
<tr>
<td>PO7</td>
<td>Assess risks</td>
<td>P S S P P P S S</td>
<td></td>
</tr>
<tr>
<td>PO8</td>
<td>Manage projects</td>
<td>P S S P P P S S</td>
<td></td>
</tr>
<tr>
<td>PO9</td>
<td>Manage quality</td>
<td>P S S P P P S S</td>
<td></td>
</tr>
<tr>
<td>PO10</td>
<td>Define automated solutions</td>
<td>P S S P P P S S</td>
<td></td>
</tr>
<tr>
<td>PO11</td>
<td>Acquire and maintain application software</td>
<td>P S S P P P S S S S S</td>
<td></td>
</tr>
<tr>
<td>Acquisition &amp;</td>
<td>Develop and maintain procedures</td>
<td>P S S P P P S S S S S</td>
<td></td>
</tr>
<tr>
<td>Implementation</td>
<td>Install and operate systems</td>
<td>P S S S S S S S S S S</td>
<td></td>
</tr>
<tr>
<td>A12</td>
<td>Identity automated solutions</td>
<td>P S S P P P S S S S S</td>
<td></td>
</tr>
<tr>
<td>A13</td>
<td>Acquire and maintain application software</td>
<td>P S S P P P S S S S S</td>
<td></td>
</tr>
<tr>
<td>A14</td>
<td>Develop and maintain procedures</td>
<td>P S S P P P S S S S S</td>
<td></td>
</tr>
<tr>
<td>A15</td>
<td>Install and operate systems</td>
<td>P S S P P P S S S S S</td>
<td></td>
</tr>
<tr>
<td>A16</td>
<td>Manage changes</td>
<td>P S S P P P S S S S S</td>
<td></td>
</tr>
<tr>
<td>Delivery &amp;</td>
<td>Define and manage service levels</td>
<td>P S S S S S S S S S S</td>
<td></td>
</tr>
<tr>
<td>Support</td>
<td>Manage third-party services</td>
<td>P S S S S S S S S S S</td>
<td></td>
</tr>
<tr>
<td>DS1</td>
<td>Manage performance and capacity</td>
<td>P S S S S S S S S S S</td>
<td></td>
</tr>
<tr>
<td>DS2</td>
<td>Ensure continuous service</td>
<td>P S S S S S S S S S S</td>
<td></td>
</tr>
<tr>
<td>DS3</td>
<td>Ensure systems security</td>
<td>P S S S S S S S S S S</td>
<td></td>
</tr>
<tr>
<td>DS4</td>
<td>Identity and allocate costs</td>
<td>P S S S S S S S S S S</td>
<td></td>
</tr>
<tr>
<td>DS5</td>
<td>Idenfically and allocate costs</td>
<td>P S S S S S S S S S S</td>
<td></td>
</tr>
<tr>
<td>DS6</td>
<td>Educate and train users</td>
<td>P S S S S S S S S S S</td>
<td></td>
</tr>
<tr>
<td>DS7</td>
<td>Assist and advise customers</td>
<td>P S S S S S S S S S S</td>
<td></td>
</tr>
<tr>
<td>DS8</td>
<td>Manage the configuration</td>
<td>P S S S S S S S S S S</td>
<td></td>
</tr>
<tr>
<td>DS9</td>
<td>Manage problems and incidents</td>
<td>P S S S S S S S S S S</td>
<td></td>
</tr>
<tr>
<td>DS10</td>
<td>Manage data</td>
<td>P S S S S S S S S S S</td>
<td></td>
</tr>
<tr>
<td>DS11</td>
<td>Manage facilities</td>
<td>P S S S S S S S S S S</td>
<td></td>
</tr>
<tr>
<td>DS12</td>
<td>Manage operations</td>
<td>P S S S S S S S S S S</td>
<td></td>
</tr>
<tr>
<td>DS13</td>
<td>Monitor the processes</td>
<td>P S S S S S S S S S S</td>
<td></td>
</tr>
<tr>
<td>Monitoring</td>
<td>Assess internal control adequacy</td>
<td>P S S S S S S S S S S</td>
<td></td>
</tr>
<tr>
<td>M1</td>
<td>Obtain independent assurance</td>
<td>P S S S S S S S S S S</td>
<td></td>
</tr>
<tr>
<td>M2</td>
<td>Provide for independent audit</td>
<td>P S S S S S S S S S S</td>
<td></td>
</tr>
<tr>
<td>M3</td>
<td>(P) primary (S) secondary</td>
<td>P S S S S S S S S S S</td>
<td></td>
</tr>
<tr>
<td>M4</td>
<td>(P) applicable to</td>
<td>P S S S S S S S S S S</td>
<td></td>
</tr>
</tbody>
</table>
We have summarized control activities involved in each process in table given below, for detailed control objectives please refer to end of this Book.

8.7 COBIT MANAGEMENT GUIDELINES

A basic need for every organisation is to understand the status of its own IT systems and to decide what security and control they should provide. Neither aspect of this issue — understanding of and deciding on the required level of control — is straightforward. What should be measured and how? In addition to the need for measuring where an organisation is, there is the importance of continuous improvement in the areas of IT security and control, and the need for a management toolkit to monitor this improvement. Whilst few would argue that this is not a good thing, all must occasionally ask themselves:

“How far should we go, and is the cost justified by the benefit?”

The response is provided by the COBIT Management Guidelines that are generic and action oriented for the purpose of addressing the following types of management concerns:

- Performance measurement – What are the indicators of good performance?
- IT control profiling – What’s important? What are the Critical Success Factors for control? • Awareness – What are the risks of not achieving our objectives?
- Benchmarking – What do others do? How do we measure and compare?

An answer to these requirements of determining and monitoring the appropriate IT security and control level is the definition of specific:

- **Benchmarking** of IT control practices (expressed as Maturity Models)
- **Performance Indicators** of the IT processes — for their outcome and their performance
- **Critical Success Factors** for getting these processes under control

8.7.1 Maturity Model

Maturity Models for control over IT processes consist of developing a method of scoring so that an organisation can grade itself from non-existent to optimised (from 0 to 5). This approach has been derived from the Maturity Model that the Software Engineering Institute defined for the maturity of the software development capability. Against these levels, developed for each of COBIT’s 34 IT processes, management can map:

- The current status of the organisation — where the organisation is today
- The current status of (best-in-class in) the industry — the comparison
- The current status of international standards — additional comparison
- The organisation’s strategy for improvement — where the organisation wants to be
## Generic Maturity Model

<table>
<thead>
<tr>
<th>Rank</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Non-Existent</td>
<td>Complete lack of any recognisable processes. The organisation has not even recognised that there is an issue to be addressed.</td>
</tr>
<tr>
<td>1</td>
<td>Initial</td>
<td>There is evidence that the organisation has recognised that the issues exist and need to be addressed. There are however no standardised processes but instead there are ad hoc approaches that tend to be applied on an individual or case by case basis. The overall approach to management is disorganised.</td>
</tr>
<tr>
<td>2</td>
<td>Repeatable</td>
<td>Processes have developed to the stage where similar procedures are followed by different people undertaking the same task. There is no formal training or communication of standard procedures and responsibility is left to the individual. There is a high degree of reliance on the knowledge of individuals and therefore errors are likely.</td>
</tr>
<tr>
<td>3</td>
<td>Defined</td>
<td>Procedures have been standardised and documented, and communicated through training. It is however left to the individual to follow these processes, and it is unlikely that deviations will be detected. The procedures themselves are not sophisticated but are the formalisation of existing practices.</td>
</tr>
<tr>
<td>4</td>
<td>Managed</td>
<td>It is possible to monitor and measure compliance with procedures and to take action where processes appear not to be working effectively. Processes are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way.</td>
</tr>
<tr>
<td>5</td>
<td>Optimised</td>
<td>Processes have been refined to a level of best practice, based on the results of continuous improvement and maturity modelling with other organisations. IT is used in an integrated way to automate the workflow, providing tools to improve quality and effectiveness, making the enterprise quick to adapt.</td>
</tr>
</tbody>
</table>

### 8.7.2 Critical Success Factors

Critical Success Factors provide management with guidance for implementing control over IT and its processes. They are the most important things to do that contribute to the IT process achieving its goals. They are activities that can be of a strategic, technical, organizational, process or procedural nature.
From the standard control model and from the IT Governance Framework, a number of Critical Success Factors can be deduced that apply to most IT processes:
Applying to IT in general

- IT processes are defined and aligned with the IT strategy and the business goals • The customers of the process and their expectations are known • Processes are scalable and their resources are appropriately managed and leveraged
- The required quality of staff (training, transfer of information, morale, etc.) and availability of skills (recruit, retain, retrain) exist.
- IT performance is measured in financial terms, in relation to customer satisfaction, for process effectiveness and for future capability. IT management is rewarded based on these measures.
- A continuous quality improvement effort is applied.

Applying to most IT processes

- All process stakeholders (users, management, etc.) are aware of the risks, of the importance of IT and the opportunities it can offer, and provide strong commitment and support
- Goals and objectives are communicated across all disciplines and understood; it is known how processes implement and monitor objectives, and who is accountable for process performance
- People are goal-focused and have the right information on customers, on internal processes and on the consequences of their decisions
- A business culture is established, encouraging cross-divisional co-operation, teamwork and continuous process improvement
- There is integration and alignment of major processes, e.g., change, problem and configuration management
- Control practices are applied to increase efficient and optimal use of resources and improve the effectiveness of processes.

Applying to IT governance

- Control practices are applied to increase transparency, reduce complexity, promote learning, provide flexibility and scalability, and avoid breakdowns in internal control and oversight
- The application of practices that enable sound oversight: a control environment and culture; a code of conduct; risk assessment as a standard practice; self-assessments; formal compliance on adherence to established standards; monitoring and follow up of control deficiencies and risk
- IT governance is recognised and defined, and its activities are integrated into the enterprise governance process, giving clear direction for IT strategy, a risk management framework, a system of controls and a security policy
- IT governance focuses on major IT projects, change initiatives and quality efforts, with awareness of major IT processes, the responsibilities and the required resources and capabilities
- An audit committee is established to appoint and oversee an independent auditor, drive the IT audit plan and review the results of audits and 3rd party opinions.

8.7.3 KEY GOAL INDICATORS

A Key Goal Indicator, representing the process goal, is a measure of “what” has to be accomplished. It is a measurable indicator of the process achieving its goals, often defined as a target to achieve.
8.7.4 **KEY PERFORMANCE INDICATORS**

Key Performance Indicators are measures that tell management that an IT process is achieving its business requirements by monitoring the performance of the enablers of that IT process. Building on the Balanced Business Scorecard principles, the relationship between Key Performance Indicators and Key Goal Indicators is as follows:

But how are the business and IT goals and measures linked? The COBIT *Framework* expresses the objectives for IT in terms of the information criteria that the business needs in order to achieve the business objectives, which will usually be expressed in terms of:

- Availability of systems and services
- Absence of integrity and confidentiality risks • Cost-efficiency of processes and operations
- Confirmation of reliability, effectiveness and compliance.

To better understand the goal and performance indicators, we also looked at the four dimensions of the Balanced Business Scorecard:

- **Financial** — How do shareholders look at us? (i.e., deliver against budget)
- **Customer** — How do customers see us? (e.g., customer satisfaction, on time delivery, service value)
- **Internal process** — How do we look at ourselves? (i.e., process orientation and quality)
- **Learning/innovation** — Can we continue to improve and create values? (i.e., employee knowledge and technical infrastructure).

Key Goal Indicators for IT are business driven and usually provide the measures needed to support the financial and customer dimensions of the enterprise Balanced Business Scorecard. Key Performance Indicators, focus on the other two dimensions of the Balanced Business Scorecard: internal processes and innovation. Financial results and customer satisfaction are typically measures of the business goal being achieved and measured *after-the-fact*. On the other hand, process excellence and ability to learn and innovate are indicators of how well an organisation is performing and gives an indication of the probability of achieving success *before-the-fact*.

Generic Key Goal Indicators is listed below that is usually applicable to all IT processes:

- Achieving targeted return on investment or business value benefits
- Enhanced performance management
- Reduced IT risks
- Productivity improvements • Integrated supply chains
- Standardised processes
- Boost of service delivery (sales)
- Reaching new and satisfying existing customers
• Creation of new service delivery channels
• Availability of bandwidth, computing power and IT delivery mechanisms fitting the business, and their uptime and downtime
• Meeting requirements and expectations of the customer of the process on budget and on time
• Number of customers and cost per customer served • Adherence to industry standards.

Generic Key Performance Indicators is listed below that is usually applicable to all IT processes:
Applying to IT in general

Reduced cycle times (i.e., responsiveness of IT production and development)

- Increased quality and innovation
- Utilisation of communications bandwidth and computing power
- Service availability and response times
- Satisfaction of stakeholders (survey and number of complaints)
- Number of staff trained in new technology and customer service skills.

Applying to most IT processes

- Improved cost-efficiency of the process (cost vs. deliverables)
- Staff productivity (number of deliverables) and morale (survey)
- Amount of errors and rework.

Applying to IT governance

- Benchmark comparisons
- Number of non-compliance reporting.

8.7.5 Conclusion

To get Information Technology under control such that IT is aligned with the business and enables it by delivering the information the organisation needs, a number of management tools have been provided in these Management Guidelines. The relationship between the Critical Success Factors, the Maturity Models, the Key Performance Indicators and the Key Goal Indicators can be expressed as:

“CSFs are the most important things you need to do based on the choices made in the Maturity Model, whilst monitoring through KPIs whether you will likely reach the goals set by the KGIIs.”

8.8 COBIT Audit Guidelines

To enable the easy application of the COBIT Framework and Control Objectives within audit and assessment activities. The purpose of the Audit Guidelines is to provide a simple structure for auditing and assessing controls based upon generally accepted audit practices that fits within the overall COBIT scheme.

Auditors have a general requirement to provide management and the business process owners with assurance and advice regarding controls in an organisation; to provide reasonable assurance that relevant control objectives are being met; to identify where there are significant weaknesses in those controls; to substantiate the risk that may be associated with such weaknesses; and, finally, to advise these executives on the corrective actions that should be taken.

COBIT provides clear policies and good practices for security and control of information and related technology. Therefore, basing the Audit Guidelines firmly on the Control Objectives takes the auditor’s opinion out of the audit conclusion, replacing it with authoritative criteria.
The COBIT *Audit Guidelines* enable the auditor to review specific IT processes against COBIT’s recommended *Control Objectives* to help assure management where controls are sufficient, or to advise management where processes need to be improved.

The objectives of auditing are to:

- Provide management with reasonable assurance that control objectives are being met,
- where there are significant control weaknesses, to substantiate the resulting risks, and
- advise management on corrective actions

The generally accepted structure of the audit process is:

- Identification and documentation
- Evaluation
- Compliance testing
- Substantive testing

The IT process is therefore audited by:

- **Obtaining** an understanding of business requirements related risks, and relevant control measures
- **Evaluating** the appropriateness of stated controls
- **Assessing** compliance by testing whether the stated controls are working as prescribed, consistently and continuously
- **Substantiating** the risk of control objectives not being met by using analytical techniques and/or consulting alternative sources.

### 8.8.1 Audit Process Requirements

Having defined what we are going to audit and provide assurance on, we have to determine the most appropriate approach or strategy for carrying out our audit work. First we need to *determine the correct scope of our audit*.

To achieve this we need to investigate, analyse and define:

- The business processes concerned
- The platforms and information systems which are supporting the business process as well as interconnectivity with other platforms or systems
- The IT roles and responsibilities defined, including what has been in- or out-sourced
- Associated business risks and strategic choices

The next step is to *identify the information requirements* which are of particular relevance with respect to the business processes. Then we will need to *identify the inherent IT risks as well as overall level of control* which can be associated with the business process. To achieve this we identify:

- Recent changes in the business environment having an IT impact
- Recent changes to the IT environment, new developments, etc.
- Recent incidents relevant to the controls and business environment
• IT monitoring controls applied by management
• Recent audit and/or certification reports
• Recent results of self assessments
### Audit Process Requirements

| Define audit scope | Business process concerned  
|                   | Platforms, systems and their interconnectivity, supporting the process  
|                   | Roles, responsibilities and organisational structure |
| Identify information requirements relevant for the business process | Relevance to the business process |
| Identify inherent IT risks and overall level of Control | Recent changes and incidents in business and technology environment  
|                   | Results of audits, self-assessments and certification  
|                   | Monitoring controls applied by management |
| Select processes and platforms to audit | Processes  
|                   | Resources |
| Set audit strategy | Controls X risk  
|                   | Steps and tasks  
|                   | Decision points |

#### 8.8.2 Generic Audit Guideline

1. Obtaining an Understanding

The audit steps to be performed to document the activities underlying the control objectives as well as to identify the stated control measures/procedures in place.

- Interview appropriate management and staff to gain an understanding of:
  - Business requirements and associated risks
  - Organisation structure
  - Roles and responsibilities
  - Policies and procedures
  - Laws and regulations
  - Control measures in place
  - Management reporting (status, performance, action items)

Document the process-related IT resources particularly affected by the process under review. Confirm the understanding of the process under review, the Key Performance Indicators (KPI) of the process, the control implications, e.g., by a process walk through.
2. **EVALUATING THE CONTROLS**

The audit steps to be performed in assessing the effectiveness of control measures in place or the degree to which the control objective is achieved. Basically deciding what, whether and how to test.

Evaluate the appropriateness of control measures for the process under review by considering identified criteria and industry standard practices, the Critical Success Factors (CSF) of the control measures and applying auditor professional judgment.

- Documented processes exist
- Appropriate deliverables exist
- Responsibility and accountability are clear and effective
- Compensating controls exist, where necessary

Conclude the degree to which the control objective is met.

3. **ASSESSING COMPLIANCE**

The audit steps to be performed to ensure that the control measures established are working as prescribed, consistently and continuously and to conclude on the appropriateness of the control environment.

Obtain direct or indirect evidence for selected items/periods to ensure that the procedures have been complied with for the period under review using both direct and indirect evidence.

Perform a limited review of the adequacy of the process deliverables.

Determine the level of substantive testing and additional work needed to provide assurance that the IT process is adequate.

4. **SUBSTANTIATING THE RISK**

The audit steps to be performed to substantiate the risk of the control objective not being met by using analytical techniques and/or consulting alternative sources. The objective is to support the opinion and to ‘shock’ management into action. Auditors have to be creative in finding and presenting this often sensitive and confidential information.

Document the control weaknesses, and resulting threats and vulnerabilities.

Identify and document the actual and potential impact; e.g., through root-cause analysis. Provide comparative information, e.g., through benchmarks.

8.8.3 **PUTTING IT ALL TOGETHER**

In summary, the detailed Audit Guidelines can always be complemented by considering the Generic Guideline and the process under review, and obtain further audit tasks to achieve the audit objective. The audit programme development itself can benefit from considering the IT audit process requirements, the COBIT Framework and High-Level Control Objectives, and the Control Considerations stated above.
8.8.4 **RISK ANALYSIS AS AN ALTERNATIVE ASSESSMENT APPROACH**

Balancing cost and risk is the next issue to address, i.e., making a conscious choice of how and whether to implement each control objective. Risk analysis approaches address this choice, even though the proactive principle remains; control objectives should be applied in the first place to achieve an information control criteria (effectiveness, efficiency, confidentiality, availability, integrity, compliance and reliability). It is self-evident that some form of business risk assessment needs to be used by management to define the measures to implement. Auditors also will do some form of risk assessment when choosing process domains and control objectives for review. A commonly accepted approach for risk analysis in IT is as follows:

![Risk Analysis Framework](image)

The model starts from the valuation of assets which in the COBIT *Framework* consists of the information that has the required criteria to help achieve the business objectives (including all the resources necessary to produce that information). The next step is the vulnerability analysis which looks at the importance of the information criteria in the process under review, i.e., if a business process is vulnerable to integrity loss, then specific measures are required. Next one looks at threats, i.e., that which can exploit a vulnerability. The probability of the threat, the degree of vulnerability and the severity of the impact are combined to conclude on the risk assessment. This is followed by the selection of countermeasures (controls) and an evaluation of their effectiveness, which also identifies residual risk. The conclusion is an action plan after which the cycle can start again.

8.9 **WEBTRUST**

An e-Commerce business faces at least two unique challenges in winning and keeping its customers.

First, e-Commerce transactions are often anonymous, which can raise customer concerns about privacy, security, and business practices. Second, the transaction is usually carried out over the powerful but
relatively insecure public Internet. Due to these factors, customers may not fully trust the e-Commerce business. The WebTrust program is designed to help e-Commerce businesses overcome these issues.

The WebTrust program is:

- A set of e-Commerce standards comprised of prevailing best practices and requirements from around the world
- Independent verification that a site meets the standards
- An internationally recognized WebTrust Seal, announcing that the e-Commerce site meets the stringent standards

For the e-Commerce business, WebTrust identifies and helps to reduce business risks. For customers and visitors, WebTrust helps build confidence in the site and ultimately helps win and keep good customers.

8.9.1 HOW WEBTRUST WORKS

WebTrust is designed to enhance confidence among sellers and buyers alike. Here's why.

1. Reduces Risk and Provides Assurance to Management and Boards

A WebTrust review focuses on risk areas related to e-commerce activities and the appropriate policies and controls to manage those risks to the benefit of both the entity and the entity's customers. The end result is a more robust and secure e-commerce system.

2. Builds Confidence and Trust for Customers and Visitors

Seeing the WebTrust seal on a site alerts customers and visitors that the e-commerce business complies with the criteria that are among the highest in the world.

WebTrust is a unique program tailored to specific aspects of e-business activities for both business-to-business and business-to-consumer entities.

3. Who Provides WebTrust Services

CPAs, Chartered Accountants, and their equivalents worldwide are recognized as trusted, independent third parties who can assure the accuracy and fairness of financial and non-financial information. Accounting firms have built reputations as experts in the area of assurance, privacy, security, and transaction testing. Firms large and small have been recognized through rewards and as service providers for their competence in these areas. In fact, certain other Internet trustmark programs employ accountants as part of their service.

Only licensed public accountants who complete special training are able to issue a WebTrust seal.

A WebTrust seal will only be awarded when a site completely passes the examination by a licensed CPA, Chartered Accountant, or equivalent based on the WebTrust criteria.

4. Strong Standards for Security and On-Line Privacy
Security and privacy have become vital aspects for the business community. From a business perspective, information privacy can be a two-edged sword.

On the one hand, merchants need certain information in order to process a customer transaction such as an order. On the other hand, the customer may not want this information used for any other purpose without prior permission. Customers expect that their privacy should be respected.

5. **Site Re-examined Periodically - Customers Know Your Site is in Continuous Compliance**

Your online business receives an on-site review process by the CPA to renew your WebTrust seal at least once every six (6) months. The CPA or equivalent will work closely with you as your e-Commerce consultant to help your site remain in compliance with the WebTrust Principles and Criteria.

8.9.2 **Trust Services Principles and Criteria**

The Trust Services Principles and Criteria are organized into four broad areas:

5. Policies. The entity has defined and documented its policies relevant to the particular principle.

6. Communications. The entity has communicated its defined policies to authorized users.

7. Procedures. The entity uses procedures to achieve its objectives in accordance with its defined policies.

8. Monitoring. The entity monitors the system and takes action to maintain compliance with its defined policies.

A two-column format has been used to present and discuss the criteria. The first column presents the criteria—the attributes that the entity must meet to be able to demonstrate that it has achieved the principle.

The second column provides illustrative controls. These are examples of controls that the entity might have in place to conform to the criteria. Alternative and additional controls may also be appropriate.

In addition, examples of system descriptions for both e-commerce and non-e-commerce systems are included in Appendix B and Appendix C, respectively, and Appendix B also includes sample disclosures for e-commerce systems.
The following principles and related criteria have been developed by the AICPA/CICA use by practitioners in the performance of Trust Services engagements such as SysTrust WebTrust.

1. **On-Line Privacy.**

The enterprise ensures that personally identifiable information obtained as a result of electronic commerce is protected as stated in its on-line privacy statement.

The online privacy principle focuses on protecting the personal information an organization may collect from its customers through its e-commerce systems. Even though the controls an organization may have in place to protect such information may extend beyond its Web-based systems and may even include its service providers, it is not the intent of this principle to address protection of the privacy of all personal information an entity may collect, from all sources. The AICPA and CICA have established a separate task force to consider principles and criteria relevant to enterprise-wide privacy.

Privacy can have many aspects, but for purposes of this principle and the corresponding criteria, privacy is defined as the rights and obligations of individuals and entities with respect to the collection, use, disclosure, and retention of personal information. Personal information is defined as any information relating to an identified or identifiable individual. Such information includes but is not limited to the customer’s name; address; telephone number; Social Security, insurance, or other government identification numbers; employer; credit card numbers; personal or family financial information; personal or family medical information; employment history; history of purchases or other transactions; credit records; and similar information.

Sensitive information is defined as personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sexual preferences, or information related to offenses or criminal convictions.

Examples of areas evaluated include:

- Information on the sources of private information being collected
- how that information will be used and distributed, as well as corrected when necessary
- how "cookies" are used
- how customers can opt out of transactions

2. **Confidentiality.**

The enterprise ensures that access to information obtained as a result of electronic commerce and designated as confidential is restricted to authorized individuals in conformity with its disclosed confidentiality practices.

The confidentiality principle focuses on information designated as confidential. Unlike personally identifiable information, which is being defined by regulation in a number of countries worldwide, there is no widely recognized definition of confidential information. In the course of communicating and transacting business, partners often exchange information they require to be maintained on a confidential basis. In most instances, the respective parties wish to ensure that the information they provide is available only to those individuals who need access to complete the transaction or resolution on any questions that arise. To enhance business partner confidence, it is important that the business partner is informed about the
entity’s confidentiality practices. The entity needs to disclose its practices relating to the manner in which it provides for authorized access to and uses and shares information designated as confidential.

Examples of areas evaluated include:

- assurance that the security surrounding transmission
- collection and distribution of confidential information is adequate
- proper procedures for confidentiality breaches
- choices provided to customers, including opting out
- safeguards on transmission to unintended recipients and against unauthorized access secure storage of backup media
3. **Security.**

The enterprise ensures that access to the electronic commerce system and data is restricted only to authorized individuals in conformity with its disclosed security policies.

The *security principle* refers to the protection of the system components from unauthorized access, both logical and physical. In e-commerce and other systems, the respective parties wish to ensure that information provided is available only to those individuals who need access to complete the transaction or services, or follow up on questions or issues that may arise. Information provided through these systems is susceptible to unauthorized access during transmission and while it is stored on the other party's systems. Limiting access to the system components helps prevent potential abuse of system components, theft of resources, misuse of software, and improper access to, use, alteration, destruction, or disclosure of information. Key elements for the protection of system components include permitting authorized access and preventing unauthorized access to those components.

Examples of areas evaluated include:

- the existence of a functioning disaster recovery plan
- procedures to handle security breaches
- the use of proper encryption technology
- the use of routine system backups

4. **Business Practices/Transaction Integrity.**

The enterprise's electronic commerce transactions are processed completely, accurately and in conformity with its disclosed business practices.

The *processing integrity principle* refers to the completeness, accuracy, timeliness, and authorization of system processing. Processing integrity exists if a system performs its intended function in an unimpaired manner, free from unauthorized or inadvertent manipulation.

- Completeness generally indicates that all transactions and services are processed or performed without exception and that transaction and services are not processed more than once.
- Accuracy includes assurances that key information associated with the submitted transaction will remain accurate throughout the processing of the transaction and the transaction or services are processed or performed as intended.
- The timeliness of the provision of services or the delivery of goods is addressed in the context of commitments made for such delivery.
- Authorization includes assurances that processing is performed in accordance with the required approvals and privileges defined by policies governing system processing.

The risks associated with processing integrity are that the party initiating the transaction will not have the transaction completed or the service provided correctly, and in accordance with the desired or specified request.
Examples of areas evaluated include:

- assurance that services or products are provided to customers as requested
- information on the condition of goods
- time frame for transactions
- payment and delivery terms
- how to cancel orders or receive customer support and service

5. **Availability.**

The enterprise ensures that e-commerce systems and data are available as disclosed. The *availability principle* refers to the accessibility to the system, products, or services as advertised or committed by contract, service-level, or other agreements. It should be noted that this principle does not, in itself, set a minimum acceptable performance level for system availability. The minimum performance level is established through commitments made or by mutual agreement (contract) between the parties.

Although there is a connection between system availability, system functionality, and system usability, the availability principle does not address system functionality (the specific functions a system performs) and system usability (the ability of users to apply system functions to specific tasks or problems). It does address system availability, which relates to whether the system is accessible for processing, monitoring, and maintenance.

Examples of areas evaluated include:

- access terms and conditions
- availability policies that conform with legal, contractual and other requirements
- procedures to handle availability problems and security incidents
- a functioning disaster recovery plan
- assurance that hardware and software have properly tested and documented availability objectives

8.10 **Control Objectives**

Management are responsible for the actions and activities of an organization. On the one hand they have a duty to shareholders to ensure that the organization is profitable and builds wealth for owners. They also have a duty of care to employees to ensure that they work in a secure and safe environment and have appropriate information to carry out their work.

As such, controls should be incorporated to meet business processes and each control implemented should be seen to have its own objective. These objectives may be summarized as supporting.

- Effective, efficient and economical operations
- Reliable financial reporting
- Effective control of systems design
- IT asset safeguarding
- Compliance with applicable laws and regulations
• Systems reliability
• Data integrity

Before implementing any control is should be possible to produce a statement that explains what the control will achieve and how it supports the business (or IT process).

8.10.1 **Effectiveness efficiency, economy of operations**

In the past IT departments have had large budgets and yet a common criticism is that they have not delivered the systems and information that the business requires. While often not considered a control issue, every organization should have in place systems to check and report on where it is spending money. The IT department is no exception.

A good starting point then is to ensure that the management and structure of the IT department is effective and running efficiently.

1. **IT strategy**

If we take a top down approach we would expect to see an IT strategic plan. We have discussed the IT strategic plan in detail in chapter 2 and 3. As information is the lifeblood of an organization there should be an information model that helps it to efficiently organize its information systems. This should be a comprehensive model that covers issues such as data ownership, data security, data relationships and data classification. It may comprise existing information such as a data dictionary or schema. The organization will need to be clear in its technology direction and how it is going to cope with emerging technologies and changing technologies. In spite of the increased use of IT to control all aspects of business, especially record keeping and accounting, effective IT departments still depend upon good interpersonal relationships. These relationships are required within the IT department and between IT and other departments. The people who work in IT have a responsibility to provide services to others. It is essential then that these people have the right skills and that they are appropriately managed. There will need to be procedures that cover all aspects from hiring a new employee to removing one. These procedures may already exist in the HR department and apply to all staff.

2. **Reliance on individual**

One issue that can be faced in the smaller to medium sized organization is the reliance on an individual. There have been cases of a programmer who developed software and is now the only person that can support it. If this programmer left the organization it may be difficult for someone else to maintain that software, especially if this programmer left the organization it may be difficult for someone else to maintain that software, especially if there is no documentation? It is also incumbent on the IT department to build its relationships with other department who are its clients. There should be effective means of communication and these can range from formal, such as a newsletter, to informal, such as IT staff having lunch with staff from other departments.

3. **Budgeting**

Budgeting is a control technique that has been around for so long that it is often not seen as a control. If you want to control how much you spend on something then you just set a limit. If you don’t give someone the money then they can’t spend it. If only it was that simple. There are many costs of IT budget over-runs
especially when it comes to IT projects. We have seen project estimating so bad that a $4 million dollar project blows out to $25 million. In addition, IT projects may have over estimated the benefits that will be achieved thus showing an attractive cost benefit analysis. While IT budgeting is a way of controlling costs on basic operational items it does not seem to work so well for projects. Thus any improvement in project estimating and subsequent budget allocation will help control this area of expenditure.

As well as controlling IT project budgets it is essential that projects be controlled by effective project management processes. There are many methods on the market but it is surprising how few organizations actually follow any methodology.

Just as IT is critical to the organization and deserves special attention so do IT projects. An IT project can waste money, time and resources, it can deliver poor applications, it can cause disruption and loss to the organization if it is not managed properly. An important control requirement for all IT departments is that they apply sound project control and management.

4. **Measures of effectiveness**

Effectiveness can be evaluated by the evaluating:

- System quality
- Information Quality
- Task completion

I. **System quality**

System includes all hardware and software components and network infrastructure. Following are the indicators of system quality:

- Response time
- Turnaround time
- Stability of the system
- Ease of interaction
- Extent of idle output (output not utilized by the users)
- Quality of documentation
- Help facilities
- Ability to integrate with other applications

II. **Information quality**

The qualities of information have been discussed in chapter 1

III. **Task completion**

A good information system must completes all the task allocated by the users within time specified and with the required quality. Some of the factors that shows the task completion are:

- Decision accuracy
8.10.2 Reliability of financial reporting

A major consideration for the external auditors is whether they can rely on the figures as produced by the computer. However, when we consider any data, whether it is used for financial reporting or to assist management we expect it to be correct. We don’t expect it to be in error or to have data omitted.

Although we will discuss this issue as a separate topic, all controls really have as their ultimate goal the correctness and reliability of data. There is an old saying in the IT industry – Garbage in. Garbage out. It is essential that the data be controlled throughout the transaction lifecycle. It needs to be input correctly, correctly processed, correctly stored and output correctly. There well need to be controls applied at all these stages.

Again, to demonstrate how controls relate to business processes (a COBIT philosophy) let us consider a manager receiving financial reports and what he or she might be looking for.

Usually the manager will want information that is relevant to them personally. A sales manager will need sales figures for his or her area, a marketing manager will want shipping statistics.

They will want to rely on the figures and this the figures are accurate. There may be reasons why figures in a report are not correct, not through error but misunderstanding. For example, a sales manager may have been recording sales in a spreadsheet. When the financial figures are published they do not agree with the total in the spreadsheet. Further investigation reveals that the financial period closed on the closest Friday to the month end but the sales manager is showing the total sales for the calendar month.

Since the sales manager’s boss wants to see the sales for a calendar month the spreadsheet figures are considered correct and the others ignored. The use of this spreadsheet then raises lots of control issues. It is preferable for the organization to agree on a standard reporting period and to ensure that reports issued from the system are considered correct. This would require a control that is basically a simple change to procedures.

We often use the words data and information interchangeable but there is a difference between the two. Data is the raw figure such as 12. Information is putting that data in context such as Quantity sold = 12. A good information system (as its name implies) provides the user with information not just data. One way of improving the information provided is to also supply comparative data such budget or previous periods. Thus knowing that the quantity sold is 12 but we were hoping to sell 10 could be cause for celebration.

8.10.3 Effectiveness of design

The best time to incorporate controls is in the design phase before anything has been built, and so this phase is particularly interesting to auditors. They should try to ensure that they can review the design and requirements documents to ensure that controls have been incorporated. Again the auditors must remain independent, as they will later be called upon to audit controls that they may have designed.

However, just like project management needs controls, there are specific controls that need to be in place to control the design process. Is being undertaken correctly there needs to be standards or benchmarks against
which to monitor it. The organization may have adopted a system development method or a CASE (computer assisted software engineering) tool.

A problem may exist if the standards are now dated or inappropriate for the current, development that may be using new technologies or development processes such as object, oriental programming.

Weber’s textbook Information System Control and Audit. Chapter 4, discusses systems development controls and describes six development processes?

- Systems Development Life Cycle approach which is the traditional multi-phased approach
- Sociotechnical Design approach which takes into account the affect on users.
- Political approach which considers changes in power bases
- Soft-systems approach which focuses on the problem especially if users cannot articulate their requirements.
- Prototyping approach, which quickly produces models of solutions that can be shown to users who can refine them until the model represents their requirements.
- Contingency approach which takes a risk assessment of factors that may impact development and then uses which ever technique is appropriate

No matter which method is used the development process will still pass through similar phases that will need to be controlled. These include:
- Requirements specification
- Analysis of existing processes
- Acquisition or development of solution
- Testing
- Implementation and roll out
- Maintenance

8.10.4 IT asset safeguarding

It has always been a duty of a manager to safeguard the organization’s assets. In many organizations especially service business the IT equipment may be the most costly asset that it owns. Even if the equipment is leased or hired there is a duty of care that must be exercised.

There are two main aspects that should be considered here:

1. is the correct equipment being acquired and will it be fit for its purpose and have an acceptable life span?
2. is equipment protected against theft, five and other disasters?

The first issue should be controlled as part of the IT strategic plan and the development of the technology infrastructure. This has been discussed earlier.

As far as the second issue is concerned we need to consider controls over three main categories of equipment:
1. Centralized computer equipment such as mainframes, servers and associated telecommunication devices.
2. Decentralized computers such as workstations that are in offices and notebook computer that are often out of the offices.
3. Consumable items that are subject to theft.

In the early days of computers the size of the equipment meant that theft was not an issue. The equipment also needed a special environment in which to operate and so it was placed in secure rooms. Fire prevention or detection devices were also common as the cost of the computers easily warranted the investment. As the price of computer dropped, and they needed no special operating conditions they could be positioned in general offices. Often there was no physical security and only the standard office fire detection devices.

In today’s office you may find that if an organization has downsized from a large computer then they may have kept the secure environment and this is where they will place their servers, routers and other network equipment. This is an ideal situation and the best way to safeguard the computer asset. Even so, it is most likely that this organization will have large amounts of capital tied up in PCs that are on desks in less secure office environments. It many cases the value of workstations is greater than that of the servers. Often little attention has been paid to safeguarding these. Theft of desktop computers is now commonplace.

We have discussed threats pertaining to physical access to an information system.

### 8.10.5 Compliance with applicable laws and regulations

Most organizations will want to obey the law. There are different obligations and compliance requirements placed on an organization including:

- Common law
- Industry specific legislation
- Tax requirements
- Copyright especially software issues
- Privacy and confidentiality of information
- Safety and ergonomic issues

In addition, when considering control issues, the organization must be looking at acts of employees and acts of third parties. For example, breaking software copyright rules is most likely to be done by an employee. A backer breaking into the system may gain access to confidential information. Each requires a separate control technique.

Before implementing the controls it is important to understand the regulatory framework in which the organization operates. One would expect that senior management would be aware of these but you may need to go back to a ruling or seek legal counsel. Also, the organization may have entered into a specific contract that places an obligation on it to provide reports and other information at regular intervals, especially joint ventures.

Typically user controls such as passwords and access right are used to control access to information and software. These can help stop backers accessing information and users coping software. They do not stop authorized users using the information illegally.
To meet the licensing requirements of your software it is necessary to also control access to the original distribution media such as CD-ROM. It is so easy today to copy a CD-ROM. The organization should also organize for a regular audit of PCs to ensure that only authorized, licensed software is in use.

We all know that an audit is not primarily designed to detect fraud but the controls that the auditor will be looking for should assist the organization meet its obligation to prevent and detect fraud error and illegal acts.
We have discussed more regulatory and external requirements in detail in the chapter Risk analysis.

8.10.6 System reliability

We have stated that the data must be reliable. It must also be timely and available when the users want it. In systems reliability we need to consider both the availability of the hardware and the quality of the software.

The organization should undertake a risk analysis and identify the impact of downtime on the organization. The analysis should consider both short and prolonged periods without access to the systems. More information on the risk analysis will be found in a later section.

At the very least we would expect to see devices such as Uninterruptible Power Supplies (UPS) for servers and critical equipments. There should be adequate backup to removable media and IT staff should be trained to be able to recover lost files.

The equipment should have appropriate maintenance procedures and this should be carried out at an appropriate time to minimize disruption to staff. Recovery procedures should also be checked and tested regularly.

Managers have a right to expect that the information that they are working with and the reports that they produce are secure. The most common way of controlling this in through user passwords and access rights. There may be a need to use encryption or stronger security on a highly confidential document.

As discussed in the section on financial reporting there should be controls to ensure that the information is correct. One important element of this is that the software operates as expected.

There are many techniques for checking the quality of the software and these are normally employed during the testing phase before the software goes live. However, it is still possible that good software is scheduled or run increased and so another control issue is to consider the processing integrity, especially if a service of programs are run. An example may help explain this.

Every night an extraction routine takes data out of the transaction processing system into a data warehouse system. The data warehouse data is input to a reporting process that manipulates the data and puts it into a file structure that can be read by a Business Intelligence (Bl) tool. The whole process takes 7 hours.

When users arrive for work at 8:00am they use the Bl tool to analyze the previous days sales figures and to fix prices and deals for that day.

One day changes are made to the transaction processing system that cause the extraction routine to fail part way through. It is possible that the rest of the sequence may continue without error but the users will be looking at inaccurate data.
8.10.7 Data Integrity

Data integrity which also implies reliability is a major goal of IT controls. In order to have confidence in the data we need to ensure that the software that processes it is controlled and that the data itself is controlled.

The diagram below shows some of the control techniques that can be applied to the software and those that can be applied to ensure that the saw data flows though to produce information. That we can rely on.

A full description of many of these controls processes was given in Module D and so we only summaries each of them here.

- Quality processes to ensure that the systems development process follows a standard approach to ensure that the software will produce the desired effect.
- Change processes to keep track of changes in equipments and versions of software to ensure that bug free and reliable software is developed and in production.
- Security processes to ensure that only authorized users can access the software that is used to capture, process or report on the data.
- Education of assets so they use the software correctly and know how to use the controls to verify data.
- Completeness controls to ensure that all the data of input, errors corrected and reentered.
- Accuracy controls to ensure that the data is correct especially at initial capture but also whenever additional processing takes place.
- Currency controls to ensure that the data is the most current and that old files or data are not used.
- Timeliness controls to ensure that the information gets to the user promptly or in a time frame that the information is still useful to them.
- Consistency controls to ensure that the information is the same no matter in which from or structure it is viewed.
- Comparability controls to ensure that the data has appropriate comparatives to provide better information to the user.
- Authorization controls to ensure that over-rides or changes made have been made by an authorized user.
- Auditability controls such as logs and audit trails so data can be tracked and traced after the event.
Chapter Roundup

- Control frameworks
  - You must know what impacts the controls required in an organisation.
  - Controls must be cost effective and meet an objective.
  - Organisation risks must be analysed and appropriate controls implanted.
  - Auditors will now be reviewing IT systems and looking for appropriate controls.
  - There are IT standards and audit review processes that may need to be adhered to such as – COBIT, SysTrust, WebTrust, SAS70, ITGI

- COBIT project provides an
  - Executive Summary,
  - a Framework for control of IT,
  - a list of Control Objectives, and
  - a set of Audit Guidelines. (The control objectives and audit guidelines are referenced to the framework.)

- Control objectives
  - Management are responsible for controls.
  - Controls have to support business objectives and safeguard resources and assets.
  - IT must be efficient and use its resources effectively.
  - IT must therefore support the business goals and strategic plan. Other plans then flow from this.
  - Technical and information plans will also be required.
  - These plans are part of the overall control process and also feed information as to what detailed level of control will be required.
  - In spite of the use of technology, interpersonal skills are still essential for the IT manager and many IT staff members.
  - Setting the IT budget is an important control process to manage the funds that are used by IT and to help use them effectively.
  - IT projects can waste funds and so need to be effectively controlled.
  - Managers must be able to rely on the data and information provided by IT especially in the financial area.
  - Systems design must also be carefully controlled.
  - It is at the design stage that system controls need to be considered and included as user requirements.
  - Different design approaches will require different control processes but the principles stay the same.
  - IT department and user workstations may represent a large value asset that needs to be safeguarded.
  - The right equipment needs to be selected in the first place based upon the strategic plan.
  - IT equipment is now very portable and so a target for theft and abuse. This needs to be controlled.
  - All organisations should be following the law and this applies to all aspect of IT development and operations. Most importantly copyright rules must be adhered to.
Attempts to thwart controls may come from an employee or external person. The former is the most common but is usually hushed up; the latter gets the largest press.

Users may not be able to do without their systems anymore and so reliability and recovery are big issues.

Data integrity is paramount and there are several control techniques that may be used including – quality processes, change processes, security processes, education of users, completeness, accuracy, currency, timeliness, consistency, comparability, authorisation and auditability.

Practice Question

**Q No.1)** COBIT management guidelines identify a list of generic Key Goal Indicators. Define in your own words a “Key Goal Indicator” and list 6 that are applicable to all IT processes.

**Q No.2)** Describe major types of computer abuse that an organisation may experience.

**Q No.3)** Describe how losses can occur through error, fraud and social costs.

**Q No.4)** When would an organisation consider a WebTrust review?

**Q No.5)** How would you determine whether the IT strategic planning process was effective?

**Q No.6)** How does having a clear IT strategy assist an organisation decide when (or whether) to adopt a new technology?

**Q No.7)** Network administrators will often be granted high level security privileges so they can administer the network. What security concerns does this raise and what can be done about this?

**Q No.8)** Give examples of different interpretation of data.

**Q No.9)** As an auditor you may be called upon to review aspects of the design of the new system. Describe briefly how data flow diagrams and entity-relationship modelling are used to represent a system.

**Q No.10)** Prepare a set of procedures that could be handed to staff who are to be issued with notebooks that could help minimise theft or loss.

**Q No.11)** What controls may be incorporated to ensure that users do not misuse data?

**Q No.12)** How could you design controls to at least warn of the processing error that was described in the example?

**Answer to Q No 1)**

Students should be able to provide a definition based on the one supplied in the COBIT guidelines but not word for word

Students might identify any of the following list of KGIs:

- Achieving targeted return on investment or business value benefits
- Enhanced performance management
- Reduced IT risks
• Productivity improvements
• Integrated supply chains
• Standardised processes
• Boost of service delivery (sales)
• Reaching new and satisfying existing customers
• Creation of new service delivery channels
• Availability of bandwidth, computing power and IT delivery mechanisms fitting the business, and their uptime and downtime
• Meeting requirements and expectations of the customer of the process on budget and on time
• Number of customers and cost per customer served
• Adherence to industry standards.

Answer to Q No 2)

Suggested solutions should include incidents of
• Hacking.
• Viruses.
• Unauthorised access.
• Denial of service.
• Theft of assets.

Answer to Q No 3)

Solutions to this question may be varied. Error and fraud should not pose much problem as these can be directly linked to money. Social costs can also occur if the government wastes money or an organisation wastes money. In the former it may result in higher taxes, with the latter there could be cost cutting and retrenchments.

Answer to Q No 4)

The solution should refer to the fact that this basically provides assurance that a Website is credible and secure. It would be a useful review if an organisation wanted to have independent proof that it can conduct e-commerce or other network services.

Answer to Q No 5)

The solution should cover areas such as:
• Obtain policies and procedures documents to identify the planning process.
• Review the long-term goals and objectives of the organisation.
• Check that the IT strategic plan supports the business.
• Evaluate the long and short term plans to ensure that they are in accordance with the strategy.
• Review minutes of meetings to understand how decisions may have been arrived at.
• Consider the process to handle change and how this could impact the plans.
• Examine how the plans have been turned into operation tasks and activities.

Answer to Q No 6)

The solution should cover issues such as:
• New technologies should not be adopted just because they are new.
• There must always be a cost benefit analysed as part of a business case.
• New technologies should be researched.
• The technology should support the organisation’s strategic plan.
• The organisation should have a policy regarding adoption of standards or new proprietary methods.

Answer to Q No 7)

The solution should consider:
• Network administrators will be in a position of trust.
• They should be carefully recruited and references and security checked.
• Parts of the job can be boring but require high-level security clearance. For example setting up a senior manager as a user and allocating this manager access to files, normally requires the administrator to have high security access.
• Administrators will know much more about the network than managers and possibly auditors.
• If administrators are to be restricted in their actions then someone will need to know the intricacies of the system to be able to shut them out.
• There may be a need for levels of administration with appropriate restricted access rights.
• All audit logs should be independently reviewed to monitor administrator accesses as necessary.

Answer to Q No 8)

Examples include:
• Timing of transaction, i.e. goods shipped on the 30th of a month but not processed until the 1st of the next month.
• Different definitions of sales value, i.e. does it include transport costs or not?
• Goods or services provided over a long period of time may be treated as a one off sale in one report but apportioned over time in another.
• Are orders really sales?
• If goods are returned should they reduce the sales amount?

Answer to Q No 9)

The solution should cover the fact that a DFD is a representation of the flow of data. ERM shows relationships between entities that are more attuned to the real world way a system operates.
Answer to Q No 10)

In the solution we would expect to see issues such as:

• Make use of any built in password/security to use the computer.
• Do not check in but carry on board when flying.
• Do not hand to porters but carry always.
• Lock away at night in a desk or storage area.
• Do not leave in cars.
• Do not place on back seat of a car.

Answer to Q No 11)

In the solution students should consider:

• Logical and physical controls that may be used to identify the user.
• Grouping of users to manage access.
• Identification of confidential data and categorisation of information.
• Effective use of permissions to control access.
• Log files and audit review to ensure appropriate access.

Answer to Q No 12)

The specific controls would depend upon the scheduling software that was used but in principle the solution should cover:

• Batch controls could be used to calculate the new, expected totals and if these did not balance a warning issued.
• If batch controls are not used other control totals or numbers of records could provide a similar warning.
• As the process progresses files may be created and subsequent operations could check for the existence of a file.
• File dates and times could be checked.
• Error logs may be manually reviewed before users start operations.
9 IS Risk Management

<table>
<thead>
<tr>
<th>Topic List</th>
<th>Syllabus Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.1 Risk Analysis</td>
<td>2.7</td>
</tr>
<tr>
<td>9.2 Threats to the Organisation</td>
<td>2.7</td>
</tr>
<tr>
<td>9.3 Specific threats</td>
<td>2.7</td>
</tr>
<tr>
<td>9.4 Consequences of the threats</td>
<td>2.7</td>
</tr>
<tr>
<td>9.5 General protective measures</td>
<td>2.7</td>
</tr>
</tbody>
</table>

Introduction

This chapter covers the risk analysis which is a part of risk management. Risk management is the core objective of any IS/IT control system, so students must understand the issues raised in this chapter. It is unlikely that a scenario involves all the threats discussed in this chapter, but students should use these as a checklist to identify the relevant threats and controls. Although we have discussed the control activities in the next chapter we have given few control measures to counter the threats discussed here. Students should use these measures in conjunction with those discussed in the next chapter to answer the scenario questions.

Study Guide

**Risk assessment (Study textReference 9.1)**
- You should discuss the basic approach to a risk analysis and if possible may want to demonstrate or show specific risk methodologies.

**Risk categories (Study textReference 9.2 and 9.3)**
- Some risk analysis material was discussed in Module D but we will go into greater depth here.
- Get students to consider what can happen if IT systems fail and consider the various events described in the Student Guide. Identify any others that students can think about.

**Probability of loss (Study textReference 9.3)**
- If you have access to a methodology they may use different ways to consider the possibility of loss. In the text we consider a simple approach.

**Consequences (Study textReference 9.5)**
- Explain that the controls may also be assessed on a cost benefit analysis. That is, what will we lose versus what it will cost us to prevent.
9. **IS Risk Management**

Risk management consists of the following steps:

- Identification of the risks.
- Estimate of their downside effects i.e., the implications of what could go wrong
- Estimation of the probabilities of the events occurring. It will be difficult to establish precise probabilities, but it will be necessary to establish some type of prioritisation: some risks will be much more likely than others. Attention must first be paid to the more important threats.
- Decide how the risks will be handled.

Risks can be handled as follows:

- Do nothing. This is appropriate where the effect is small or the chance of occurrence very remote.
- Insure against the risk.
- Off-load the risk, for example by arranging for third parties to complete part of the project.
- Investigate the risk further and try to protect against it. For example arrange to have additional staff available in case of project overrun.

### 9.1 Risk Analysis

To say Risk Analysis is an important issue is an understatement. It is difficult to quantify the losses suffered each year by businesses arising from the use and misuse of Information Systems (IS). In Ernst and Young’s 1998 report *Fraud: the unmanaged risk* the total losses experienced by 132 companies exceeded US$628 million, with over half of the respondents having been the victims of fraud during the year. Add to that the costs from virus infection, accidental and malicious damage and from technical failures and the total is staggering. Conservative estimates start at around US$7.5 billion.

The risk analysis may be specifically undertaken when a new application is being planned or implemented or if new equipment or technologies are being installed.

IS risk analysis is the process of:

- identifying potential threats that may cause a loss;
- designing and implementing controls to prevent them, and, should these fail;
- designing and implementing controls to detect any occurrences and to minimise their effect.
9.2 THREATS TO THE ORGANISATION

There are always threats to an organisation during the operation of any system, whether the system is manual or computer-based. Computer systems are much more vulnerable to risk because of the power and speed of the computer, and because problems are more difficult to identify.

The extra problems of computer systems are:

(a) Data stored on magnetic media is much more liable to undetected corruption or loss.

(b) The computer can be accessed remotely via the public communications network - unauthorised people can access and change data.

(c) No automatic trace of computer transactions is created. If a problem occurs, it may be impossible to correct or even detect inaccuracies in the data.

(d) The computer can carry out processes so fast that a great deal of damage can be done by the time that an error has been detected.

(e) The computer does not have an automatic 'feel' for what is reasonable.

9.2.1 Types of threat

Five basic types of threat to an organisation relate to information technology are stated under, in the next section we will study some specific threats in detail.

1. Physical damage to hardware or computer media

Malicious damage, poor operating conditions, natural disasters and simple wear and tear can physically damage machinery and storage media such as disks, tapes and diskettes. This carries a triple threat - the cost of repair or replacement of hardware; the danger of damaged data or program files; and the cost of computer down time.

2. Damage to data

Hackers, viruses, program bugs, hardware and media faults can all damage data files. The havoc caused by damaged data is made worse if it is not detected and rectified quickly.

3. Damage to humans

Computers and peripherals can cause hazardous conditions for operators and users. They can receive electric shocks, trip over wires, gash themselves on sharp corners, or be injured in fires. Sometimes physical precautions against computer damage can themselves create danger. Some units, for example, are protected against fire by being flooded by CO₂ gas. If someone were trapped when this happens, serious injury or death may result.

RSI - Repetitive Strain Injury is an injury caused by constant repetition of specific activities such as the use of keyboards. It can cause long-term problems and has forced many individuals into premature retirement and their employers have had to pay large damages claims.
To avoid physical trauma to users of computer equipment, attention should be paid to their needs when designing workstations and setting up the computer installations. Measures that can be taken to protect staff include:

(i) Good ergonomic design

Workstations should be designed for comfortable use by the people who are going to use them. The lighting must be such that there is no glare or reflection from screens. The screens themselves should be designed to reduce the amount of flicker, which is extremely tiring to the eyes. Furniture must be a comfortable height for the average user, and should be adjustable to fit the needs of the non-average user. The designers of workstations should also avoid sharp corners and projections that users could accidentally bang themselves on. Wires should not be in a position where people can trip over them.

(ii) Ducting and false floors

To avoid the damage to both users and equipment that can be caused by tripping over cables, they should be fed through ducting or passed through false floors and false ceilings.

(iii) Safety awareness and training

Most accidents are caused by human error, so it is important to stress awareness of safety in the workplace. A high priority must be placed on the well being of staff, which will cut down on absenteeism and sickness, reduce costs and increase the effectiveness of staff.

4. Operational Problems

Program bugs and operational mistakes can cause significant problems, ranging from the need to resuscitate files and repeat computer runs to the possibility of losing customers.

5. Industrial espionage/fraud

Industrial espionage and sabotage can yield significant advantages to competitors, and fraud and blackmail is a significant threat.

9.2.2 The underlying causes of problems

The basic causes of problems are:

- Human error - The most prolific cause of problems is human error
- Technical error - Hardware or software malfunction is another significant risk, with communications equipment giving especial problems.
- Natural disasters - Natural disasters (bad weather, earthquakes, fire, flood, etc) cannot be avoided completely, but their possibility must be catered for.
- Fraud, espionage, sabotage - The deliberate actions of individuals can result in significant loss, whether these actions are for personal gain, for competitive advantage or for revenge or malice.
- Poor personnel relations
• Technology obsolescence - The pace of change shows no signs of slowing down. Equipment can become obsolete long before it is written out of the books. Often its trade-in value is nothing. While there is nothing intrinsically wrong with using out of date equipment the organization may eventually find:
  • spares are difficult to source
  • competitors are using new technologies and gaining an advantage
  • staff want to work on the latest equipment and so it is difficult to attract and retain them
  • new applications will not work with older equipment or operating systems.

• Vendor goes out of business - Although there are fewer proprietary systems than there used to be there is still a risk that vendor goes out of business. This can immediately impact the support of your equipment and applications. Even large companies are not immune to this as witnessed by the demise (for takeover) of DEC, Sperry, Control data, Lotus, etc.

There are another group of risks that are likely with IT projects so these have been grouped together below.

• Excessive cost - A control objective is to ensure that funds are not wasted. There have been many reported cases of projects that blew their budgets or were abandoned, often with no deliverables to the organization.

• Takes longer than estimated - Usually related to cost blow out, many projects are not delivered on time. This may mean that the organization does not enjoy the benefits that were expected or by the time of delivery the situation had changed and the project deliverable is no longer useful.

• Statutory changes - Some IT projects may take several years to complete. During that period there may be many changes that will impact the project such as changes in legislation, economic outlook, environment, etc. again this can result in wasted resources or constant changes.

• Champion changes - It is normally good for a senior person to champion project and to keep pushing it through. However, if this period on leaves it may be that the new person has different priorities and the project is not one of them.

9.3 Specific threats

Now will identify and briefly describe some specific risks that computer systems are exposed to and, for each of these risks, suggest some appropriate controls.

9.3.1 Physical threats

Physical threats can result in many kinds of damage to an installation. All parts of the system are vulnerable, including the machinery, the environment, computer media, software and the people using the system. The resulting damage can be so crucial that companies can be completely bankrupted by physical disasters that they have not properly protected themselves against.

Once the physical threats to an installation have been catalogued, measures can be developed to counter them. Many of these measures will cost money, but others may just entail the introduction of good working practices.

Those counter-measures that do cost money need to be cost-justified. The cost-justification will not always be formally carried out, but management will need to know how much their counter-measures are costing.
The actions that can be taken to protect against physical threats can be categorised as follows:

(a) Preventative measures
All possible measures must be taken to stop problems from occurring.

(b) Detective measures
If a problem has occurred, the organisation must find out what has happened so that the effects are minimised

(c) Corrective measures
After a problem has been discovered, its effects must be minimised and the organisation must take action to return the situation to normality.

The problems that do escape the net of the preventative measures adopted by the organisation may reveal weaknesses that need to be countered in the future. Planning against threats must be regarded as an ongoing process.

**Environmental control**

One of the most powerful protections against physical threats is to isolate the computer installation as far as possible from the rest of the world. The degree to which this can be done will depend upon the size and value of the computers and the importance of the systems that run upon them. Mainframe computers are likely to be enveloped in a protective cocoon, whereas personal computers have fewer external protections and must be more inherently robust - more tolerant to imperfections in their environment. Some machines are built to withstand extreme conditions, especially those that are designed to be used outside.

More generally, however, business computers have protective measures built into their environment. These measures include:

(a) A separate/segregated area that will enable the section of a building containing the computer facilities to be totally controlled. Air conditioning and dust controls will ensure that the computer equipment operates under optimum conditions.

(b) Static control mats that dissipate static electricity before it can build up into a damaging charge.

(c) Connection through separate electrical circuits.

Spikes, surges and dips in the electricity supply are not only caused by problems in the public network. There may also be problems caused locally within the building itself. A particular danger is when more than one piece of electrical equipment shares the same circuit. The switching on of a power-hungry piece of equipment is likely to cause a significant dip in the power available to machines that are already switched on. Even machinery such as electric kettles and vacuum cleaners can cause problems to computers. It is unwise, therefore, to connect sensitive equipment such as computers to circuits shared by other machinery.
Physical threats include:

1. Fire

Fire is a very serious hazard to a computer system. It can damage or destroy every part of a computer installation - hardware, software, data files and the original transaction documents. Even the people involved and the fabric of the computer installation are at risk from fire.

It is not just the flames that cause the damage; heat, smoke, dust and the substances used to fight the fire are all very destructive.

Controls

There is a range of measures that can be adopted to protect against the risk of fire:

(a) training of staff to be alert against fire;
(b) control of combustible materials;
(c) regular fire drills;
(d) smoke and heat detectors;
(e) fire alarms;
(f) fire doors and automatically closing doors;
(g) automatic extinguishers - carbon dioxide - water sprinklers (where appropriate)
(h) manual foam based extinguishers;
(i) regular backing up of files and transaction data;
(j) fire-proof, water-proof safe for back-up media;
(k) holding back-up materials off-site;
(l) regular servicing of machinery and maintenance of electrical equipment;
(m) the use of computer bureaux if machinery is damaged;
(n) 'planned redundancy' - the availability of more than one machine, so that work can be transferred onto another machine if one is affected;
(o) insurance cover.

Not all of the above measures are adopted in every organisation - some measures are alternatives to others - but there is often a synergy between some of the above measures, with several measures being more effective if they are used in combination. Insurance premiums are likely to be reduced if insurance
companies are satisfied with the other measures adopted. Regular backing up of data is of little use unless the back-ups are stored in a fireproof safe or at another location.

2. Clamminess and bad weather

Water can be extremely damaging to any kind of electrical equipment. Rivers and seas overflowing may cause flooding, or it may be caused by the results of fighting fires within the building. Computers sited in the basement or ground floor of buildings are more susceptible to flooding than those sited on upper floors, although the floor immediately underneath a water tank may also be at risk.

Bad weather can harm an installation by physically damaging the fabric of the building, by damaging hardware or computer media, or by interrupting the power supply. The worst damage is caused by extreme weather such as high winds, torrential rain or thunderstorms, but long term erosion of weathering can also degrade the fabric of the building and harm the computer installation.

Although the threats posed by wind, rain and extreme temperatures are significant, the most common weather-based threat is lightning. This can act in a number of ways:

(i) A lightning strike on the building may damage the fabric of the building or burn out electrical cabling and other equipment.

(ii) The cabling connecting different machines in a network may be struck. This can damage several machines at the same time, and disable the network.

(iii) Overhead pylons carrying high voltages are very commonly struck by lightning. This can cause power surges and spikes in the electricity supply to the computer installation and damage equipment several miles from the lightning strike. Data files corrupted by this occurrence must be reconstructed and can cause a great deal of ‘down time’ in an unprotected organisation.

Controls

Several of the measures to protect against flood and weather have a more general value. The regular taking and safe storage of back-ups, the use of external bureaux or planned redundancy and the use of insurance policies to mitigate the results of disasters are examples of general-purpose protective measures.

Some of the more specific measures are:

(a) Careful siting of hardware

Computer machinery should be installed away from dangers. Organisations will usually avoid the basement and other areas that are vulnerable to flooding. Most computers of any kind, including PCs, micro computers, will not be put into temporary office buildings unless operational reasons dictate that they should be.

(b) Regular building maintenance

If the building is well maintained there is less chance that leaks will cause major problems.

(c) Shielded cabling

Cables and wires are vulnerable to water as well as to lightening strike. If there is a weakness in the cable, electricity will ‘track’ across a damp surface causing further degrading.
(d) Current isolators

Specialised equipment can be connected to the power supply to 'flatten out' spikes and other uneven patterns in the amount of electricity coming through. Spikes can cause computers to make errors and damage disk contents.

This minimises the danger of damage to computer media or hardware.

(e) Back-up generators

In the event of a power failure, a back-up generator can be switched on to enable processing to continue. These generators may be tripped automatically to minimise disruption.

(f) Shatter-proof glass

Shatter-proof glass will minimise the problems caused by explosions and similar terrorist activities.

3. Natural disasters/terrorist attack

Earthquakes and explosions are potentially disastrous to people, machinery and buildings. They are also likely to disrupt communication lines. Damage caused by terrorists may be an accidental side effect of an attack on another target, or it may be specifically aimed at a commercial or military organisation.

4. Uncontrolled physical environment

A great deal of equipment and computer media needs to be operated in a controlled physical environment. Although it is less important for PCs, they are still susceptible to many hazards. Dangers include:

(i) dust
(ii) heat
(iii) cold
(iv) humidity
(v) spillages (coffee/tea/soft drinks/food)
(vi) static electricity
(vii) magnetic fields
(viii) power failure/irregular current/surges/spikes.

5. Deliberate physical attack/fraud

In addition to the sort of terrorist attack described above, computers are also liable to attack from disgruntled employees, ill-disposed members of the public, thieves, industrial spies, blackmailers and extortionists, and other criminals. There are a number of such hazards that installations need protecting against:

(i) hardware sabotage
(ii) hardware theft
(iii) software piracy
(iv) blackmail and extortion
(v) copied or stolen data
(vi) unauthorised alteration of programs
(vii) false transactions being applied to data files
(viii) loss of confidentiality
(ix) physical interception of data communication
(x) the use of detection equipment to show what is being displayed on computer monitors. Equipment similar to television detector vans can intercept the radiation from a monitor and display a facsimile of what is displayed on the screen. This equipment can operate over a distance of many yards.

Control against fraud and data theft

Once people have gained access to computer facilities they may try to enter false transactions or to copy data. There are a number of measures that can be taken to detect when this is happening and to avoid likely problems. The measures that can be taken include the use of physical devices, operational procedures and security software.

The sort of security procedures that may be adopted include:

(a) Strict controls over input/processing/programs
(b) Strict division of duties.

There should be no confusion over which person should be doing each job. In this way the chance of problems occurring is very much reduced, and if problems do occur than it is much easier to establish what has happened and to rectify the situation.

(c) Internal audit review systems

It should be possible to trace back all the events that affect data files. An audit trail will enable management to identify when any problems have occurred and find out what the causes of those problems were.

(d) Encryption of data

Data may be 'coded' so that it is not understandable to any casual observer who does not have access to suitable decryption software. Encryption provides a double benefit. It protects against people managing to gain access to the system, and it protects against the 'tapping' of data whilst being transmitted from one machine to another.

(e) Shielding of VDUs

To protect against people with detection equipment being able to remotely view what is being displayed on VDUs, the units may be shielded to prevent the transmission of radiation that can be detected. Computers containing sensitive material can also be sited so that they are out of the range over which detector vans can operate. Some defence establishments have been known to install PCs accessing sensitive information in metal lined rooms with no outside windows to eliminate the chance of unauthorised individuals viewing what is being shown on the screen.
9.3.2 Unauthorised access from inside

According to some surveys, 84% of reported IS related frauds were carried out by the companies own employees, most often managers. Common examples include the setting up of ghost employees onto payroll systems and changing delivery note details to divert goods to the employee’s home address.

Controls

A job sensitivity analysis should be performed identifying roles where there is a higher than average potential for fraudulent transactions e.g., payroll supervisors, system supervisors.

Recruitment procedures for these roles should be particularly stringent with at least two references and criminal record report obtained. These staff should also be actively monitored, in particular for unusual behaviour. Long periods without holidays, a surprisingly lavish lifestyle (holiday destinations, car driven) or a tendency to regularly work late at night or during weekends when there are no other staff around are good early indicators that a problem may exist. User logs, maintained by the computer system, can be helpful in this review.

The next step is to ensure that only these reliable staff can access the system. This is usually achieved by using a good password protection system, that is one requiring passwords which are imaginative, chosen by the user, changed at regular intervals, not divulged to anyone else and not displayed on screen.

Passwords are often accompanied by a User ID, created by the system administrator and allocated to users. These restrict which parts of a system a user can access and what tasks (s)he can perform.

A typical User ID might have a pattern such as ACS-SNR-GM. The ACS denotes that the user can access the accounts system, SNR (for Senior) will restrict the tasks (s)he can perform (they might be able to inquire about employee wage rates but not be able to change them) and the final GM their initials, allowing a log to be kept that can differentiate between the accounts departments seniors.

The password controls who can access the system, the user ID controls what they can do once logged on.

9.3.3 Viruses

The recent hysteria surrounding viruses such as Melissa and Chernobyl probably do overstate their impact, but viruses can cause significant disruption, most commonly slowing system performance by generating high volumes of e-mail traffic and sometimes by corrupting or destroying data stored on fixed disks. They can be introduced innocently or deliberately, by your own staff or by third parties via e-mail.

Controls

Antiviral software such as Dr. Solomon Anti Virus Toolkit should be acquired and any updates received loaded onto the system promptly.

Where there is internet or e-mail connection a firewall should be set up. Most often a firewall is a separate computer installed to inspect incoming data and decide whether it appears suitable for acceptance onto the main system. Typically they search for files that are unusually large or have a specific filename or extension (such as .exe files). Any suspicious files would either be returned to their sender or opened by a systems supervisor on a separate computer.
Viruses are often transferred innocently by employees taking work from an infected home PC back to their office computer. This can be prevented by allowing the employee to reclaim the cost of anti-virus software for the home PC. Alternatively, the disk drives on their work computers can be disabled. This has the effect of requiring data to be transferred via e-mail (where viruses will be intercepted by the firewall) or by diskette where the diskette can only be loaded and simultaneously virus scanned by a system supervisor.

9.3.4 Unauthorised access from outside

In addition to increasing the risk of virus infection, the widespread acceptance and use of e-mail and the internet brings increased risk of external access to systems either to amend data or to obtain commercially sensitive information. A website from which you can download software (BO2K from CDC) that allows users to obtain remote access to another PC has now had more than 130,000 hits.

Controls

The control required depends on where the authorised outside access will come from. Where external access always comes from predictable locations - say the regional head office of a supermarket chain being contacted by one of the 50 stores in its region a callback system is best -

Where external access comes from unpredictable locations - say an audit practice allowing staff to dial in for e-mails from hotel rooms or client premises - the system cannot know the telephone number to make the return call to and so a code generator system will be used

9.3.5 Natural disasters

Lightning never strikes twice? I have worked for a company where, in a three month period, there were two separate lightning strikes, each knocking out the company’s main transaction processing system. (The substantial above ground power and network cabling attracted the atmospheric electrical activity.) Damage caused by fire and flooding is more common and when these affect computer systems they cause substantial damage.

Controls

The main computer room should not be in the basement (flooding) but ground floor or higher. You can also learn from one New York company whose 42nd floor computer room was flooded - by a burst pipe. Do not place your computer underneath any air-conditioning units or water pipes.

The room should have at least one wall of fireproof glass - this visibility allows passing staff to detect any problems and also deters unauthorised access - and be equipped with smoke detectors and extinguishers suitable for electrical fires.

The main servers should be connected to the power supply through an Uninterruptible Power Supply (UPS). UPSs have two purposes:

- to protect the computer from damage by any electrical surges, as can be caused by lighting strikes onto power supply cables;
- to provide a reserve of power sufficient for users to complete current processes and allow the system to be shut down properly in the event of a power failure.

Similar anti-surge devices are recommended for modems in the event of lightning striking phone lines.
Should the disaster prevention controls above fail, a disaster recovery plan ought to be in place. It needs to consider not just how to replace the lost hardware, software and data but how the company will continue until these are recovered.

Where systems are Mission Critical there should be a full back-up system available which will allow the organisation to continue its operations. One UK bank estimated that if their Information Systems failed for just 30 minutes the loss of customer confidence would be so great that it would take them 20 years to win back enough new customers to replace the ones they had lost. As a result of this, that bank has designed a fault tolerant system that, whilst very expensive, virtually guarantees undisrupted processing.
Back-up manual systems are often viable. British Airways have a paper alternative available should their Checking-in system at Heathrow Airport fail. Passengers are asked to check-in at a specific desk, determined by their flight number. At that desk, the flight is represented by a cardboard seating plan of the particular aircraft. A label is peeled off this floor plan as each customer is allocated their seat, thus ensuring no seats are double booked and the plane is not overfilled.

Hardware recovery - stand-by agreements with hardware suppliers are recommended. For a monthly charge they will hold an appropriate server in stock to be used whilst a new server can be bought.

Data and software recovery - back-up software such as ArcServe are commonplace, and available for less than £250. These automatically create back-up tapes at specific points during the day or night so the only staff effort required is to remove the back-up tape from the tape drive and to store it in a safe place away from the computer room.

Off-site storage is also available where the data is backed-up over phone lines to another location. This facility is available on the internet - for instance www.i-FileZone.com offer 10mb of storage space, free of charge.

9.3.6 Technical errors

Faults in either hardware or software will obviously have a significant impact.

Controls
The processes covered in System Design - using methodologies such as SSADM, performing walk-through tests, conducting extensive testing during both design and implementation and so on - are all relevant here as preventative controls.

Once the system is in operation, controls are also needed to ensure the system remains error free. The main emphasis of these controls is to ensure that only valid amendments can be made to software. Staff with the ability to amend software must be carefully recruited and supervised and given access to amend software only when there is a valid reason. The amended software must be thoroughly tested to ensure it operates correctly. A final review should ensure that all of the changes made were actually required and that there weren’t additional changes made for other ulterior motives.

Back up copies of each version of the software must be kept so that when an error is identified a clean version can be quickly recovered.

9.3.7 Human error

No matter how good the system installed and no matter how well maintained it is, if staff are not using correctly it isn’t going to work.

Controls
Selecting and implementing user friendly systems will eliminate many errors as will good training, both during implementation and throughout the systems life.
The system should also have adequate input controls to ensure users are entering data correctly. These should combine a mix of error and exception controls.
• **Error controls**: These identify where data input is clearly wrong and will not be accepted for processing. Examples include:
  
  - *format checks* where an account code must be six characters long to be accepted;
  - *check digits* where stock item codes must match a mathematical pattern recognized by the computer and
  - *existence checks* where codes such as customer codes or account numbers must exist in the appropriate master files.

• **Exception controls**: These identify where input is unusual and so may be wrong. The operator is asked to reconsider the input and confirm if they believe it to be correct. Examples include:
  
  - *deletion checks* - the "Are you sure?" question when deleting files as range checks where chargeable hours would be expected to fall within a certain range and warning messages created if the hours entered were, say, less than three or more than 80 hours in a week.

**9.3.8 Industrial action**

For companies that rely heavily on information systems (see the banking example above) a strike by a few key IT staff can have the same effect on the organisation as an all out strike. Such strikes can also last far longer - the striking employees can be paid either by the remaining employees or by their Trade Union.

**Controls**

These key staff need to be identified and required to sign an employment contract with a No Strike clause. They should be subject to regular appraisal interviews where an assessment should be made as to whether there are any grievances affecting them that might result in the withdrawal of their labour. If these cannot be resolved then replacement staff - often more senior managers - need to be identified and trained.

**9.4 Consequences of the Threats**

Having identified those events that we want to consider in our risk analysis to some extent considering preventative, minimization or recovery activities, we must consider how much to spend on these. We need to estimate the possible loss to the organization if any such event happens.

Some of the events are easier to put a value on than others. For example, if on average you Internet shop is turning over US$60,000 per hour and it is down for 10 minutes you could lose US$10,000. However, is it that simple? If you are selling a unique product that is not available anywhere else then what might happen is that your customers will just have to wait a while before ordering. You may therefore suffer no loss?

On the other hand suppose that your site is regularly down and the product can be purchased elsewhere. Your reputation will be tarnished and not only may customers go elsewhere to satisfy their current requirement but they now stop coming to you for future purchases. You loss may be much more than $10,000?

The risk analysis team need to carefully consider the various scenarios and try to arrive at accurate estimates. There may also be none monetary consequences. In the above example there is no denying that customer service has suffered. Many organization today do have improving customer service as a strategic...
plan and so the risk analysis can show that the event is reducing the effectiveness of the business goals. Another consequence is any legal action or penalty that may be incurred. For example, there may be penalty clauses in a contract. An IT application may be used to monitor progress. Against the contract. If this application provides misleading information or causes deliveries to be late there may be penalties to pay.

Armed with the cost of the event you can now start considering the controls that you want to implement. As we have seen some of the control mechanisms, we will be going in further details regarding controls in the rest of the book. We will not look at them here in detail but it would be during the risk analysis that they would be identified.

9.5 General protective measures

Although many of the measures have been discussed above and many will be described in more detail later on, it is relevant at this point to list a number of measures that organisations should take to protect themselves whenever they build information systems. You can generally suggest these control measures for any situation in exam case studies.

9.5.1 Physical security

Access to hardware should be controlled and restricted to authorised personnel. This will reduce the chances of physical sabotage, accidental damage and hacking.

9.5.2 Protection against remote access

Passwords and user numbers can be used to limit the chances of unauthorised people accessing the system via the public communications network.

9.5.3 Back up procedures

Data should be backed up on a regular and systematic basis. This will enable problems to be recovered with the minimum of trouble.

9.5.4 Strict operating procedures

Imposing strict operating procedures and controls reduces the chances of human error.

9.5.5 Attention to health and safety

All dangers should be eliminated from the working environment by passing cables through ducts and being alert to safety hazards. The danger of RSI and eyestrain will be reduced by the careful ergonomic design of workstations and the use of flicker free visual display units.
9.5.6 Encryption of data

If data is encrypted, the only people who can read the data are those who have the key to the encryption technique. This means that even if an industrial spy were to gain access to a computer system or intercept a communications link, the damage they could do would be limited.

9.5.7 Vigilance

The most dangerous situation is where people become over-confident and blasé. All people in the organisation should be alert to danger at all times.

Practice Questions.

Q no.1) Can you think of any IT systems that would not be critical for an organisation?

Q no.2) Why do you think that we have so many virus and hacker problems today compared with the days of mainframes and mini computers?

Q no.3) How can you place monetary and none monetary measures on a virus attack?

Answer no 1

The solution should consider:

- Is it a trick question? If a system is not critical then should the organisation have wasted money on it! Systems must support the business goals and be needed.
- All systems today are normally critical to the organisation.

Answer no 2

The solution should consider:

- The sheer number of PCs means that a virus can spread rapidly.
- In the early days each system was proprietary and so a virus could not spread to incompatible systems. Now most people use a common operating system or standard protocols.
- Many people have e-mail access and are not security conscious and so can inadvertently spread viruses.
- There are detailed documentation and Internet sites that explain how things work and how to break into them.

Answer no 3

Students should consider:

<table>
<thead>
<tr>
<th>Monetary (assuming time is money)</th>
<th>None-monetary</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT staff time to recover data and files</td>
<td>Reputation of organisation if attack is made public.</td>
</tr>
<tr>
<td>Wasted user staff time while waiting for recovery</td>
<td>Staff moral if they suffer down time</td>
</tr>
<tr>
<td>Time taken to reconstruct any lost data</td>
<td>Restricted activities may impact moral if, say, bans</td>
</tr>
<tr>
<td></td>
<td>are now placed on using e-mail</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>Cost of new virus checking</td>
<td></td>
</tr>
<tr>
<td>software</td>
<td></td>
</tr>
<tr>
<td>Time taken to virus check</td>
<td></td>
</tr>
<tr>
<td>all data in the future.</td>
<td></td>
</tr>
</tbody>
</table>
10 IS Organizational Issues

<table>
<thead>
<tr>
<th>Topic List</th>
<th>Syllabus Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1 Roles and Responsibilities</td>
<td>2.4</td>
</tr>
<tr>
<td>10.2 Structure of an IS department</td>
<td>2.4</td>
</tr>
<tr>
<td>10.3 IS Environment</td>
<td>2.5/2.6</td>
</tr>
</tbody>
</table>

Introduction

The concept of risk analysis has been discussed in the previous chapter. Once risk has been assessed and its consequences have been given a value, a system of internal control can be devised. First step to implement a system of internal control is to establish an organizational structure. In this chapter we will consider those organizational issues that effect the assessment of risk and that require effective implementation of control. We will start by discussing the roles and responsibilities of different people involved in different functions and extend our discussion by identifying how these people interact, in a centralised or decentralised fashion. We will also consider the issues relating to IS department and environment by discussing the control environment and control layers.

Study Guide

Responsibility for control *(Study text reference 10.1 & 10.2)*

Role and responsibilities of key parties

- Auditors are NOT the only people responsible for controls.
- Discuss the fact that it starts at the top and works its way down. Stress the difference between responsibility and operational procedures.
- Explain what the responsibilities are at the different levels.

Layer of control *(Study text reference 10.3)*

- Earlier we discussed that physical access to the equipment was an outer layer of control. We now take the concept of controls as layers further.
- Societal
  - Discuss the students’ view of how society accepts (or doesn’t) crime or criminal acts. Ideally discuss any recent cases that may have appeared in the press.
- Organisational environment
  - Now you need to consider the impact of the organisations that students work in. Discuss both the culture that an organisation may try to promote and the way the managers behave and the example they set.
- Technology infrastructure
  - Discuss physical access to the office and the computer and options available.
  - Discuss how networks are making it easier to bypass physical controls and what may be done about this. Ideally use any recent cases.
### Study guide

**Software**
- Users should only be allowed to run appropriate software and this is normally controlled by logical controls.

**Business process**
- Compare the traditional way of operating with several people in the chain with today’s method

**Control environment (Study text reference 10.3)**

**External regulatory controls**
- Identify what regulations the students think could impact controls. Some examples are given in the text.
- Discuss the issues with the “global” corporation

**Board/audit committee governance**
- Discuss any current standards that may be in the pipeline or recently adopted that may relate to compliance and controls.
- You can visit the web sites of the accounting bodies and consider the impact in Pakistan.

**Management philosophy and operating style**
- You should discuss briefly leadership ideals and the impact on staff. Identify any ethical issues with students.

**Plans/structure of organisation**
- You may wish to use COBIT guidelines in this section since they stress the need for adequate management and planning in the IT area.

**Method to communicate the assignment of authority and responsibility**
- Discuss examples of good and bad communication within organisations that the student may be familiar with.

**Management control methods**
- We keep stressing the controls start at the top and this section continues the theme.
- Appropriate high level plans need to be set for the organisation. You may wish to discuss how well this is done and how they should then flow down to more detailed plans.

**Human resource policies and practices**
- Students may not normally consider these to be part of control procedures. Discuss how HR procedures could impact controls before reviewing the material.

**Financial policies and practices**
- Discuss how budgeting may be used to control expenditure.
- Examine the issues with IT projects and how these can be a drain on financial and human resources. Try to find cases of large project overruns.
- Discuss why IT charge back is not as common as it used to be.
10. IS ORGANIZATIONAL ISSUES

10.1 ROLES AND RESPONSIBILITIES

10.1.1 Information system department

The information systems department within an organisation will have various tasks and responsibilities in relation to the information systems within that organisation. These tasks and responsibilities will tend to be pervasive to the whole organisation, like other service departments such as finance, rather than focusing on one or two small areas.

The main functions of the department, as shown in the diagram below:

1. Information systems manager / director

The IS department will be under the control of the information systems manager or director, who will normally occupy a position on the Board or similar executive decision making body in the organisation.

In his book *Introducing information systems management*, Malcolm Peltu, describes the skills that the IT director should possess. These are:

- good management ability;
- good understanding of how the organisation operates and the organisational activities; and
- good technical expertise in developing and running information systems.

It is easy to see that this range of skills might not always be balanced in an organisation by envisaging where such a person would come from. If the person has a background in management and those skills have been developed, then the first area may be covered. People who make good managers unfortunately do not always have the technical wizardry to have an IT vision for the future, as well as an understanding of the day-to-day computing problems that can crop up. Whilst it may be possible to find a manager with technical ability, it would seem much more difficult to find one that also knew how the organisation operates and all of the activities.

The role of the information director is likely to include the following:
(a) Developing the information systems strategy to tie in with the overall organisational strategy. This aspect of the role covers the purchase and use of the technology to fit with the organisation's goals and objectives.

(b) Ensuring that there is interaction with the environment. This aspect covers:

- information systems' flexibility and connections between other organisations, e.g., electronic data interchange (EDI), shared databases and communications links with customers and suppliers. It also entails looking constantly at the trends in new technology and the new systems enhancements that are being marketed;

- the legal environment of IS, which involves the data protection legislation, trans-border flows of information and systems security matters covered in the Computer Misuse Act 1990;

- the public relations required to convince suppliers, customers and employees of the benefits of the IS.

(c) Responsibility for the information infrastructure, which incorporates the technical and software standards, the establishment of databases and the provision of a systems service function.

(d) Setting up and servicing links between the IS staff and the rest of the organisation. This part of the role involves the provision of technical assistance, informal discussion with users about their needs, discussion with finance and management accounting about the payoff of IS investments.

(e) Participating in a steering committee to oversee the general direction of IS policy and taking decisions on individual IT projects.

2. The role of the steering committee

Because of the size of the investment involved and the importance of key systems to the organisation, many firms are establishing committees to help manage information processing activities.

A steering committee is a collection of members from the various departments within the organisation and is not, therefore, biased toward one particular functional area of the business. The purpose of a steering committee is to decide how to allocate scarce IT resources and to plan for future system developments. Other activities of the steering committee include

(a) ensuring that all the IT activities are in line with the strategic plans of the organisation as a whole

(b) providing leadership at senior level for the exploitation and management of IT

(c) ensuring that resource allocation decisions are effective

(d) co-ordinating requirements in any organisational restructuring

(e) creating the terms of reference for the project teams
monitoring the progress of the various projects.

Some firms establish a corporate level steering committee for information processing whose objective is to review plans and determine the size of the firm's investment in information processing. The corporate committee reviews division plans, organises and approves education about systems, and seeks areas for the development of common systems serving two or more sub-organisations, such as two different companies with common information processing requirements. The purpose of a common system is to avoid the cost of developing a tailored application at each site.

Each division has a local steering committee that is charged with the responsibility of developing and approving long-range plans for information in that sub-organisation. The local committee also reviews and approves short-term plans and the annual budget for information processing activities in the division. This committee serves to review proposals for new systems and to assign priorities to them. Finally, the local committee reviews and approves staffing requirements for information services.

The problems that arise with steering committees are

(a) the experience and skills of the members does not match the purpose of the committee
(b) the level of operation of the committee is wrong, e.g. it is either too high in the organisation or too low, and the discussions that take place are not relevant to the issues that need addressing
(c) having the wrong balance of people on the committee, for example, having those that feel they should be represented rather than those with the actual knowledge required
(d) a failure in the communication process from the committee to the rest of the organisation
(e) meetings become too frequent and this leads to a concentration on tactical matters and a possible loss of commitment from some of the members.

3. Administration

Administration includes the secretarial, accounting and library services associated with the systems department. Department staff will still need secretarial support, for example, to communicate information about changes in information systems to other user departments and to provide standard secretarial functions to managers. The Human Resources department may handle other functions, such as staff recruitment and similar personnel issues, if the organisation is large enough to have one.

Similarly, monitoring actual expenditure compared to budget may be performed by the accounts department, with regular expenditure summarises being provided to the IS department.

Maintaining a library of programmes being used, information about hardware and software issued to staff etc. will be the responsibility of the IS department. It is essential to maintain a record of software issued to ensure that licence agreements are adhered to while basic security of computer equipment means that a database of users and computers issued will have to maintained and updated as each change occurs.

4. Database administrator

One very important administrator is the person in-charge of the databases within the organisation; this is the Database Administrator (or DBA).
The DBA's work can be split into strategic and organisational activities.

(a) **Strategic tasks**
   
   (i) working with strategic management to help define the organisation's present and future needs
   
   (ii) choosing suitable file structures for data storage
   
   (iii) analysing the data required for each application
   
   (iv) preparation of a data model
   
   (v) preparation and maintenance of a data dictionary
   
   (vi) assignment and recording of the ownership of each set of data
   
   (vii) defining hardware needs and planning any changes required
   
   (viii) reconciliation of conflicting information needs.

(b) **Organisational tasks**

   (i) ensuring data integrity by implementing and controlling database procedures
   
   (ii) production of operating manuals
   
   (iii) provision of training for users and applications programmers on a regular basis
   
   (iv) assessing the ongoing performance of the database.

In some organisations the data administrator's job is split into two parts.

A data administrator will be in charge of coordinating, analysing and recording all data items. The tasks will include:

   (a) analysing the data required by each application
   
   (b) the preparation of a data model
   
   (c) the preparation and maintenance of the data dictionary and instructions to users for its use
   
   (d) the recording of the ownership of all the data.

A database administrator will be concerned with the upkeep and maintenance of the actual database itself. The DBA would be responsible for the following:

   (a) database design and structure, including the planning of any changes required
   
   (b) the planning of any hardware changes needed
   
   (c) evaluating proposals to update or upgrade the database
   
   (d) ensuring data integrity by implementing and controlling database procedures
   
   (e) the production of operating manuals
   
   (f) the provision of training for users on a regular basis
   
   (g) assessing the on-going performance of the database.

5. **User support Staff**

The IS department will be providing user support, normally in the form of an information centre or similar system. An information centre would be expected to provide aid and support to people who use computers and to help users develop their own software. It responds to the organisation’s need to control technology by:

   • Establishing hardware standards;
• Approving a range of suppliers of hardware;
• Establishing software, testing and documentation standards;
• Becoming a central point for the release of updated software;
• Ensuring data integrity in the databases;
• Enforcing security procedures e.g., backup and virus checking.

Other services offered by information centres include:

• Training in the use of high-level languages and software development tools.
• Help when searching for reference publications on software, hardware, development methods etc.
• Specific help with identifying the location of data in the corporate database and ensuring that end-users are not using data that is out of date.
• Technical assistance in dealing with particular problems when writing applications in high level programming languages.
• Guidance when purchasing hardware, software, application packages or external support services to maintain compatibility.

Information centre personnel usually act as consultants and trainers to computing users in departments. They will need a wide range of skills as the end users may be varied in the extent of their computer knowledge. The information centre may provide guidance to a manager purchasing personal computers to be used for word processing and give specific technical assistance to a programmer working in an end user department.

Information centres try to keep their staff to a minimum by training end users to carry out any function, which would otherwise cause the numbers of staff in the centre to grow. Take for example a centre that found that it received a large number of calls for assistance from end users when setting up laser printers. The information centre would organise a course on configuring laser printers, run the course at regular intervals and then only accept calls for assistance from staff that had attended the course.

User support will also be supplemented with a Help Desk, to provide assistance on day-to-day problems with computers such as logging on to the network or amending passwords. The Help Desk tends to focus on small, easy-to-solve issues, whereas the Information Centre will be involved with more long-term projects.

User support staff may also include data analysts who are responsible for analysing data within the organisation’s databases and presenting this information to the users in accordance with their specific requirements.

6. System development staff

The IS department will maintain a number of programmers and analysts to design and development new in-house software, or amend off-the-shelf software for specific use within the organisation. In fact, the full range of systems analysis and design may be accommodated within the department including:

• Systems analysis – carrying out a study of existing systems to ensure they are meeting their objectives
• Systems design – designing new systems or amending existing systems to ensure that the system objectives are met
• Systems specification – Designing a new system in detail including producing the full systems specification document
• Systems testing – checking a system works correctly and then implementing that system
• Systems review – continually reviewing systems to ensure objectives continue to be met.

7. **Operational personnel**

With the rise of end-user computing, the responsibility of the IS department for basic processing of data has fallen. Most departments tend to input and process their own data rather than batch input documents and send these to the DP department for input.

One major exception to this rule remains with organisations that collect a significant number of payments in the form of cash or cheques (for example electricity or gas supply organisations or banks in the processing of those cheques). These organisations will still require an extensive data entry department to be able to process the large volume of transactions.

8. **Librarian**

The librarian is required to record, issue, receive and safeguard all program and data files that are maintained on computer tapes and/or disks by an IPE. Depending upon the size of the organization the librarian may be a full-time individual or a member of the data control section who also performs this function. It is an integral part of the overall operations of the IPF.

This is a crucial position. Therefore, many organizations provide additional support for this function through the use of software, which assists in maintaining the inventory as well as manages the movement of the tape reels and cartridges. The use of library control software also helps to maintain version control and configuration management of programs.

9. **Security Administration**

Security administration begins with management’s commitment. Management must understand and procedures to be followed. The duties of the security administrator should be defined in the policy. To provide adequate separation of duties, this individual should be a full-time employee who reports directly to the director of the IPF. However, if it is a small shop it may not be practical to hire an individual for this position. Common sense should prevail. The individual performing the function should ensure that the various users are complying with the corporate security policy and that controls are adequate to prevent unauthorized access to the company assets (including data, programs and equipment). The security administrator’s functions usually include:

• Maintaining access rules to data and other IT resources
• Maintaining security and confidentiality over the issuance and maintenance of authorized users IDs and passwords
• Monitoring security violations and taking corrective action to ensure that adequate security is provided
• Periodically reviewing and evaluating the security policy and suggesting necessary changes to management
• Preparing and monitoring the security awareness program for all employees
• Testing the security architecture to evaluate the security strengths and to detect possible threats
10. Quality Assurance

The quality assurance group usually performs two distinct tasks, namely: quality assurance (QA) and quality control (QC).

- Quality assurance helps the IS department to ensure that the personnel are following prescribed quality processes. For example; QA will help to ensure that programs and documentation adhere to the standards and naming conventions.

- Quality control is responsible for conducting tests or reviews to verify and ensure that the software is free from defects and meets user expectations. This could be done at various stages of the development of an application system, but it must be done before the programs are moved into production.

The quality group also can assist by periodically checking the accuracy and authenticity of the input, processing and output of various applications. In enable this group to play an effective role it should be independent. In some organizations this groups may be a part of the control group but under no circumstances should it be a function of programming staff.

10.1.2 IS Department and Responsibilities of User Departments

1. Transaction Authorization

Transaction authorization is the responsibility of the user department. Authorization is delegated to the degree that it relates to the particular level of responsibility of the authorized individual in the department. Periodic checks must be performed by both management and audit to detect the unauthorized entry of transactions.

2. Reconciliation

Reconciliation is ultimately the responsibility of the user. In some organizations, limited reconciliation of applications may be performed by the data control group with the use of control totals and balancing sheets. This type of independent verification increases the level of confidence that the application ran successfully and that the data are in proper balance.

3. Custody of Assets

Custody of corporate assets must be determined and assigned appropriately. The data owner is usually assigned to a particular user department and duties should be specific and written. The owner of the data has responsibility for determining authorization levels required to provide adequate security, while the data security administration group is often responsible for implementing and enforcing the security system.

4. Access to Data

Control over access to data are provided by a combination of physical, system and application security in both the user area and the IPF. The physical environment must be secured to prevent unauthorized personnel from accessing the various tangible devices connected to the central processing unit and thereby permitting access to data. System and application securities are additional layers of security that may prevent unauthorized individuals from gaining access to corporate data. Access to data from external connections is a growing concern since the advent of the Internet. Therefore, IS management has added responsibilities to protect information assets.

5. Authorization Forms

Managers of user departments must provide IS with formal authorization forms (either hard copy or electronic) that define the access rights of their employees. In other words managers must define who should have access to what. Authorization forms must be properly evidenced with management approval. Generally, all users should be authorized specific system accessories written request of management. In
large companies or in those with remote sites, signature authorization logs should be maintained and written requests should be compared to the signature log. Access privileges should be periodically reviewed to ensure that they are current and appropriate to the user’s job functions.

6. **User Authorization Tables**
The IS department should use the data from the authorization forms to build and maintain user authorization tables. These will define who is authorized to update, modify, delete and or view data. These privileges are provided at the system, transaction or field level. In effect these are user access control lists. These authorization tables must be secured against unauthorized access by additional password protection or data encryption. A control logs should record all user activity, and appropriate management should review this log. All exception items should be investigated.

7. **Exception Reporting**
Exception reporting should be handled at the supervisory level and require evidence, such as initials on a report noting that the exception has been properly handled. Management also should ensure that exceptions are resolved in a timely manner.

10.2 **Structure of an IS Department**

The IS department can be maintained in one central location within an organisation, or alternatively, spread out within the organisation. As you would expect, the decision to centralise or decentralise has various advantages and disadvantages, which the individual organisation will have to evaluate before making a decision on the structure of the department.

10.2.1 **Reasons for decentralising**

The main reason for decentralising at least part of the IS department, is to provide a more local service. However, care must be taken in deciding which sections of the department to decentralise as this may otherwise result in un-necessary duplication of work.

Some of the reasons for decentralising the IS function are discussed below.

- **Size** - the process of decentralisation breaks an IS department up into more manageable units, this enables decision-making to proceed quickly and effectively and, in theory, a closer control to be maintained on the day to day running of each section of department’s activities.

- **Need for specialists** - as a business grows the nature of its activities often becomes more complex so that each department has to rely on experts to provide appropriate support for that particular segment of the business. For example, a department providing services to customers may require a higher level of (and be prepared to pay for) a higher level of IT support than an internal service department.

- **Motivation** - if managers are made to feel responsible for a particular part of a department then it is generally found that their efforts within that part of the business are improved and, therefore the business prospers.

- **Uncertainty** - with ever-changing market conditions, decisions cannot be pre-planned or centrally planned. It is important to have local managers who are closer in touch with each particular part of the business environment to be in a position to respond quickly as problems arise. Decentralising the IS department means that changes can be made more quickly to respond to the individual needs of each user department.

- **Geographical** - decentralization often refers to the delegation of responsibilities at a single location, an office or a factory; however, it is important for an IS department to get close to different
departments in those far-flung locations. On-site support can be a lot more effective than trying to mend a computer by telephone, for example.

**Fiscal** – providing a decentralised structure enables user departments to be able to decide on the level of expenditure that they are prepared to make for the service being provided. Placing money into a central resource may not appear to provide any additional tangible benefit, whereas hiring additional staff to work only in one department has an immediate and obvious benefit of more IS staff available within the department.

**Training** – training can be focused onto the requirements of the individual department, rather than generic training courses being produced for the whole organisation.

### 10.2.2 Reasons for Centralisation

Some of the reasons for retaining a central IS department are:

a. **There is a requirement for only one set of files.** Everyone in the organisation uses the same data, which is readily accessible in a standard format.

b. **Economies of scale.** It may be advantageous to acquire one large computer, with greater processing capabilities, rather than several small computers. Centralisation of personnel may also remove unnecessary duplication of activity and allow for regulation and control of analysis and programming functions. It is necessary, however, to balance the cost element against the benefits derived by users (the latter may be greater with decentralisation).

c. **Staff shortages/turnover.** Centralisation mitigates the effect of both, so that individuals are less indispensable; they can also be provided with greater scope in their working experience. Fewer employees may be needed so higher quality staff and specialists may be affordable.

d. **Ease of control.** Senior management is better placed to control operating functions, particularly when a standard reporting system is being utilised.

### 10.3 IS Environment

Organizations do not exist in a vacuum. When considering the implementation of controls there are many factors that have to be considered. There are the external influences such as regulatory controls and the internal influences such as the polices and procedures that the organization follows. In this section we will discuss how these influence controls. We can divide the environmental influences in factors effecting the environment like external factors and Layers like public or societal layer.

#### 10.3.1 Layers of Control

It is possible to view controls and security procedures as acting in layers. For example when considering physical security the outer layer would be the controls and procedures to be followed to enter the building. Then there is the specific security to access a computer such as a locked office. Next layer is the access to the PC which could be controlled by a key or card system. The inter layer is the logical password protection.

In the same way we can consider the approach and attitude to controls as consisting of layers.
1. **Societal layer**

The outer or direst layer can be thought of as the attitude that society has to laws and regulations and the culture and upbringing of individuals. For example, in some countries blatant copying of software is commonplace and authorities do not appear to clamp down on it. Students often feel that it is acceptable to copy a friend’s software and are encouraged by that peer group to share software.

If that attitude prevails in society then when an individual works in an organization they may follow a more cavalier approach to security and control.

This may be an important issue for auditors that work for international organization. They may find that what is expected and accepted in one country will be rejected in another.

2. **Organizational environment layer**

At the next level is the culture that the organization tries to impart on its employees. Some organizations such as banks are very security conscious and find it easier to implement control processes because the staff expect high levels of control. Others, especially smaller organization find that it can be difficult to get staff to log on and not share passwords because they have a friendly, trusting culture.

In addition, just as parents influence their children, the directors can set the tone for the organization. For example, if it is known that senior management condone shady practices such as false advertising over charging, failure to pay, etc, then staff will not be inclined to act honestly themselves.

3. **Technology infrastructure layer**

No matter what an individual’s attitude may be to security and control they have to be able to get through this layer, which controls the way they access the hardware and IT facilitates.

There is of course the physical security that surrounds the office itself. If that is strict then the controls over hardware can assume that only an authorized person has access. If it is non-existent to there is the possibility the equipment may be stoke then there may be a need for controls over the hardware itself.

As discussed earlier we would expect to see servers and other critical equipment in a secure area but desktop computers may be vulnerable. It is possible to secure these with physical locks so that they cannot be powered on. Alternatively card readers may be incorporated in the hardware so that the logon process requires a user to swipe a card and enter associated pin hardware so that the logon process requires a user to swipe a card and enter an associated pin.

With the increased use of networks and the Internet, a perpetrator may not need to have office access since they can make use of modem connection to get to the organization’s data. Thus network security becomes extremely important. Even major organization like Microsoft have been the target of backers and have seen their networks penetrated.

Of course not all organizations will attract backers but since so many seem to attack sites just for fun no organization can feel safe.

Network security devices were discussed in Module D and this is where organization would need to consider devices such as firewalls and techniques such as data encryption.
4. **Software layer**
Once past the hardware layer you get to the software and applications itself. Access is normally controlled by the use of permissions. The simple philosophy is that only authorized users should be given permissions in the first place and these permission should be just enough to allow them to do their job.

The problem is that this normally require quite a bit a work to set up and maintain. Also you may find that during holiday periods or if staff are absent, some users need to be granted additional access to cover for colleagues. In many sites it is so easy to just give all staff all permissions and so keep them out of the administrator/s hair. Logical controls and permission were discussed in module D. Consider also the developments in biometrics access control eg fingerprints, retina scanning and the impact that these might have on securing various layers.

5. **Business process layer**
We must not forget that the business process themselves may also form one of the layers of control. We all know about the concept of segregation of duties and management supervisor.

If a process requires someone else to continue working with data that one user has created then there is a chance that any errors will come to light. If a manager is checking a subordinate’s work then mistakes or fraudulent transaction may be spotted.

It is important to be able to identify those parts of a transaction that do rely on one person only and unfortunately these are becoming more common.

Traditionally data went through several processes that were handled by different people. This itself was an element of control and was known as segregation of duties. The basic flow was summarized as in the table below.

<table>
<thead>
<tr>
<th>Action</th>
<th>Carried out by</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collate input documents</td>
<td>User – clerk</td>
</tr>
<tr>
<td>Enter documents to computer</td>
<td>Data entry operator</td>
</tr>
<tr>
<td>Verify processing completed</td>
<td>Data operations clerk</td>
</tr>
<tr>
<td>Check controls</td>
<td>Data controller</td>
</tr>
<tr>
<td>Use results of processing</td>
<td>User – manager</td>
</tr>
<tr>
<td>to control assets</td>
<td></td>
</tr>
</tbody>
</table>

One of the most important elements of this control was the separation of the physical control of assets and the recording of asset.

With today’s online systems and the removal of clerks from the chain of operation we no see senior managers controlling assets and performing the record keeping on the computer. In extreme cases that same person may even develop a database or spreadsheet application to record the data.

10.3.2 **Control Environment**

1. **External regulatory controls**

There are few countries in the world that do not have legislation that governs the way commercial organizations are to operate. Most of the regulations are concerned with ensuring that the people that run the company have a duty of care to the people that own the company. Different Acts and Regulations
Tin particular, there is a need for adequate record keeping. Correct books of account must be maintained and the very existence of these is, to a certain extent, control in its own right. However in this module we have been looking at control techniques to ensure that these books are accurate, reliable and complete.

Of course one of the other reasons that the books must be accurate is so the government can accurately assess an organization’s liability to taxations.

As business becomes more global then we do see similar laws and regulations being enacted around the planet. This is particularly important as we see the growth of the multi-national corporation, some of which have a turnover greater than some small countries.

The organization will now be subject to privacy and copyright rules in its own country and in those countries that it operates in. Senior management will need to be aware of the environment in which they work and ensure that their systems of controls are sufficient to meet the rules of the country in which the operate.

Following regulations are of interest that an information system auditor may find relevant:

I. THE DATA PROTECTION ACT 1998

Introduction

The Data Protection Act initially was introduced into UK law in 1984 for two major reasons:

(a) To counteract the threat to privacy caused by the increased ability of computers to hold, transfer and process personal data

(b) To enable the UK to meet its obligations to ratify the Council of Europe Data Protection Convention. When fully operational this convention will enable the countries that have signed it to refuse to allow data to be transferred to other countries that do not have equivalent data protection laws.

The Act was amended in 1998, the new Act becoming law in the middle of 1999.

One feature of the amended Act is that the transfer of personal data outside the EU is restricted. Personal data may only be transferred outside the EU if the other country has a similar level of data protection law. This appears to rule out data transfers to the US, where the authorities promote industry self-regulation as an alternative to national data protection legislation. The 1998 Act defines the transfer of data in this regard as simply making it possible to transfer personal data, so a terminal connection from the USA to a site in the UK could be illegal. This law could cause serious disruption in business practices internationally.

Another feature of the current Act is that it gives more powers to individuals whose details are being held, for example the individual's explicit consent is required when processing sensitive data such as racial origin, criminal convictions or political opinions.

The Data Protection Principles

The Act establishes eight general principles or standards to be observed by data users and bureaux. Failure to comply with these principles can result in seizure of data and unlimited fines. The Secretary of State has the power to amend the principles.

Personal data held by users
(1) The information to be contained in personal data shall be obtained, and personal data shall be processed, fairly and lawfully.

(2) Personal data held shall be held only for one or more specified and lawful purposes.

(3) Personal data held for any purpose or purposes shall not be used or disclosed in any manner incompatible with that purpose or those purposes.

(4) Personal data held for any purpose or purposes shall be adequate, relevant and not excessive in relation to that purpose or those purposes.

(5) Personal data shall be accurate and, where necessary, kept up to date.

(6) Personal data held for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

(7) An individual shall be entitled:

(a) at reasonable intervals and without undue delay or expense:

(i) to be informed by any data user whether he holds personal data of which that individual is the subject; and

(ii) to access to any such data held by a data user; and

(b) to have such data corrected or erased, where appropriate,

(8) Appropriate security measures shall be taken against unauthorised access to, or alteration, disclosure or destruction of, personal data and against accidental loss or destruction of personal data.

II. THE COMPUTER MISUSE ACT 1990

Introduction

Until the introduction of the Computer Misuse Act in 1990, two highly damaging activities were not against the law. These were hacking and the deliberate infection of computer systems with viruses. Although an offended organisation could use the civil courts, there was no effective protection against these two acts.

Hacking

Hacking is the gaining of unauthorised access to a computer system. It may form part of a criminal activity or it may be a hobby, with hackers acting alone or passing information to one another. Hacking is often a harmless activity, with participants enjoying the challenge of breaking part of a system's defences, but severe damage can be caused.

Viruses

A virus is a piece of software that seeks to infest a computer system, hiding and automatically spreading to other systems if given the opportunity. Most computer viruses have three functions - avoiding detection, reproducing themselves and causing damage. The damage caused may be relatively harmless and amusing
('Cascade' causes letters to 'fall' off a screen), but are more often severely damaging. In recent years two viruses in particular ('Melissa' and 'I Love You') were spread by email address books around the world within a very short time, and inflicted considerable damage to systems, and the businesses that depended on them.

'Hackers' and 'viruses' are examined in greater depth in chapter 4 of this book.

The criminal offences created by the Act

This act was designed to outlaw hacking, the introduction of viruses and the unauthorised copying of data. Three new offences were created by the Act:

(a) Unauthorised access (hacking)

It has become illegal to gain access or to attempt to gain access to a computer system without authorisation. It is not necessary to succeed in gaining access to be guilty of this crime. The maximum penalty is up to six months in prison and/or an equivalent level of fine (£2000).

(b) Unauthorised access with intent to commit another offence

The maximum penalties for this crime are significantly greater than for unauthorised access alone:

- on summary conviction an offender is liable for up to six months in prison and/or an equivalent fine
- on conviction or indictment an offender may be imprisoned for up to five years and/or an unlimited fine

(c) Unauthorised modification of data or programs (introduction of viruses and computer sabotage)

A person is guilty under this offence if the intention is to prevent or hinder access to any program or data or to compromise the reliability of data or programs.

The penalties for this crime are the same as for the crime of unauthorised access with intent to commit another offence.

III. COPYRIGHT LAW

Introduction

Copyright in general terms is the right to publish, reproduce and sell the matter and form of a literary, musical, dramatic or artistic work. The owner of the copyright can therefore sell the item that the copyright relates to, and can stop other people from selling the same work because they are breaching the copyright obtained by the original author.

Within the UK, the Copyright, Designs & Patents Act of 1988 provides the same protection to the authors of computer software as it does to literary, dramatic and musical works. However, selling software is
slightly different to selling a book or painting, for example. When computer software is sold, it is not sold outright to the purchaser. Instead, the purchaser is granted a right to use that software as explained in the user licence. This normally means that only one person at a time can use the software, and that making of copies of the software is limited to backup purposes only. The purchaser cannot therefore simply copy the software onto another CD or floppy disk, as this would breach the copyright.

Most software suppliers allow more than one person to use one copy of the software, where, for example, the software is loaded onto a network server, and a licence to use multiple copies of the software has been purchased.

Some software can be copied legally; this is **shareware**. The software can be loaded onto a computer and tested; however, it the user decides to keep the software then a royalty payment is due to the author. **Freeware** is software that can be copied and used without charge, although the software author retains the copyright to that software. Finally, **public domain software** is freely available and sharable software that is not copyrighted.

Anyone convicted of an offence under this Act can expect a fine of unlimited amount plus a prison sentence of up to two years.
Software contracts – ‘off-the-shelf’ software

Software contracts can be in respect of either packages or bespoke software. The contracts governing most packages are standard. As explained above, users are normally licensed to use a copy or copies of the software; they do not own the software as such and the licence can be withdrawn if the contract is breached.

The important terms found in package software contracts govern the user’s rights of use and limit the software vendor’s liability.

A typical licence agreement is reproduced below:

Software Licence Agreement

1. WHAT THIS IS. This sheet contains the Software Agreement (the 'Agreement'), which will govern your use of the ABC Company software package 'XXXXX'.

YOU AGREE TO THE TERMS OF THIS AGREEMENT BY THE ACT OF ORDERING OR RUNNING OR INSTALLING THE SOFTWARE.

2. GRANT OF LICENCE. On acceptance of your order, ABC Company will grant you, and you will accept, a limited licence to use the ordered software, user instructions, and any related materials (collectively called the 'Software' in this Agreement). You may use one copy of the software. If installed on a network, only one user may use the software at any time.

You may not transfer or sublicense, either temporarily or permanently, your rights to use the Software under this Agreement without the prior written consent of ABC Company.

3. TERM. This Agreement is effective from the day you receive the Software and continues until you return the original magnetic media to ABC Company. You must also certify in writing that you have destroyed any copies you may have recorded on any memory system or magnetic medium.

4. ABC COMPANY'S RIGHTS. You acknowledge that the Software is the sole and exclusive property of ABC Company. By accepting this Agreement, you do not become the owner of the Software, but you do have the right to use the Software in accordance with this Agreement. You agree to use your best efforts and all reasonable steps to protect the Software from unauthorised use, illegal reproduction, or illicit distribution.

5. YOUR ORIGINAL DISKETTE/HARD DISC COPY. You may use the original diskette to make a hard disk copy for the purpose of running the Software program. You should not use the original diskettes when running the Software program. After making a hard disc copy place the original diskette in a safe place. Other than the authorised hard disk copy, you agree that no other copies of the Software will be made.

6. LIMITED WARRANTY. ABC Company warrants for a period of ninety (90) days from the effective date of this Agreement that, under normal use, and in accordance with the installation instructions, the magnetic diskette will not prove defective, that the program is properly recorded on the diskette and that the accompanying instructions are substantially complete and contain all the information which ABC Company deems necessary for the use
of the program. If, during the ninety day period, a defect in the Software should appear, you may return the software to ABC Company for replacement without charge. Your sole right with respect to a defect in the Software is replacement of the Software.

EXCEPT FOR THE LIMITED WARRANTY DESCRIBED IN THIS PARAGRAPH, THERE ARE NO WARRANTIES, EITHER EXPRESSED OR IMPLIED, BY THIS AGREEMENT. THESE INCLUDE, BUT ARE NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, AND ALL SUCH WARRANTIES ARE EXPRESSLY DISCLAIMED.

7. LIABILITY. You agree that regardless of the form of any claim you may have, ABC Company's liability for any damages to you or to any other party shall not exceed the license fee paid for the Software.

ABC COMPANY WILL NOT BE RESPONSIBLE FOR ANY DIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, SUCH AS, BUT NOT LIMITED TO, LOSS OF PROFITS RESULTING FROM THE USE OF THE SOFTWARE OR ARISING OUT OF ANY BREACH OF THE WARRANTY, EVEN IF ABC COMPANY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

8. TERMINATION OF AGREEMENT. If any of the terms and conditions of this Agreement are broken ABC Company has the right to terminate the Agreement and demand that you return the Software to ABC Company. At that time you must also certify in writing that you have not retained any copies of the Software.

9. GOVERNING LAW. This Agreement is to be governed by, and interpreted in accordance with the law of England.

V. Software contracts - Bespoke software

The user should have more say when negotiating for bespoke programs to be written. Of particular importance will be who owns the copyright to the program and the source code. Unless otherwise stated, the law will assume that the software writer will own these. The full list of matters that should be addressed is as follows:

- Precise description and specification of the software.
- Performance warranties (that it will operate with certain response times)
- Price
- Terms of payment
- Dates for completion
- Acceptance tests and period for acceptance
- Penalties for late delivery and poor performance
- Conditions of use
- Ownership of copyright
- Ownership of source code
- Documentation
• Training
• Warranties
• After sales service and levels of support
• Protection against copyright infringement
• Confidentiality (client's business matters)

All these items will be included in an agreement to write the software, prior to that writing being commenced.

2. **Board/audit committee governance**

In most major countries the various accounting bodies have had a large part to play in drafting the regulations and standards under which organizations should operate. There are large accounting practices that are represented in most countries and partners from these firms are often co-opted onto committees and working parties that set standards.

In addition there are international organizations such as IFAC (International Federation of Accountants promoting worldwide acceptance of common standards and guidelines. Qualified accountants around the world are encouraged to follow international standards especially if there are no local pronouncements.

IFAC has published papers that discuss IT controls and audit and some of their recommendations are described in this module. They stress that IT controls and security are the responsibility of management and that responsibility starts at the board level.

It is the responsibility of senior management to comply with regulations and their fiduciary obligations and most are aware of that. But there is also a need to be involved in IT governance and system reliability. This may be achieved by direct involvement or through the use of various audit committees.

3. **Management philosophy and operating style**

Management set the standards for other staff to follow. Many management theories show the manager as a leader, someone who influences staff by their own behaviour.

In accountancy, ethics is seen as an important quality to possess. This is true of managers and one would expect them to be people of integrity and to observe ethical values.

Managers should lead by example, and they cannot expect their staff to behave ethically and adhere to security and control procedures if the manager does not act in the same way.
4. **Plans/structure of organization**

COBIT has a high-level control objective that evaluates the organization and the management of the IT department. There are two issues to be considered here:

1. how the IT department is perceived by other managers and the relationship it has at the board level
2. the leadership and management of the IT department

In most organizations IT is an essential service and any loss could be critical. The manager of IT should be able to develop a rapport and gain the respect of peers in order to be able to explain IT requirements and the need for control. Only then will adequate funding and resources be made available. The IT manager needs to be a leader to the staff in the department and also able to build relationships with user departments. In today’s environment the manager has to be capable of developing business relationships with third parties such as vendors and customers.

As it becomes all pervasive it is essential to control the boundaries of responsibility both to encourage ownership of systems and resources but also to maintain segregation of roles. The use of segregation of roles as a control has been discussed already.

5. **Method to communicate the assignment of authority and responsibility**

Many people complain that ‘management never tell them anything’. Management text books extol the need for good communication between parties.

It is no point developing policies, procedures and best practices if staff are not made aware of them. Not only that but there needs to be way of regularly checking that they are adhered to.

6. **Management control methods**

COBIT sees management control as an important element in the whole system of internal control. Management not only set an example in the way they operate and perform but they must be actively involved in the whole planning process.

They must see IT as part of the organization’s long and short term plans. This implies that the organization has a strategic plan in the first place?

Once the organization has an agreed upon direction, management can work to develop the IT plans to ensure integration with business goals. From this will flow technology, architecture, data and system plans?

Then the budget can be set. Restricting the amount of money you can spend can be a way of controlling expenditure but, without careful planning and monitoring, funds can still be wasted. Indeed budgetary cut backs are often blamed for not implementing controls.
7. **Human resources policies and practices**

People work effectively when they:

- do a job that they enjoy
- respect and believe in their managers
- are challenged in their work
- can see the value of what they are doing
- feel that they are being treated fairly

To a certain extent, people will adhere to controls only if they feel that there is a reason for them. If they get in the way of doing work then they will find workarounds. If staff feel cheated or see managers behaving un-ethically then they will do the same. Thus one can consider the HR policies and procedures as an important element of control. Following are general components of any HR policy, however in practice HR policies vary greatly in contents and complexity.

I. **Hiring:**

An organization’s hiring practices are impertinent to ensure that the most effective and efficient staff is chosen and company is in compliance with the legal recruitment requirement. Theses would include:

- Background checks
- Confidentiality agreements
- Employees bonding to protect against losses due to theft
- Conflicts of interest agreements
- None compete agreements.

Control risks are:

- Staff may not be suitable for the position they are recruited to fill.
- Reference checks are not carried out.
- Temporary staff and third party contractors may introduce uncontrolled risks.

II. **Employee Handbook:**

Employee handbooks, distributed to all employees upon hire, should explain items such as:

- Security policies and procedures
- Company expectations
- Employee benefits
- Holiday policies
- Overtime rules
- Outside employment
• Performance evaluations
• Emergency procedures
• Disciplinary actions for:

1. Excessive absence
2. Breach of confidentiality and/or security
3. Non-compliance with policies.

In general there should be a published code of conduct for origination that specifies all employees’ responsibilities to the company.

III. Promotion Policies:

Promotion policies should be fair and understood by the employees. Policies should be based on the objective criteria and consider an individual performance, education, experience, and level of responsibility.

The IS auditor should ensure that the IS organization has well defined policies and procedures for promotion and is adhering to them.

IV. Training:

Training should be provided on the fair and regular basis to all employees. This is particularly important for IS professionals given the rapid rate of technology and procedures. Training not only assures efficient and effective use of IS resources but also strengthens employee morale. Training must be provided when a new software or hardware is being implemented, training should include relevant management training, project management and technical training.

Cross training is having more than one individual properly trained to perform a specific job or procedure. This practice has the advantage of decreasing dependence on one employee and can be part of succession planning. It also provides the backup for the personnel in the event of absence for any reason and thereby provides for continuity of operations. However, in using this approach it would be prudent to have first assessed the risks of any one person knowing all parts of a system and what exposure(s) this may cause.

V. Scheduling and Time Reporting:

Proper scheduling provides for a more efficient operations and use of computing resources. Time reporting allows management to monitor the scheduling process. Management can than determine if staffing is adequate and if the operation is running efficiently. It is important that the information being entered and recorded into such a system is accurate.

VI. Employee Performance Evaluation:
Employee assessment must be a standard and regular feature for all IS staff. The human resources department should ensure that the IS managers and IS employees are set mutually agreed goals/expected results. Assessment can only be against theses if the process is objective and neutral.

Salary increments, performance bonuses and promotions should be based on performance. The same process can also allow the organization to gauge employee aspirations and satisfaction and to identify problems.

VII. Required Vacation:
A required vacation ensures that once a year, at a minimum, someone other than the regular employee will perform a job function. This reduces the opportunity to commit improper or illegal acts. During this time it may be possible to discover fraudulent activity as long as there had been no collusion between employees to cover possible discrepancies.

Job rotation provides an additional control, since the same individual does not perform, the same tasks all the time. This provides an opportunity for an individual other than the regularly assigned person to perform the job and notice possible irregularities.

VIII. Termination Policies:
Written termination policies should be established to provide clearly defined steps for employee separation. It is important that policies be structured to provide adequate protection for the organization’s computer assets and data. Termination practices should address:

- Voluntary termination
- Immediate termination
- Return of all access keys, ID cards and badges to prevent easy physical access.
- Deletion of assigned logon ID and passwords to prohibit system access.
- Notification to other staff and facilities security to increase awareness of the terminated employees status.
- Arrangement of the final pay routines to remove the employee from active payroll files.
- Performance of a termination interview to gather insight on the employee’s perception of management.
- Return of all company property
- Escort from premises.

Controls are designed to find errors before they enter the system. One way of improving the error rate is to ensure that staff is appropriately trained. In many cases staff receive no training on a new system and have to pick it up as they go. No wonder error rates are high.
8. **Financial policies and practices**

IT can consume a lot of funds. COBIT control objectives include the management of the IT investment.

Control starts with the setting of the budget. While a full description of the budgeting process is outside the scope of this module it is essential that an appropriate budgeting process is undertaken.

This should be integrated with the organization’s long term and short term planning. As we discussed, the organization should have a good idea of what it wants from the IT area. There may be a need to distinguish between operational costs and project or development costs. The former should be easier to estimate and will cover the running costs of the department.

Projects should be linked to the strategic plans and be shown to support organization goals. In some organizations the cost of projects is funded by the user department that will benefit most or is sponsoring the project. This is a good way to fund a project since it should mean that:

- the user department ‘buys in’ to the project and will support it
- the budget can be used as a control mechanism to monitor progress
- any changes requested can be costed and the user department can decide whether to fund any additional costs. Often if a budget is centralized, users will not think twice when asking for changes since they are not paying for them.
- The benefits will normally occur in the user department and it can be clearer to see the cost benefit relationship

Several years ago it was common for IT departments to institute a system of charge-back to users. This was seen as a way of controlling the cost of the IT department and ensuring that scarce resources were used effectively.

This practice is not as widespread today especially with the use of PCs and networks. The philosophy though still has value and making people pay for the resources that they use will often make them look for more effective ways to operate.

**Practise Questions**

Q no 1) Give examples of socially accepted behaviour that may actually be illegal

Q no 2) Assume that an organization’s security policies state that passwords should not be revealed to others. You discover that a senior manager has told an administrative assistant what their user id and password is so that the assistant can log on as the manager and check the manager’s e-mail. Describe how you would handle this situation.

Q no 3) One of the advantages of IT is to improve productivity by removing the separate operations and staff that were involved in data processing. This means that the control process afforded by segregation of duties also disappears. What can be put in its place?

Q no 4) You are introducing a new financial system to users and will be running training sessions. One of the sections is on security; list the topics you would expect to see in this section.

Q no 5) Describe how managers could use IT to act unethically or without integrity.
Q no 6) What would be an effective way to communicate?
1. a new e-mail policy
2. stricter control over password and user identifier sharing

Q no 7) An organisation is impacted by budget cuts and they decide not to install a fault tolerant system to save money. What should they have considered before making such a decision?
Suggested Solutions

**Answer No 1.**
The solution will vary but in most countries the general public accepts the following:
- Speeding a little over the limit.
- Recording television programs for later viewing or sharing with friends.
- Copying software for use on more than one computer.
- Recording music from a friend’s CD.
- Taking office supplies.

**Answer No 2**
The solution should consider:
- Risks faced but we could assume a senior manager has access to confidential data.
- Whether the AA would normally be able to see the same information as the manager and do they have similar access.
- Assuming the AA now has greater access than they should, this is a weakness.
- Also manager is not setting a good example to others.
- Manager should be trained so they can get mail or if it is acceptable for AA to get mail, the AA should be given the appropriate access to get the manager’s mail.

**Answer No 3.**
The solution should discuss:
- Should balance the need for productivity and security.
- Logging of user actions can be an effective control.
- Computer controls must be tighter such as over-ride controls.
- Management review becomes more important.
- Control over assets and recording of assets should be separated.

**Answer No 4.**
The solution should discuss:
- How users will log on to the system.
- Levels of authority.
- What users can access and what will be restricted.
- Any over-ride facilities.
- Typical security messages that may occur.
- Security indicators that users should look out for.

**Answer No 5.**
In the solution we would expect to see:
- Using logs to check on how much staff have been working.
- Obtaining data about friends and relatives that they should not have access to.
- Finding personal information about colleagues.
- Deleting incriminating evidence such as e-mails.
- Falsifying figures by editing data directly.

**Answer No 6.**
In solution the student should:
- Distinguish when face-to-face communication is preferred to written communication.
- All policies should be written down but they need to be communicated effectively rather than just added to the procedures manual.
- Policies may be sent out by e-mail or in meetings.
- Some polices may require a signed response. For example an employee may be required to sign a document stating that they understand the policy and its impact on them.

**Answer No 7.**
In this solution we should see:
- Reference to the risk analysis (which is covered in more detail in the next section).
- Why are there budget costs? Have the long-term plans been changed?
- Was a FT system part of the IT plan originally? Were there strategic reasons for FT as part of improved services internally or to customers?
- Management may decide to run the risk but should only do so once they have considered all issues.

**Answer No 8.**
In the solution the student should consider:
- Why the employee is disgruntled in the first place. If they feel cheated then they may cheat the organisation.
- The employee may work to rule or even sabotage the system.
- The employee may be planning to leave and may copy confidential files.
- The employee may try to break into restricted areas.
- The employee may no longer concentrate and so have a higher error rate.
- In extreme cases, disgruntled employees have caused bodily harm to others.

**Answer No 9.**
The solution should consider:
- Is there still a good business case for the project? That is, does it show a cost benefit?
- Why are there overruns? Have more requirements been added or was it poor estimating in the first place?
- What are the estimates for the remainder of the project? How reliable are they?
- What will be lost if project is abandoned now?
- Where will the extra funds come from?
11 Control Activities I

<table>
<thead>
<tr>
<th>Topic List</th>
<th>Syllabus Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1 Control design</td>
<td>2.8</td>
</tr>
<tr>
<td>11.2 Control Procedures</td>
<td>2.8</td>
</tr>
</tbody>
</table>

Introduction

We have discussed some controls in the context of risk analysis. In this chapter we will discuss in detail what are the control activities undertaken by the management to encounter a specific risk. Control activities consist of designing and implementation of system of controls over the activities of information system.

Study Guide

Control activities
- This is one of the biggest sections to cover. A lot of detail of controls and associated technologies will be found in the textbook.
- You may find that students without a good IT background may not be aware of the technology issues that require a control. You may therefore need to discuss appropriate technology issues.

Control design (11.1)
- Explain that many controls can be implemented as polices and procedures. In some cases the control relies on an individual carrying out a process and this may be difficult to confirm.
- It can be useful to summarise the top down approach to controls and responsibilities.
- Each textbook may define and group controls differently. Discuss some of the options.

Control procedures (11.2 &)
- Discuss the fact that control principles stay the same; it is just the technology that changes.
- You can point out that with automatic approval systems, anyone who logs on as a manager can approve funds as if they were that manager. This is why safeguarding user ids and passwords are so important.
- Discuss the different levels of access that various operating systems may allow and how a user authorisation matrix may be used to help plan access.
- You may want to discuss the new problems that organisations will now face with on-line transactions. These can be easily lost.
- You should discuss the fact that real-time systems can still generate exceptions and errors and that there should be an adequate way of capturing these and following them through.
Study Guide

- The example discussed in the text about over or undercharging is another demonstration of how individuals or organisations can deal un-ethically.
- You may wish to discuss any developments in privacy legislation and the importance of looking at legislation in other countries.
- Students may want to consider what sort of information about themselves that they would not want to be made freely available. Ask if any have had un-solicited e-mails or other correspondence and questioned how organisations got their address.
- Discuss the need for data classification that can help develop the appropriate control techniques.
- You should discuss the basic control principles and ask students what could happen if controls are too restrictive.
- You should get examples of the physical controls that students may have experienced at various sites.
- Discuss why most organisations only use the User Id and password access method and have not embraced physical devices such as cards to restrict access to PCs.
- Explain that even though operating system permissions can control access to files it is possible for database system to have other access controls.
- Discuss the fact that we are now seeing increasing numbers of attacks against popular operating systems.
- Discuss the issues with application software. You could lead the students through the main security issues with typical financial systems and even get software for a demonstration.
- An increasingly important control is the monitoring of activity. Discuss why this is required and how it should be implemented.
- Discuss the ethics of other forms of monitoring employees. How would students react if they were being monitored constantly?
11. Control Activities I

11.1 Control Design

Many controls are relatively cheap to implement, they do not require any special hardware or software, what they need is a policy and procedure and people who follow the same.

11.1.1 Objectives, framework, environment, activities, monitoring

How do we ensure that the organization, management, auditors and others understand the framework that encompasses the controls? This will normally involve interviewing senior managers including Chief Financial Officers to ensure that someone in the organization has considered the issue and then communicate that information to appropriate the staff. The communication may be in the form of policy and procedures manuals or handbooks. There could also be minutes of meeting that summarize the discussion and recommendations made. There should be evidence of risk analysis being undertaken and appropriate procedures and changes put in place.

The organization may have invested in a control methodology and you should be able to get a copy of this. You would also expected to be able to discuss the control framework with the internal and/or external auditors and review their findings.

1. Policies:

Policies and high level documents. They represent the corporate philosophy of an organization and strategic thinking of senior management and the business process owners. To be effective they must be clear and concise. Management must create a positive control environment by assuming responsibility for formulating, developing, documenting, promulgating and controlling policies covering general goals and directives. Management should take the steps necessary to ensure that employees effected by a specific policy receive a full explanation of the policy and that they understand the intent.

In addition to the corporate policies that set the tone for organization as a whole, individual division and departments should define lower level policies. These would apply to the employees and operations of these units and would focus at the operational level.

A top-down approach to the development of the lower level policies in instances when they are derived from corporate policies is desirable, as it ensures consistency across the organization. However some organization begin by defining operational level policies as immediate priorities. Theses companies view this as being the more cost affective approach since these policies are often derived and implemented as the result of risk assessments. This is bottom-up approach; where in corporate policies are a subsequent development and a synthesis of existing operational policies. This may seem more practical but it leaves room for inconsistency and conflicting situation in policies.

Management should review all policies. Policies need to be updated to reflect new technology and significant changes within the organization or department.
2. Procedures:

Procedures and detailed documents. They must be derived from the parent policy and must implement the spirit (intent) of the policy statement. Procedure must be written in a clear and concise manner so that they may be easily and properly understood by those governed by them. Procedure document (administrative and operational) business processes and the control embedded therein.

Procedures are usually more dynamic than their respective parent policies. They must reflect the regular changes in the business focus and environment. Hence, frequent review and updates of procedures are essential if they are to be relevant. An auditor will find a divergence between practice and precept in organizations that neglect the review process. Auditors review procedures in order to identify and thereafter test controls embedded in procedures are evaluated to ensure that they fulfill necessary control objectives while making the process as efficient and practical as possible. Where operational practices do not match documented procedures or where documented procedures do not exist, it is difficult for management and auditors to identify controls and ensure that they are in continues operations.

An independent review is necessary to ensure that policies and procedures have been properly understand and executed. The reviewer should maintain independence at all times and not be influenced by anyone in the group being reviewed. Evidence of work performance should be adequate and provide the viewers with a level of confidence that the work was performed in compliance with established policies and procedures.

11.1.2 Legal, ethical, professional standards /requirements

To ensure the organization meets these requirements the COBIT guidelines suggest that first of all the requirements must be fully understood and their impact gauged. Then there should be appropriate measures to comply with them.

You would gain information by interviewing senior managers in appropriate areas such as legal. HG, taxation, commercial etc. there may be requirements documented in industry or trade association documents or even specific legislation. There may be contracts that impact compliance and need to be reviewed.

There should be standards and policies in place to cover these requirements and audit tests will need to be devised to ensure that staff are adhering to these

11.1.3 Preventative/detective/corrective strategies

The objective of a control is to reduce any expected loss from a risk event occurring. In some cases the loss may be reduced to zero. There has to be a balance between the cost of the control and the maximum or expected loss.

As an orgazition plans its control strategies it may be convenient to consider controls as

1. Preventative – reduces probability of event arising in the first place
2. Detective – discovers the problem before too great a loss has occurred
3. Corrective – discovers an error and is able to correct it

When planning the controls these work together. Extra effort that may be applied in preventative controls usually means that detective and corrective controls are not so important. If preventative controls are poor then the detective controls will need to be enhanced to catch the errors.


11.1.4 **Effective control environment (personnel management methods)**

Before we start to look in detail at more technical or automated control techniques we must remember that controls often work with and through people.

The wood control implies two parties – one exercising control and the other which is controlled. In IT controls we can see two scenarios:

1. the computer system is controlling the user
2. the user controls the computer.

We have already shown how HR policies on recruitment retention and training of staff will impact the controls that need to be incorporated. It is important to realize that staff will usually make the final decision as to how effective a control will be.

For example, an audit log file may be produced showing that an employee attempted to access a secure file. If no one follows up on this then the control may just as well not exist.

Managers in particular will need to understand what their roles are in the control environment. This goes all the way to the top because, taking the same example, if the CFO has been trying to access a secure file then the managing director needs to know, who checks what the MD has been doing?

COBIT specifically identifies managing human resources as a high-level control objective. The auditors would find it useful to examine the HR procedures and to see if there is sufficient emphasis on employee areas of control responsibility.

11.1.5 **Contingency plans, insurance**

One important aspect of overall controls design is to consider what will happen if a major disaster strikes. This is normally the function of a disaster planning or contingency planning exercise.

The process will be described in more detail later but it is important to consider it as part of the control plan the control of last resort. Most of the controls that we will discuss cannot prevent a natural disaster such as fire, flood, earthquake, etc. In such a case there will need to be a recovery plan.

Also to be considered is how insurance should fit into the control plan/design. It is usual to insure equipment against common risks such as fire or theft. Even business disruption and recovery of records an be insured but the premiums may be very expensive. If the organization is out of action for a long period of time then customers may go elsewhere, never to return, even when full services are resumed.

Insurance policies may have clauses in them requiring the organization to take special precautions or to meet other obligations such as having a fire sprinkler system. These clauses need to be met by the controls design because they are now part of the controls framework .......... which is where we came in?
11.2 CONTROL PROCEDURES

As you look at IT applications there are many controls that can be applied. Weber devotes 6 chapters to these and categorizes them as

- Boundary controls
- Input controls
- Communication controls
- Processing controls
- Database controls
- Output controls

This is a useful categorization as it follows the way applications can be viewed. First the boundary controls consider access to the application. Then, once authorized, data can be input. Today that input data is likely to follow across communication lines before being processed. The results of processing will usually update a database somewhere and finally staffs receive and rely on the output. Of course as you examine the specific hardware and software mechanisms that are used for these you could further analyse them as preventative or detective controls.

11.2.1 Boundary controls

The subsystem that interfaces the computer system with its environment is called boundary subsystem. The major function of such system is to provide the following features:

- Identification of users
- Authentication of users
- User request handling

The controls implemented to restrict the unauthorized access are called boundary controls. We will first discuss the ways in which a link with the system can be established and then we will discuss the controls over them.

There are two types of controls implemented in the access system:

- Physical access controls
- Logical access controls

1. Physical access controls

I. Controls within computer department

Security in the computer department itself is likely to be very tightly controlled. Some of the controls that may be operated are:

(a) The computer department being sited in a secure part of the building, often on an upper floor.
(b) Access may be past a separate reception or security desk.
Access being via locked doors. These doors may be opened in a number of different ways:

(i) typing in a personal identification number (PIN) may unlock the door
(ii) an electronic key card may allow access
(iii) conventional keys may be issued to authorised personnel
(iv) combination locks requiring a person to type in a set sequence of digits, which can be periodically changed.

(d) Closed circuit TV can be used to monitor what is happening in a particular part of a building. This may be backed up by security video cameras.

(e) Doors can be automatically locked in the event of a security alarm.

(f) Computer equipment can be electronically or physically tagged to activate an alarm if an attempt is made to carry it out of the building or computer area.

Other devices to identify unauthorised persons such as machines which can identify fingerprints or scan the pattern of a retina are often seen in TV programs, but are not in general use, either for technological reasons or because they are too expensive.

II. Data security

The first line of defence against interlopers is to physically control who is allowed near to the computer. The second line of defence is to reduce the damage that can be caused when the first line of defence is breached.

This can happen when an interloper succeeds in getting past the security measures or when a hacker manages to access the computer remotely.

In either case it is vital to prevent unauthorised users from changing or viewing data and to limit the damage that they can do. There are a number of points to consider:

(a) Diskettes and CDs (both referred to hereafter as disks) are vulnerable to theft and to damage. Although the disks themselves are not valuable, the data they hold can be much more so. They can be easily smuggled out of a building in a briefcase or a pocket, and disk security is often a weak link in an organisation.

Disks should not be left lying around on desks and working surfaces. They may be lost, stolen, inadvertently re-used or damaged by spillages of hot drinks. Disks should be locked away when not being used, and should be filed for easy reference. All disks containing important information must be backed up on a regular basis.

(b) Computer printout may well contain confidential data. Many industrial spies make a habit of investigating the rubbish for useful titbits of information. Disks are also sometimes discarded and, even if files have been deleted, the data on them can be recovered. Both printout and disks should be shredded or otherwise destroyed before being thrown away.

(c) Passwords and user numbers are used as a way of identifying who is authorised to access the system. There may be several levels of password, with particularly sensitive applications protected by multiple passwords. There may also be a system of 'electronic handshakes'; these enable the computer to recognise which terminal is accessing it. This allows some applications to be restricted only to certain terminals. These protections can also be used to help track down the culprits when a security breach has occurred.
It is important to maintain strict security over the passwords used. Unauthorised users may discover passwords in several ways. For example, a written reference to the password may be secreted somewhere near the computer (often taped to the underside of a desk drawer). The hacker may be able to guess the password from knowledge of the private life of an authorised user; the password or user number might be worked out through trial and error (sometimes carried out systematically by a computer program) the password may have been 'lent' or otherwise discovered because of carelessness.

To protect passwords and user numbers against discovery, a number of precautions should be adopted:

(i) Passwords should be regularly changed.

(ii) Passwords should be memorable but not obviously related to a user's private life (common password choices such as children's or pets' names or birthdays).

(iii) There should be strict controls over passwords - they should never be 'lent' or written down where they can be easily seen.

(iv) There should be automatic sentinel or watchdog programs to identify when a password has been keyed incorrectly.

(d) PIN numbers are used in certain circumstances. These personal identification numbers can be used in combination with magnetic strip cards to reinforce security. Cash dispensers are a typical example of this kind of protective measure.

2. **Logical Access Controls**

Access or points of entry to an organization’s information systems infrastructure can be gained through several avenues. Each avenue is subject to appropriate level of access security. For example, paths of logical access often relate to different level occurring from either a backend or front-end interconnected network of systems for internally or externally based users front-end systems are network-based systems connecting an organization to outside untrusted networks, such as corporate websites, where a customer can-access the website externally in initiating transactions that connects to a proxy server application which in turn connects for example to back-end database system in updating a customer database.

I. **General Points of Entry**

General points of entry to either front-end or back-end systems relate to an organizations networking or telecommunications infrastructure in controlling access into their information resources (e.g., application, databases, facilities, networks). The approach followed is based on a client-server model where for example a large organization can have literally thousands of interconnected network servers. Connectivity in this environment needs to be controlled through a smaller set of primary domain controlling servers, which enables a user to obtain access to specific secondary points of entry (e.g., application, servers, database, etc).

General modes of access into this infrastructure occur through the following:

- **Network Connectivity** – Access is gained by physically connecting a PC to a segment of an organization network infrastructure. At a minimum, such access requires user identification and authentication to a domain controlling server. More specific access to a particular application or database may also require the user to identify and authenticate themselves to that particular server (secondary point of entry). Other modes of access into the infrastructure
can also occur through network management devices, such as routers and firewalls, which should be strictly controlled.

- **Remote Access**—A user deal in remotely to an organization’s server which, generally requires the user identify and authenticate to the serve for access to specific functions that can be performed remotely (e.g., e-mail, ftp, internet or some application specific function). Using VPN, a user can also attain complete access to view all network resources and authenticate into those where privileges have been granted. Remote access points of entry can be very extensive and should be centrally controlled where possible. Within a networked environment, the more traditional points of entry into specific computer systems still apply (i.e., secondary points of entry, related only to server’s own environment for example, points of entry for mainframe-based systems used for large database system “legacy” applications would include the following:

- **Operator Console**—The privileged computer terminals control most computer operations and functions. To provide security, these terminals should be located in suitably controlled facility so that physical access can only be gained be authorized personnel. Most operator consoles do not have strong logical access controls and do provide a high level of computer systems access. Therefore, the terminal must be located in a physically secured area.

- **Online Terminals**—Online access to computer systems through terminal typical requires the entry of at least a logon-Id and password to gain access to the host computer system and may also require further entry of authentication or identification data access to application specific systems. Separate security and access control software to be employed on larger systems to improve the security provided by the operating system or application system. Traditionally, this level of access was completed through mainframe’s proprietary network. Today, however computers (PCs) are connected to organization’s networking system infrastructure that includes the mainframe as a network node. To access, personal computers (PCs) are often used as online access term through terminal emulation software. This poses a particular risk as the PCs can programmed to store and recall user access codes and passwords.

From a security standpoint. It is incumbent upon the organization to know all of its point of entry into its information resource infrastructure, which in many organizations will not be a trivial task (e.g., remote access users in the thousands). This is significant because any point of entry not appropriately control can potentially compromise the security of an organization's sensitive and critical information resources. IS auditors, in performing detailed network assessments and access control reviews, should determine whether points of entry are known and should support management’s effort in obtaining the resources to identify all access paths.

II. **Logical Access Issues and Exposures**

Inadequate logical accesses controls increase an organization’s potential for losses resulting exposures. These exposures can result in minor inconveniences unto total shutdown computer functions.

Exposures that exist from accidental or international exploration of logical access weaknesses can include:

- technical exposures and
- computer crime.

III. **Technical Exposures**
It involves the unauthorized, (international or unintentional) implementation or modification of data and software. Following are some common ways in which such an act is carried out:

- **Data diddling** involves changing data before or as they are entered into the computer. This is one of the most common abuses because it requires limited technical knowledge and occurs before computer security can protect data.

- **Trojan horses** involve hiding malicious, fraudulent code in and authorized computer program. This hidden code will be executed whenever the authorized program is executed. A classic example is the Trojan horse in the payroll calculating program that shaves a barely noticeable amount off each paycheck and credits it to the perpetrator's payroll account.

- **Rounding down** involves drawing off small amounts of money from a computerized transaction of account and rerouting this amount to the perpetrator's account. The term rounding down refers to rounding small fractions of a denomination down and transferring these small fractions into the unauthorized account. Since the amounts are so small, they are rarely noticed.

- **Salami techniques** involve the slicing of small amounts of money from a computerized transaction or account and are similar to the rounding down technique. The difference between the rounding down technique and the salami technique is that in rounding down the program rounds off by the penny. For example, if a transaction amount in U.S. funds were $1,235,954.39 the rounding down technique may round the transaction to $1,235,954.35. The Salami technique truncates the last few digits from the transaction amount so $1,235,954.39 becomes $1,235,954.30 or $1,235,954.00 depending on the calculation built into the program.

- **Viruses** are malicious program code inserted into other executable code that can self-replicate and spread from computer to computer, via sharing of computer diskettes transfer of logic over telecommunication lines or direct contact with an infected machine/code. A virus can harmlessly display cute messages on computer terminals dangerously erase or alter computer files or simply fill computer memory with junk to point where the computer can no longer function. An added danger is that a virus may be dormant for some time until triggered by a certain event or occurrence, such as date (1 January - Happy New year!) or being copied a pre-specified number of time. During this time the virus has silently been spreading.

- **Worms** are destructive programs that may destroy data or utilize tremendous computer and communication resources but do not replicate like viruses. Such program do not change other programs, but can run independently and travel from machine to machine across network connections. Worms may also have portions of themselves running on many different machines.

- **Logic bombs** are similar to computer viruses, but they do not self-replicate. The creation of logic bombs requires some specialized knowledge, as it involves programming the destruction or modification of data at a specific time in the future, page. However, unlike viruses or worms logic bombs are very difficult to detect before they below up; thus of all the computer crime schemes, they have the greatest potential for damage. Detonation can be timed to cause maximum damage and to take place long after the departure of the perpetrator. The logic bomb may also be used as a tool of extortion, with a ransoms being damaged in exchange for disclosure of the location of the bomb.

- **Trap doors** are exists out of an authorized program that allows insertion of specific logic, such as program interrupts, to permit review of data during processing. These holes also permit insertion of unauthorized logic.

- **Asynchronous attacks** occur in multiprocessing environments where data move asynchronously (one character at a time with a start and stop signal) across telecommunication lines. As a result, numerous data transmission must wait for the line to be free (and flowing in the proper direction) before being transmitted. Data that are waiting are susceptible to unauthorized accesses called asynchronous attacks. These attacks, which are usually very small pin like insertions into cable, may be committed via hardware and are extremely hard to detect. There are many forms of asynchronous attack. This is a very
complex and technical exposure and the US auditor will require the assistance of a network manager and/or a system software analyst to evaluate it.

- **Data leakage** involves siphoning or leaking information out of the computer. This can involve dumping files to paper or can be as simple as sealing computer reports and tapes,
- **Wire-tapping** involves eavesdropping on information being transmitted over telecommunications lines.
- **Piggybacking** is the act of following an authorized person through a secured door or electronically attaching to an authorized telecommunications link to intercept and possibly alter transmissions.
- **Computer shut down** can be initiated through terminals or microcomputers conversed directly (online) or remotely (dial-up lines) to the computer. Only individuals knowing a high-level systems logon-ID can usually initiate the shutdown process. This security measures is effective only if proper security access controls are in place for the high-level logon-ID and the telecommunications connections into the computer. Some systems have proven to be vulnerable to shutting themselves down under certain conditions of overload.
- **Denial of service** is an attack that disrupts or completely denial service to legitimate users, networks, systems, or other resources. The intent of any such attack is usually malicious in nature and often takes little skill because the request tools are readily available.

IV. **Viruses**

Viruses are a significant and a very real logical access issue. We have discussed viruses in detail in chapter 4. here we will consider how can we avoid the threat imposed by computer viruses.

V. **Controls Over Viruses**

Computer viruses are a threat to computers of any type. Their effects can range from the annoying, but harmless, prank to damaged files an crashed networks. In today's environment, networks are the ideal way to propagate viruses through a system. The greatest risk is from electronic mail (e-mail) attachments from friends and/or anonymous people through the internet. There are two major ways to prevent and detect viruses that infect computer and network systems. The first is by having sound polishes and procedures in place and the second is by technical means, including antivirus software. Neither is effective without the other.

The best way to protect the computer against viruses is to use antivirus software. There are several kinds. Two types of scanners are available one checks to see if your computer has any files that have been infected with known viruses; the other checks for atypical instructions (such as instructions to modify operating system files) and prevents completion of the instruction until the user has verified that it is legitimate.

Once a virus has been detected, an eradication program can be used to wipe the virus from the hard disk. Sometimes eradication programs can kill the virus without having to delete the infected program or data file, while other times those infected files must be deleted. Still other programs, sometimes called inoculators, will not allow a program to be run if it contains a virus.

Some of the policy and procedure controls that should be in place are:

- Build any system from original, clean master copies. Boot only form original diskettes whose write protection has always been in place.
- Allow no disk to be used until in has been scanned on a stand-alone machine that is used for no other purpose and is not connected to the network.
- Update virus software scanning definitions/signatures frequently.
• Write protect all diskettes
• Have vendors run demonstrations on their machines, not yours.
• Enforce a rule of not using shareware without first scanning the shareware thoroughly for a virus.
• Commercial software is occasionally supplied with a Trojan horse (viruses or worms). Scan before any new software is installed.
• Insist that field technicians scan their disks on a test machine before they use any of their disks on the system.
• Ensure that the network administrator uses work station and server anti-virus software.
• Ensure that all servers are equipped with an activated current release of the virus detection software.
• Consider encrypting files then decrypt them before execution.
• Ensure that bridge, router and gateway updates are authentic. This is a very easy way to place and hide a Trojan horse.
• Backups are a vital element of anti virus strategy. Be sure to have a sound and effective back up plan in place this plan should account for scanning selected backup files for virus infection once a virus has been detected.
• Educate users so they will heed these policies and procedures.
• Review antivirus policies and procedures and identify a contact person.
• Prepare a virus eradication procedure and identify a contact person.

Technical methods of preventing viruses can be implemented through hardware and software means. The following are hardware tactics that can reduce the risk of infection:

• Use boot virus protection (i.e., built in hardware based virus protection)
• Use remote booting
• Use a hardware-based password
• Use write protected tabs on floppy disks

There are three different types of antivirus software:

1. **Scanners** look for sequence of bits called signatures that are typical of virus programs. Scanners examine memory, disk boot sectors, executables, data files and command files for bit patterns that match a known virus. Scanners therefore need to be updated periodically to remain effective.

2. **Active monitors** interpret DOS and ROM basic input-output system (BIOS) calls, looking for virus-like actions. Active monitors can be annoying because they cannot distinguish between a user request and a program or virus request. As a result, users are asked to confirm actions like formatting a disk or deleting a file or set of files.

3. **Integrity checkers** compute a binary number on a known virus-free program that is then stored in a database file. The number is called a cyclical redundancy check or CRC. When that program is called to execute, the checker computes the CRC on the program about to be executed and compares it to the number in the database. A match means no infection; a mismatch means that a change in the program has occurred. A match means no infection; a mismatch means that a change in the program has occurred. A change in the program could mean a virus within it. Integrity checkers take advantage of the fact that executable programs and boot sectors do not change very often, if at all.
VI. Computer Crime Exposures

Computer systems can be used to steal money, goods, software or corporate information. Crimes also can be committed when the computer application process or data are manipulated accept false or unauthorized transactions. These also is the simple, non-technical method of computer crime by stealing computer equipment.

Computer crime can be performed with absolutely nothing physically being taken or stolen. Supply viewing computerized data can provide an offender with enough intelligence to steal ideas or confidential information (intellectual property).

Committing crimes that exploit the computer and the information it contains can be damaging to the reputation, morale and very existence of an organization. Loss of customers, embarrassment to management and legal actions against the organization can be a result. Threats to business include the following:

- **Financial loss**—These losses can be direct, through loss of electronic funds or indirect, through the costs of correcting the exposure.
- **Legal repercussions**—There are numerous privacy and human rights laws an organization should consider when developing security policies and procedures. These laws can protect the organization but can also protect the perpetrator from prosecution. In addition, not having proper security measures could expose the organization to lawsuits from investors and insurers if a significant loss occurs from a security violation. Most companies also must comply with industry-specific regulatory agencies. The IS auditor should obtain legal assistance when reviewing the legal issues associated with computer security.
- **Loss of credibility** or competitive edge—Many organizations, especially service firms such as banks, savings and loans and investment firms, need credibility and public trust to maintain a competitive edge. A security violation can severely damage this credibility, resulting in loss of business and prestige.
- **Blackmail/industrial espionage**—By gaming access to confidential information or the means to adversely impact computer operations, a perpetrator can extort payments or services from an organization by threatening to exploit the security breach.
- **Disclosure of confidential, sensitive or embarrassing information**—As noted previously, such events can damage an organization’s credibility and its means of conducting business. Legal or regulatory actions against the company may also be the result of disclosure.
- **Sabotage**—Some perpetrators are not looking for financial gain. They merely want to cause damage due to dislike of the organization or for self-gratification. Logical access violations are when the same people who exploit physical exposures, through the skills needed to exploit logical exposures are more technical and complex.
- **Hackers**—Personal with the ability to explore the details to programmable systems and the knowledge to stretch or exploit their capabilities, whether ethical or not. Hackers are typically attempting to test the limit of access a computer with the intent of overcome the obstacles. Some often do not access a computer with the intent of destruction, although, this is often the result. Other categories of hackers include, script kiddies, hack-activists and criminal hackers. Script kiddies refer to individuals who use scripts and programs written by others to perform their instructions and are often incapable of writing similar script on their own. Hack-activists refer to individuals using their skills to forward a political agenda, possibly breaking the law in process, justifying their action for political reason (end justifies the means). Finally, there are hackers more malicious in nature whose primary purpose or satisfaction (also referred to as crackers).
- **Employees**—(authorized or unauthorized)
- **IS Personnel**—these individuals have the easiest access to computerized information since they are the custodians of this information. In addition to logical access controls, good
segregation of duties and supervision help reduce logical access violations by these individuals.

- Competitors
- Foreigners
- Organized criminals
- Crackers (paid hacker working for third party)

- **Part Time and Temporary Personnel**—Remember that office3 cleaner often have a great deal of physical access and may be competent in computing.
- **Vendors and Consultant**
- **Accidental Ignorant**—someone who knowingly perpetrates a violation.

### VII. ACCESS CONTROL SOFTWARE

The access control software interfaces with other system software programs. For example access control software on the mainframe interfaces with the tape/disk management system, job scheduling system, application programs, system catalogs, system exits, system logs, databases and online telecommunications systems.

Access control software generally performs the following tasks:

- Verification of the user
- Authorization of access to defined resources
- Restriction of users to specific terminals
- Reports on unauthorized attempts to access computer resources, data or programs

Access control software may provide the following authorization functions:

- Verify user authorization to sign-on at the network and subsystem levels
- Verify user authorization at the application and transaction level.
- Verify user authorization within the application.
- Verify user authorization at the held level for changes within a database.
- Verify subsystem authorization for the user at the file level.

The following are some of the standard functions of access control systems:

- Establishing logon-IDs and user authentication
- Limiting of specific terminals for specific logon-IDs
- Limiting access based on predetermined times
- Limiting specific tasks to be initiated from a predefined authorized library
- Establishing rules for access
- Creating individual accountability and audit ability
- Creating installation-level restriction keys and default file creation access masks
- Creating or changing, user profiles
- Creating or changing data files and database profiles
• Logging events
• Logging user activities
• Logging database/data communications access activities for monitoring access violations
• Reporting capabilities

The following is a list of computerized files and facilities that should be protected by logical access controls:

• Data
• Application software (test and production)
• Utilities
• Telecommunications lines
• Libraries/Directories
• Passwords
• Temporary disk files
• Tape files
• System software
• Access Control software
• Procedure libraries
• Logging files
• Bypass label processing feature
• Operator system exits
• Dialup lines
• Data dictionary/directory
• Spool queues

3. LOGICAL SECURITY, TOOLS AND PROCEDURES

I. Authentication Techniques or logical Access control

Authentication techniques are the process of proving one's identity where the system verifies the identity of the user. These techniques are typically categorized as something you know, something you have, and something you are (a biometric feature). These techniques can be used stand alone or in combination to authenticate a user.

For example, a two factor authentication technique involves the use of something you know, such as a pin number with something you have, such as a token card. A three factor authentication techniques is the same as the above, expect for adding in attributes of something you are, such as a palm or iris biometric scan.

II. Logon-IDs and Passwords

This two-phase user identification/authentication process based on something you know can be used to restrict access to computerized information, transaction, programs and system software. The computer can maintain an internal list of valid logon-IDs and a corresponding set of access rules for each logon-ID. These
access rules identify the computer resources the user of the logon-ID can access and constitute the user's authorization. Access rules can usually be specified at the operating system level (controlling access to files) or within individual application systems (controlling access to menu functions and types of data).

The logon-ID provides individual identification. Each user gets a unique logon-ID that can be identified by the system. The format of logon-IDs is typically standardized.

The password provides individual authentication. Identification/authentication is a two-step process by which the computer system first verifies that the user has a valid logon-ID (user identification) and then requires the user to substantiate his/her validity via a Password.

FEATURES OF PASSWORDS

- A password should be easy for the user to remember but difficult for a perpetrator to guess.
- Initial passwords may be allocated by the security administrator or generated by the system itself. When the user logs on for the first time, the system should force a password change to improve confidentiality. Initial password assignments should be randomly generated and assigned, where possible, on an individual, and not a group, basis. Accounts never used with or without an initial password assignment should be removed from the system.
- If the wrong password is entered a predefined number of times, typically three, the logon-ID should be automatically and permanently deactivated (or at least for a significant period of time).
- If a logon-ID has been deactivated because of a forgotten password, the user should notify the security administrator. The security administrator should then reactivate the logon-ID only after verifying the user's identification
- (challenge/response system) much like a bank verifies an account holder's ID before giving information over the phone (such as mother's maiden name) by returning the phone call after verifying the user's extension or calling the user's supervisor for verification.
- Password should be internally one-way encrypted. Encryption is a means of encoding data stored in the computer. This reduces the risk of a perpetrator gaining access to other user's password (if the perpetrator cannot read and understand it, he cannot use it). Password should not displayed in any form—either on a computer screen when entered, on computer reports in index or card files or written on pieces of paper taped inside a person's desk. these are the first places a potential perpetrator will look.
- Password should be changed periodically. On a regular basis (for example, every 30 days), the user should change his/her password should be changed by the user at his or her own terminal/workstation rather than at the administrator's terminal or in any location where their new password might be observed. The best method is for the computer system to force the change by notifying the user prior to the password expiration date. Voluntary changing is just that, voluntary so it probably will not be done.
- Password must be unique to an individual: if a password is know to more than one person, the responsibility of the user for all activity within their account cannot be enforced.

Password Syntax (format) Rules

- Ideally, password should be five to eight characters in length. Anything shorter is too easy to guess. Anything longer is too hard to remember.
- Password should allow for a combination of alpha, numeric, upper and lower case and special characters.
• Password should not be particularly identifiable with the user (such as first name, last name, spouse name, pet’s name, etc). Some organizations prohibit the use of vowels, making word association/guessing of passwords more difficult.

• The system should not permit previous password(s) to be used after being changed.

• Logon-IDs not used after a number of days should be deactivated to prevent possible misuse. This can be done automatically by the system or manually by the security administrator.

• The system should automatically disconnect a logon if no activity has occurred for a period of time (one hour). This reduces the risk of misuse of an activity logon session left unattended because the user went to lunch; left for home, went to a meeting or otherwise forgot to logoff. This is often referred to as a time out.

III. LOGGING COMPUTER ACCESS

With most security packages today, computer access and attempted access violations can be automatically logged by the computer and reported. The frequency of the security administrator's review of computer access reports should be commensurate with the sensitivity of the computerized information being protected. The IS auditor should ensure that the logs cannot be tampered with or altered without leaving an audit trail.

When reviewing or performing security access follow-up, the IS auditor should look for

• Patterns or trends that indicate abuse of access privileges, such as concentration on a sensitive application

• Violations (such as attempting computer file access that is not authorized) and/or use of incorrect passwords

• What to do with reported attempted violations:

  • Today attempted violations can be detected on either a real-time basis and acted upon or after the fact. For interconnected networks often the first line of defense for attacks on organization’s trusted networks and system is intrusion detection software (IDS). IDS refers to the process of discovering unauthorized use of computers and networks through the use of software designed for this purpose. IDS works in a variety of ways, either host-or network based in analyzing incoming, data captured that is logged for signs of unauthorized access. In designing these systems, organization's should identify scenarios or events that constitute a high-risk where there is real-time notification of these events occurring (IDSs interfacing with pagers) to system administrators and procedures established for responding to those events.

  • Once a violation has been identified:

    • The person who identified the violator should refer the problem to the security administrator for investigation.

    • The security administrator and responsible management should work together to investigate and determine the security of the violation. Generally, most violations are accidental.

    • Generally if a violation attempt is serious, executive management should be notified, not law enforcement officials. Executive management is normally responsible for notifying law enforcement officials. Involvement of external agencies may result in adverse publicity that is ultimately more damaging than the original violation and the decision to involve external agencies should therefore be left to executive management.

  • Procedure should be in place to manage public relations and the press.
• To facilitate proper handling of access violations, written guidelines should exist that identify various types and levels of violations and how they will be addressed. This effectively provides direction for judging the seriousness of a violation.

• Disciplinary action should be a formal process that is consistently applied. This may involve a reprimand, probation or immediate termination. The procedures should be legally and ethically sound to reduce the risk of legal action against the company.

• Corrective measures should include a review of the computer access rules, not only for the perpetrator but for interested parties. Excessive or inappropriate access rules should be eliminated.

IV. One Time Passwords

A two-factor authentication technique, such as microprocessor-controlled smart cards, generates one-time passwords that are good for only one log-on session. Users enter this password along with a password they have memorized to gain access to the system. This technique involves something you have (a device subject to theft) and something you know (a personal identification number). Such devices gain their one time password status because of a unique session characteristics (e.g., ID or time) appended to the password.

V. Biometric Security Access Control

Biometric access controls are the best means of authenticating a user's identity based on a unique, measurable attribute or trait for verifying the identity of a human being. This control restricts computer access based on a physical (something you are) or behavioral (something you do) feature of the user. Example of a physical feature include a fingerprint, eye retina pattern, face or hand. Behavior traits include voice, signatures and keystroke dynamics. Traditionally, biometric systems have been used very little as an access control technique. However, due to advances in hardware efficiencies and storage, biometric systems are becoming a more viable option as an access control mechanism.

Generally, a reader interprets the individual's biometric features before permitting authorized access, However this is not a foolproof process because certain biometric features can change (e.g., scarred fingerprints, signature irregularities, change in voice, etc). For this reason, biometric access control systems are not all equally effective.

Entering a user's biometric into a system occurs through an enrollment by storing a user's particular biometric feature. This occurs through an interactive averaging process of acquiring a physical or behavior sample, extracting unique data from the sample (converted into a mathematical code) creating an initial template, comparing new samples(s) with what has been stored an developing a final template that can be used for authenticating the user. Subsequent samples will be used in determining whether a match or non match condition exists for granting access.

Generally, the ordering of biometric devices with the best response times and low EERs are palm, hand, iris, retina, fingerprint, and voice, respectively.

VI. Workstation (PC or terminals) Usage Restraints

• **Workstation security**--This security feature restricts the number of workstations that can access certain transactions based on the physical/logical address of the workstation.

• **Workstation Locks**—This security feature prevents turning on a PC workstation until a key lock is unlocked by a turn key or card key.
VII. Dial-back procedures

When a dialup line is used, access should be restricted by a dial-back mechanism, user calling line identify to verify the calling number, or strong two factor authentication. Dial-back interrupts the telecommunication dialup connection to the computer by dialing back the caller to validate user authority. Dial-back can be manual (the computer operator calls back the user) or automatic, (the computer calls back the user using a computerized list of valid phone numbers). If the call back is not to a valid telephone number, access is permitted. As added precautions, dialup telephone numbers should be changed periodically, should not have the same prefix as the office phone numbers and should not be displayed on modems or terminals. Once a dialup connection is made, logical access controls should provide the same restriction as if the user were using a terminal from within the organization.

VIII. Logging Online Activity

Many computer systems can automatically log computer activity initiated through a logon-ID or computer terminal. This is known as a transaction log. The information can be used to provide a management/audit trail.

IX. Data Classification

Computer files, like documents, have varying degrees of sensitivity. By assigning classes or levels of sensitivity to computer files, management can establish guidelines for the level of access controls that should be assigned. Classification should be simple, such as high medium and low. End user managers and the security administrator can then use these classifications to assist with determining who should be able to access what.

Data classification reduces the risk and cost of overprotecting computer resources. Data classification is extremely important when identifying who should have access to production versus test data and programs. Production data are live or historical data used to run the business. The owner must grant access to that data or program.

Thus, data classification as a control measure should define:

- Who has access rights?
- Who is responsible for determining the access rights and access levels?
- What approvals are needed for access?

In order to ensure that the appropriate levels of access are allowed organizations may develop an authorizations matrix such as the one shown below.

<table>
<thead>
<tr>
<th>User</th>
<th>Group</th>
<th>File 1</th>
<th>File 2</th>
<th>File 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>User 1</td>
<td>Group 1</td>
<td>Read, write</td>
<td>Road</td>
<td>Print to</td>
</tr>
<tr>
<td>User 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User 3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User 4</td>
<td>Group 2</td>
<td>Read</td>
<td>Read, write</td>
<td>Manage</td>
</tr>
<tr>
<td>User</td>
<td>Group</td>
<td>Read/Write</td>
<td>Delete, owner</td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>--------</td>
<td>------------</td>
<td>---------------</td>
<td></td>
</tr>
<tr>
<td>User 5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User 6</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User 7</td>
<td>Group 3</td>
<td>Read. Write</td>
<td>Read. Write.</td>
<td></td>
</tr>
<tr>
<td>User 8</td>
<td></td>
<td>Delete, owner</td>
<td>Delete, owner</td>
<td></td>
</tr>
<tr>
<td>User 9</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Control Activities II

<table>
<thead>
<tr>
<th>Topic List</th>
<th>Syllabus Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1 Application Control procedures</td>
<td>2.8</td>
</tr>
<tr>
<td>12.2 Communication Controls</td>
<td>2.8</td>
</tr>
<tr>
<td>12.3 Database controls</td>
<td>2.8</td>
</tr>
<tr>
<td>12.4 General controls procedures</td>
<td>2.8</td>
</tr>
</tbody>
</table>

Introduction

We have discussed controls relating to the system access in the previous chapter. In this chapter we will continue with the other areas of control.

Study Guide
12. CONTROL ACTIVITIES II

12.1 APPLICATION CONTROL PROCEDURES

Application controls are controls over input, processing and output functions. Application controls include method for ensuring that:

- Only compete, accurate and valid data is entered and updated in a computer system
- Processing accomplishes the correct task
- Processing results meet acceptation’s
- Data is maintained

These controls may consist of edit tests, totals, and reconciliation, and rectifications and reporting of incorrect, missing or exception data. Automated controls should be coupled with manual procedures to ensure proper investigations of acceptance.

The IS auditors tasks include the following:

- Identifying the significant application components and the flow of transaction through the system and gaining a detailed understanding of the application by reviving the available documentation and interviewing appropriate personnel.
- Identifying the application control strength and evaluating the impact of the control weaknesses to develop a testing strategy by analyzing accumulated information.
- Testing the control to ensure their functionality and effectiveness by applying appropriate audit procedures
- Evaluating the control environment to determine that control objectives were achieved through analyzing the test results and other audit evidence
- Considering the operational aspects of the application to ensure its efficiency and effectiveness by comparing the system with efficient programming standards, analyzing procedures used and comparing them to management’s objectives for the system.

12.1.1 Input Controls

Input control procedure must ensure that every transaction to be processed is received, processed and recorded accurately. These controls should ensure that only valid and authorized information is input and that these transactions are processed only once. In an integrated system environment, output generated by one system is the input of the other system, therefore the edit checks, validations and access controls of the system generating the output must be reviewed as input/organization controls.

Input is important because it usually involves routine human intervention and prone to errors. Input is usually through input devices like keyboard, mouse, and more advanced EPOS (Electronic Point of Sale) terminals and ATM (Automated Teller Machines). It is obvious that input will be subject to more control from devices such as ATM and EPOS then conventional keyboard entry.
Generally input control techniques include:

- **Transaction log**—contains a detailed list of all updates. The log can be whether manually maintained or provided through automatic computer logging. A transaction log can be reconciled to the number of source documents received to verify that all transactions have been input.

- **Reconciliation of data**—controls are needed to ensure that data received are recorded and properly processed.

- **Documentation**—written evidence of user, data entry, and data control procedures.

- **Error correction procedures:**
  - Logging of errors
  - Timely correction
  - Upstream resubmission
  - Approval of correction
  - Suspense file
  - Error file
  - Validity of correction

- **Anticipation**—the user or control group anticipates the receipt of data

- **Transmittal log**—this log documents the transmission or receipt of data

- **Cancellation of source documents**—procedures to cancel source documents e.g. by purchasing with holes or marking them, to avoid duplicate entry.

After having an idea about the general controls we will now look at more detailed controls that can be implemented over the input function of an information system. They include:

1. Input authorization
2. Batch control and balancing
3. Error reporting handling
4. Data validation and editing
5. Source document design
6. Data entry screen design
7. Caption design
8. Field design

1. **Input Authorization:**

Input authorization verifies that all transactions have been authorized and approved by management. Authorization of input helps and ensures that only authorized data are entered into the computer system for processing by applications. Authorization can be performed online at the time when the data are entered into the system. A computer-generated report listing the items requiring manual authorization also may be generated. It is important that the controls exist throughout processing to ensure that the authorized data remain unchanged. This can be accomplished through various accuracy and completeness checks incorporated into an application design.

Types of authorization includes:

- Signatures on batch form provide evidence of proper authorization.
- Online access controls ensure that only authorized individual may access data or perform sensitive functions.
- Unique passwords are necessary to ensure that access authorization can not be computerized through use of another individual’s authorized data access. Individual password also provides accountability for data changes.
- Terminal or client workstation identification can be used to limit input to specific terminals or workstations as well as to individuals. Terminals in a client workstation in a network can be configured with a unique form of identification such as serial numbers or computer names that is authorized by the system.
- Source documents are the forms used to record the data. A source document can be a piece of paper, a turned around document or an image displayed for online displayed for online data input. A well-designed source document achieves several purposes, it increase the speed and accuracy with which the data can be recorded, controls workflow, facilities the preparation of data in machine readable form for pattern recognition devices, increases the speed and accuracy with which data can be read and facilities subsequent reference checking.

2. **Batch control and balancing:**

Batch control group transactions in order to provide control totals. The batch control can be based on total monetary amount, total items, and total documents or hash totals.

Batch header forms are a data preparation control. All input forms should be clearly identified with the application names and transaction codes. Where possible, predetermined and pre-numbered forms with transaction identification codes and other constant data items are recommended. This would help ensure that all pertinent data has been recorded on the input forms and can reduce data recording/entry errors.

Types of batch controls include;

- **Total monetary amount**— verification that the total monetary value of the items processed equals the total monetary value of the batch document. E.g., the total monetary value of the sales invoices in the batch agrees with the total monetary value of the sales invoices processed.
- **Total items**— verification that total number of items included on each document in the batch agrees to the total number of items processed. E.g. total number of units ordered in the batch of invoices agrees with the total numbers of units processed.
- **Total documents**— verification that the total number documents in the batch equals total number of documents processed. E.g. the total number of the invoices in the batch agrees with the total number of invoices processed.
- **Hash totals**— Verification that a predetermined numeric field existing for all documents in a batch agrees with the total of documents.

Batch balancing can be performed through manual and automated reconciliation. Batch totaling must be combined with adequate follow up procedures. Adequate control should exist to ensure that each transaction create an input document, all documents are included in a batch, all batches are submitted for processing, all batches are accepted by the computer, batch reconciliation is performed, procedure for investigation and timely correction of differences are followed and controls exist over the resubmission of rejected items.

Types of batch balancing include:

- **Batch registers**— the registers enable manual recording of batch totals
- **Control accounts**— Control account use is performed through the use of an initial edit file to determine batch totals. The data are then processed to the master and reconciliation is performed between the total processed during initial edit file and the master file.
3. **Error Reporting Handling**:

Input processing requires that controls be identified to verify that the data are accepted into the system correctly, and that input errors are recognized and corrected. Data conversion error corrections are needed during the data conversion process. Error can occur due to duplication of transaction and inaccurate data entry. These errors can in turn greatly impact the completeness and accuracy of the data. Correction to data should be processed through normal data conversion process and should be verified, authorized, and reentered to the system as a part of normal processing.

Input error handling can be processed by:

- **Rejecting only transaction with errors**—only transaction containing error would be rejected; the rest of the batch would be processed.
- **Rejecting the whole batch of transactions**—Any batch of transaction containing errors would be rejected for correction prior to processing.
- **Accepting batch in suspense**—any batch containing errors would not be rejected, however the batch would be posted to suspense pending correction.
- **Accepting batch and flagging error transactions**—any batch containing error would be processed; however, those transactions containing errors would be flagged for identification enabling subsequent error correction.

4. **Data Validation and Editing**

Procedures should be established to ensure that input data are validated and edited as close to the point of origination as possible. Pre-programmed input formats ensure that data are input to the correct field in the correct format. If input procedures allow supervisor overrides of data validation and editing, automatic logging should occur. A management individual who did not initiate the override should review this log.

Data validation identifies data errors, incomplete or missing data and inconsistencies among related data items. Front-end data editing and validation can be performed if intelligent terminals are used.

Edit control are preventative controls that are used in a program before data are processed. If the edit control is not in place or does not work effectively, the preventative control measures do not work effectively. This may cause processing of inaccurate data. Exhibit describes various types of data validation edits.

<table>
<thead>
<tr>
<th>Exhibit</th>
<th>Data Validation Edits and Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Edits</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Sequence check</td>
<td>The control number follows sequentially and any out of sequence or duplicated control numbers are rejected no noted on an exception report for follow-up purposes. For example, invoices are numbered sequentially. The day’s invoices begin with 12001 and end with 15045. If any invoice larger than 15045 is encountered during processing, that invoice would be rejected as an invalid invoice number.</td>
</tr>
<tr>
<td>Limit check</td>
<td>Data should not exceed a predetermined amount. For example, payroll checks should</td>
</tr>
<tr>
<td>Control Activity</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Not exceed US $4,000.00. If a check exceeds US $4,000.00, the data would be rejected for further verification/authorization.</td>
<td></td>
</tr>
<tr>
<td><strong>Range check</strong></td>
<td>Data should be within a predetermined range of values. For example, product type codes range from 100 to 250. Any code outside this range should be rejected as an invalid product type.</td>
</tr>
<tr>
<td><strong>Validity check</strong></td>
<td>Programmed checking of the data validity in accordance with predetermined criteria. For example, a payroll record contains a field for material status and the acceptable status codes are M or S. If any other code is entered the record should be rejected.</td>
</tr>
<tr>
<td><strong>Reasonableness check</strong></td>
<td>Input data are matched to predetermined reasonable limits or occurrence rates. For example, in most instances, a widget manufacturer usually receives orders for no more than 20 widgets. If an order for more than 20 widgets is received, the computer program should be designed to print the record with a warning indicating that the order appears unreasonable.</td>
</tr>
<tr>
<td><strong>Table look-ups</strong></td>
<td>Input data complies with predetermined criteria maintained in a computerized table of possible values. For example, the input clerk enters a city code of 1 to 10. This number corresponds with a computerized table that matches the code to a city name.</td>
</tr>
<tr>
<td><strong>Existence check</strong></td>
<td>Data are entered correctly and agree with valid predetermined criteria. For example, a valid transaction code must be entered in the transaction code held.</td>
</tr>
<tr>
<td><strong>Key verification</strong></td>
<td>Keying in process in repeated by a separate individual using a machine that compares the original keystrokes to the repeated keyed input. For example, the worker number is keyed twice and compared to verify the keying process.</td>
</tr>
<tr>
<td><strong>Check digit</strong></td>
<td>A numeric value that has been calculated mathematically is added to data to ensure that the original data have not been altered or an incorrect but valid value substituted. This control is effective in detecting transposition and transcription errors. For example, a check digit is added to an account number so it can be checked for accuracy when it is used.</td>
</tr>
<tr>
<td><strong>Completeness check</strong></td>
<td>A field should always contain data and not zeros or blanks. A check of each byte of that field should be performed to determine that some form of data, not blanks or zeros, is present. For example, a worker number on a new employee record is left blank. This is identified as a key field and the record would be rejected, with a request that the field be completed before the record is accepted for processing.</td>
</tr>
<tr>
<td><strong>Duplicate check</strong></td>
<td>New transactions are matched to those previously input to ensure that they have not already been entered. For example, a vendor invoice number agrees with previously recorded invoices to ensure that the current order is not a duplicate and therefore, the vendor will not be paid twice.</td>
</tr>
<tr>
<td><strong>Logical relationship check</strong></td>
<td>If a particular condition is true, then one or more additional conditions or data input relationships may be required to be true and consider the input valid. For example, the hire date of an employee may be required to be more than sixteen years past his or her date of birth.</td>
</tr>
</tbody>
</table>
5. **Source document design.**

Source documents are documents that are used to capture data that will be recorded into the computer. It must be designed in such a way that it reduces the instance of error at the very beginning, increases the speed with which data can be recorded, facilitates data entry and increases accuracy and efficiency where pattern recognition devices are used. It involves the following activities:

- Use of pre-numbered printed forms
- Provide titles, headings, notes and instructions
- Arrangement of fields for ease of use
- Use of captions
- Use of MCQs and default or most common values

6. **Data entry screen design.**

If data is keyed into terminals a high quality design is important to ensure that appropriate controls are in place to avoid fraud and errors. Following must be considered in this regard:

- The organization of components on a screen must follow some logical grouping consistency and symmetry
- It must match with the sequence of fields as presented in data capture forms
7. **Caption design.**

Caption indicates the nature of data that is to be entered in the fields. Usually it is written on the right hand side or above data fields. Following must be ensured:

- It must be fully spelled out
- Abbreviations should be avoided
- Caption must be distinguished from each other and data fields
- It must be in simple language and use of computer jargon should be avoided
- It must precede the data field to which it relates

8. **Data entry Field design.**

These are the fields in which users will enter the data. Following must be ensured in designing such fields:

- Where data such as dates is entered the format mask must be specified e.g. DD/MM/YYYY
- Automatic tabbing or skipping of fields should be avoided unless fields are of predefined size e.g. dates.
- Use of different colours should be adopted to differentiate groups of related fields.

12.1.2 **Processing Control Procedures**

Processing controls ensure the completeness and accuracy of accumulated data. They ensure that data on a file/database remains complete and accurate until changed as a result of authorized processing or modification routines.

The following are processing control techniques that can be used to address the issues of completeness and accuracy of accumulated data.

- **Manual recalculations** - A sample of transactions may be recalculated manually to ensure that processing, is accomplishing the anticipated task.

- **Editing** - An edit check is a program instruction or subroutine that tests for accurate, complete and valid input and updates in an application.

- **Run-to-run totals** – Run-to-run totals provide the ability to verify data values through the stages of application processing. Run-to-run total verification ensures that data read into the computer was accepted and then applied to the updating process.

- **Programmed controls** – Software can be used to detect and initiate corrective action for errors in data and processing. For example, if the incorrect file or file version is provided for processing, the application program could display messages instructing that the proper file and version be used.

- **Reasonableness verification of calculated amounts** – Application programs can verify the reasonableness of calculated amounts. The reasonableness can be tested to ensure appropriateness to predetermined criteria. Any transaction that is determined to be unreasonable may be rejected pending further review.

- **Limit checks on calculated amounts** – An edit check can provide assurance through the use of predetermined limits that calculated amounts have not been keyed incorrectly. Any transaction exceeding the limit may be rejected for further investigation.

- **Reconciliation of file totals** – Reconciliation of file totals should be performed on a routine basis. Reconciliations may be performed through use of a manually maintained account, a file control record or an independent control file.
• **Exception reports** – An exception report is generated by a program that identifies transactions or data that appear to be incorrect. These items may be outside a predetermined range or may not conform to specified criteria.

1. **DATA FILE CONTROL PROCEDURES**

File controls should ensure that only authorized processing occurs to stored data.

Types of control over data files are shown in exhibit.

<table>
<thead>
<tr>
<th>Exhibit</th>
<th>Data File Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Method</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td><strong>Before and after image reporting</strong></td>
<td>Computer data on a file prior to and after a transaction is processed can be recorded and reported. The before and after images make it possible to trace the impact transactions have on computer records.</td>
</tr>
<tr>
<td><strong>Maintenance error reporting and handling</strong></td>
<td>Control procedures should be in place to ensure that all error reports are properly reconciled and corrections are submitted on a timely basis. To ensure segregation of duties, error corrections should be properly reviewed and authorized by personnel who did not initiate the transaction.</td>
</tr>
<tr>
<td><strong>Source documentation retention</strong></td>
<td>Source documentation should be retained for an adequate time period to enable retrieval, reconstruction or verification of data. Policies regarding the retention of source documentation should be enforced. Originating departments should maintain copies of source documentation and ensure that only authorized personnel have access. When appropriate, source documentation should be destroyed in a secure, controlled environment.</td>
</tr>
<tr>
<td><strong>Internal and external labelling</strong></td>
<td>Internal and external labelling of removable storage media is imperative to ensure that the proper data are loaded for processing. External labels provide the basic level of assurance that the correct data medium is loaded for processing. Internal labels, including file header records, provide assurance that the proper data files are used and allow for automated checking.</td>
</tr>
<tr>
<td><strong>Version usage</strong></td>
<td>It is critical that the proper version of a file be used as well as the correct file, for processing to be correct. For example, transactions should be applied to the most current database while restart procedures should use earlier versions.</td>
</tr>
<tr>
<td><strong>Data file security</strong></td>
<td>Data file security controls prevent unauthorized access by unauthorized users that may have access to the application to alter data files. These controls do not provide assurances relating to the validity of data, but ensure that unauthorized users who may have access to the application cannot improperly alter stored data.</td>
</tr>
<tr>
<td><strong>One-for-one checking</strong></td>
<td>Individual documents agree with a detailed listing of documents processed by the computer. It is necessary to ensure that all documents have been received for processing.</td>
</tr>
<tr>
<td><strong>Pre-recorded input</strong></td>
<td>Certain information fields are pre-printed on blank input forms to reduce initial input errors.</td>
</tr>
<tr>
<td><strong>Transaction logs</strong></td>
<td>All transaction activity is recorded by the computer. A detailed listing including date of input, time of input, use------- and terminal location can then be generated to provide an audit trail. It also permits operations personnel to determine which transactions have been posted. This will help to decrease the research time needed to investigate exceptions and to decrease recovery time if a system failure occurs.</td>
</tr>
</tbody>
</table>
| **File updating and maintenance** | Proper authorization for file updating and maintenance is necessary to ensure that stored data are adequately safeguarded, correct and up-to-date. Application programs may contain access restrictions in addition to the overall system access restrictions. The
Authorization

Additional security may provide levels of authorization as well as to providing an audit trail of file maintenance.

Parity checking

Data transfers in a computer system are expected to be made in a relatively error-free environment. However, when programs or vital data are transmitted, additional controls are needed. Transmission errors are controlled primarily by error detecting or correcting codes. The former is used more often because error-correcting codes are costly to implement and are unable to correct all errors. Generally, error detection methods such as a check bit and redundant transmission are adequate. Redundancy checking is a common error detection routine. A transmitted block of data containing one or more records or messages is checked for number of characters or patterns of bits contained in it. If the numbers or patterns do not conform to predetermined parameters, the receiving device ignores the transmitted data and instructs the user to retransmit. Check bits are often added to the transmitted data by the telecommunications control unit and may be applied either horizontally or vertically. These checks are similar to the parity checks normally applied to data characters within on premises equipment. A parity check on a single character generally is referred to as a vertical or column check and a parity check on all the equivalent bits is known as a horizontal, longitudinal or row check. Use of both checks greatly improves the possibilities of detecting a transmission error which may be missed when either of those checks is used alone.

12.1.3 OUTPUT CONTROLS

Output controls provide assurance that the data delivered to users will be presented, formatted and delivered in a consistent and secure manner.

Output controls include the following:

- **Logging and storages of negotiable, sensitive and critical forms in a secure place** – Negotiable, sensitive or critical forms should be properly logged and secured to provide adequate safeguards against theft or damage. The form log should be routinely reconciled to inventory on hand and any discrepancies should be properly researched.

- **Computer generation of negotiable instruments, forms and signatures** – The computer generation of negotiable instruments, forms and signatures should be properly controlled. A detailed listing of generated forms should be compared to the physical forms received. All exceptions, rejections and mutilations should be accounted for properly.

- **Report distribution** – Output reports should be distributed according to authorized distribution parameters which may be automated or manual. Operations personnel should verify that output reports are complete and that they are delivered according to schedule. All reports should be logged prior to distribution. In most environments, processing, output is spooled to a buffer or print spool upon completion of job processing where it waits for an available printer. Controls over access to the print spools are important to prevent reports from being accidentally deleted from print spools or directed to a different printer. In addition, changers to the output print priority can delay printing of critical jobs. Access to distributed reports can compromise confidentiality. Therefore, physical distribution of reports should be adequately controlled. Reports containing sensitive data should be printed under secured, controlled conditions. Secured output drop-off points should be established. Output disposal also should be adequately secured to ensure that no unauthorized access may be considered. Logical access to these reports also should be carefully controlled and subject to authorization.

- **Balancing and reconciling** – Data processing application program output should be routinely balanced to the control totals. Audit trails should be provided to facilitate the tracking of transaction processing and the reconciliation of data.
• **Output error handling** - Procedures for reporting and controlling errors contained in the application program output should be established. The error report should be timely and delivered to the originating department for review and error correction.

• **Output report retention** – A record retention schedule should be firmly adhered to. Any governing legal regulations should be included in the retention policy.

• **Verification of receipt of reports** – To provide assurance that sensitive reports are properly distributed, the recipient should sign a log as an evidence receipt of output.

### 12.2 Communication Controls

A communications infrastructure is a collection of devices and procedures for communicating signals in the form of a message between a sender and receiver. Transmission components and message commutation/switching techniques are used to reach the final destination. The transmission components (links or communication lines) define the real means of transmission and the data encoding, or channelling techniques, such as multiplexing used for data transport. The switching components (nodes) include data transmission and reception devices and use circuits or packet switching techniques. Such an infrastructure facilitates an operating system’s communications with users who are either internal or external to an organization.

Telecommunication networks, particularly data networks, generally vary widely in their design, configuration and purpose. The following are the most common components:

• **Modems** (modulators/demodulator) are data communications equipment (DCE) devices that provide connections for computers over a telecommunication network (generally the public telephone network). Modems convert computer digital signals into analog data signals that can be transmitted along the telecommunication lines. A modem on the other end of the line or link then convert the analog signal back into a digital signal.

• **Multiplexers** are devices that use several communication channels at the same time. A multiplexer allows a physical circuit to carry more than one signal at one time when the circuit has more capacity (bandwidth) than required by individual signals. It transmits and receives message and controls the communication lines to allow multiple users access to the system. It can also link several low-speed line to enhance transmission capabilities.

• **Protocols converters** are devices used to convert from one protocol to another, such as between asynchronous and synchronous transmission.

• **Spooling** is process that allows more efficient use of output devices. A device creates spool files representing virtual output devices so that write operations to a device, such as a printer, can occur without having the physical device available. The spool files will be processed when the physical device is available. Spooling is used because output devices often work at slower speeds than processing devices.

• **Buffers** are a temporary storage area (used by spooling) to compensate for different rates of data flow when transmitting data from one device to another, such as from a computer to a printer.

Devices that can be integrated into the system to extend the network include the following:

• **Repeaters** – Devices that regenerate and propagate electrical signals between two network segments

• **Hubs** – Generally are devices that serve as the center of a star-topology network (also used as a concentrator, a device that concentrates the traffic of a LAN). Hubs can be active (where
they repeat signals sent through them) or passive (where they do not repeat, but merely split, signal sent through them).

- **Bridges** – Devices that connect two separate networks to form a logical network (e.g., joining an Ethernet and token network). This hardware device must have storage capacity to store frames and act as a store and forward device.

- **Switch** – Bridges have been replaced by switches, which provide a method for building bridges. The main differences between switches and bridges are in the number of ports (switches can have a large number of them), internal speed (thousands, and in some cases, millions of frames can be filtered and forwarded per second by switches) and in presentation (switches may have different speed ports and may have switchable or shareable ports).

- **Routers** – Switching devices, by examining the IP address, can make intelligent decisions to direct the packet to its destinations,

- **Brouters** – Devices that perform the functions of both bridges and routers are called brouters.

- **Gateways** – Devices that are protocol converters. Typically, they connect and convert between LANs and mainframe or between LANs and the Internet. Depending on the type of gateway the operation occurs in various OSI layers. The most common from of gateway is a SNA gateway, converting between a TCP/IP, Net Bios session (emulating a 3270 terminal) and the mainframe.

### 12.2.1 Transmission Media

Common transmission media are:

- Copper (twisted pair) circuits, which are two insulated wires twisted around each other. One wire carries electricity to the telephone or modem and the other carries electricity away from the telephone or modem.

- Coaxial cables, which have a higher capacity than twisted pairs. A single coaxial cable can carry many voice, data and video signals at one time.

- Fiber optic system, which use glass fibers to carry binary signals as flashed of light. Fiber optic systems have low transmission loss as compared to twisted pairs. The speed of operation is that of light.

- Microwave radio system, which are used by line-of-sight carrier systems to carry large quantities of voice and data signals. Microwave radio waves are transmitted through the air. Most common carrier microwave systems carry analog signals.

- Satellite radiolink systems, which contain several receiver/amplifier/transmitter sections called transponders. Each transponder operates at a slightly different frequency. Like microwave, satellite signals can be affected by weather.

The following can degrade a signal during transmission:

- **Attenuation** ---- As a signal propagates along a transmission medium, its amplitude decreases. This is especially apparent when the medium is copper wire. Amplifiers, also known as repeaters, are used to counteract this effect.

- **Delay distortion** ---- The rate of propagation of a signal along a transmission line varies with the frequency of the signal. Consequently, when transmitting a digital signal with varying frequency components, the various components arrive at the receiver with varying frequency components, the various components arrive at receiver with rate of transmission and can result in misinterpretation of the signal.

- **Noise** ---- In the absence of a signal, a transmission line should ideally have zero electrical signal present. However, there is generally a small amount of electrical fluctuation even in the absence of a signal. When the power of the noise is high, it can interfere with the interpretation
of the signal by the electrical coupling between adjacent lines causes the signal in one wire to be picked up by the signal in the adjacent wire.

It is very easy for electrical signals representing a bit stream to be changed by electromagnetic interference. This means that a binary 1 could be misread as a binary 0 or vice versa. Two techniques are used to detect and correct errors:

- **Forward error control**—Additional redundant information is transmitted with each character or frame so that the receiver can not only detect when errors are present, but can also determine where the error has occurred and thus correct it.
- **Feedback (backward) error control**—Only enough additional information is transmitted to allow the receiver to identify that an error has occurred. An associated retransmission control scheme is then used to request that another copy of the information be sent.

Error detection methods include:

- **Parity check**—The transmitter adds an additional bit to each character prior to transmission. The parity bit used is a function of the bits making up the character. The recipient performs the same function on the received character and compares it to the parity bit. If it is different an error is assumed.
- **Block sum check**—It is an extension of the parity check in that an additional set of parity bits is computed for a block of characters (or frame). The set of parity bits is known as the block (sum) check character.
- **Cyclic redundancy check (CRC)**—The CRC or frame check sequence (FCS) is used for situations where bursts of errors may be present (parity and block sum checks are to effective at detecting burst of errors). A single set of check digits is generated for each frame transmitted, based on the contents of the frame, and appended to the tail of the frame.

### 12.2.2 Subversive threats

Such threats include attempts by intruders to violate the data or system integrity. The messages transmitting through the network mediums may also be tapped or impaired before they reach their destination. Following controls may be used to avoid subversive threats:

- **Link encryption.** It involves the encryption of messages by the sending node and decryption by the receiving node.
- **End to End encryption.** This involves the encryption of data by sender and its decryption by receiver.
- **Message Authentication Code (MAC).** Similar to check digits it involves the creation of secret key using specific algorithm (DEC algorithm) using specific data characteristics. It is used in electronic fund transfer system.
12.3 DATABASE CONTROLS

12.3.1 Exposure to failure

Databases are vulnerable to failure due to following reasons.

- **Application program error.** Application program can update data incorrectly because it contained a bug.
- **System software error.** Error may be in the operating system, DBMS, network management system or a utility program. The error may lead erroneous update or corruption of data held by the database.
- **Hardware Failure.** Data may be lost due to hardware failure or malfunctioning.
- **Procedural error.** Procedural error can be made by the operator that can damage the database.
- **Environmental Disaster.** Such as flood, sabotage etc.

12.3.2 Control procedures

It is critical that database integrity and availability be maintained. The following are some of the controls to ensure database integrity:

- Establish definition standards and closely monitor for compliance.
- Establish and implement data back-up and recovery procedures to ensure database availability.
- Establish various levels of access controls for data items, tables and files to prevent inadvertent or unauthorized access.
- Establish controls to ensure only authorized personnel can update the database.
- Establish controls to handle concurrent access problems, such as multiple users desiring to update the same data elements at the same time.
- Establish controls to ensure accuracy, completeness and consistency of data elements and relationships in the database. It is important that these controls, if possible, be attached to the table/columns. In this way, they will be active when specialized tools (not the application) are used to manipulate data.
- Use database checkpoints at points in the job stream that minimize data loss and recovery efforts to restart processing after a system failure.
- Perform database reorganization to reduce unused disk space and verify defined data relationships.
- Follow database restructuring procedures when making logical, physical and procedural changes.
- Use database performance monitoring tools to monitor and maintain database efficiency (available storage space buffer size, CPU usage, disk storage configuration and deadlock conditions).
- Minimize the ability to use non-system means, for instance, those outside security control, to access the database.
1. **Backup strategies**

In order to avoid the total loss of data organization must follow a backup strategy. There are different backup strategies available; some of them are as follows:

- **Grandfather Father Son strategy.** This involves maintaining two historical backups. For example if a current version of master file (Son) is corrupted it can be recovered from its previous version (Father). If however, during the backup the previous version also gets corrupted we still have an older version (Grandfather) to reconstruct the previous version (Father).

- **Mirroring.** This involves maintaining two separate copies of the same database. This technique is offered by most database management systems. It is also known as replication.

- **Dumping.** This involves the copying of whole or critical part of the database to a medium from which it can be rewritten. Both physical and logical dumps can be created. Dump can be automatically created in the event of failure or corruption by most of the DBMS.

- **Logging.** It involves logging all the events that update, create or delete any record in the database.

12.4 **GENERAL CONTROLS PROCEDURES**

There are many control activities that are of general nature and apply to more than one of above:

1. **Asset safeguards: limitation of access to assets**

As already mentioned, an important element of segregation of duties is to separate the physical control of assets. Consider an Inventory system. In manual systems there would have been bookkeepers that recorded the transactions for sales and purchases and these would then link to the inventory system, which may have been kept by yet another clerk. Then there would have been the warehouse staff that stored and moved the actual stock.

In today’s environment there is likely to be a terminal in the warehouse that is used for data entry that is operated by warehouse staff. The purchasing and sales systems may be fully automated with little operator intervention. It is now much easier for people in the warehouse to cover any stock losses without anyone else noticing.

To combat this the auditor should be looking out for these types of segregation problems look at ways to combat them. This may require other managers to be sent various reports such as stock losses rather than the warehouse managers. See the next section also.

2. **Physical count**

This type of checking can also help overcome the lack of segregation of duties. This type of check is not so much to verify that the computer system is working but rather to verify that what the books believe exist does actually exist. This control can be applied to all types of asset ranging from petty cash floats to inventory or major assets such as computers, cars and machinery,

3. **Audit trails**
As the data is stored electronically it may be difficult to trace transitions from the detail to the summary. For example a report may claim to show total sales for the month but there is no way to check manually that every single invoice has been included unless each transaction is logged. The ability to rack transactions through various reports is known as the audit trial. In traditional paper based systems the trail was often very visible. In computer systems it may be necessary to run additional software to separately verify the completeness of the figures.

4. **Error identification/investigation/correction/tracking**

There are controls that have as their main purpose the reporting of an error. For example, as an invoice is received the system checks the quantity on invoice with the quantity already recorded in the goods received database. If the amounts do not agree then the invoice may be rejected or accepted but flagged as an error. Someone should follow this up.

It is essential that the control procedures identify a method for regularly investigating these types of exception and also that there is documentary evidence that a final decision was made or a revised transaction was processed.

However, it is recommended that the control procedures be extended to consider other errors and exceptions that may arise.

Generally speaking people will not complain if you either:

- undercharge them or
- pay them too much

But they will complain if you:

- overcharge them or
- pay them too little.

So the only complaints that an organization will receive will be the ones that will cost it money. For example, goods are shipped to company A but the invoice is sent to company B. when B gets a statement asking for payment they will refuse to pay. Meanwhile A is keeping quiet and most unlikely to contact the organization to complain about not being charged for the goods.

In response to the complaint from B someone investigates the matter and agrees that B should not have the invoice and so issues a credit note. The matter should not stop there since the invoice should now be reissued to A.

A good system of control will deep drill record of such incidents and record how they were resolved and show that the organization did not lose money. Not only should there be an investigation as to how the error occurred in the first place, but are there other companies and transactions also in error, and what processes need to be changed to ensure that it does no happen again.

5. **Program security techniques**

When we consider program security we identify two main types of programs – operating systems and application programs. Usually auditors have been concerned with application programs and, especially when the application is developed in-house, have tried to apply control procedures to secure the data the application maintains.
I. Operating Systems

However, there have been well publicized reports of security problems with common operating systems especially Windows based. One reason for the auditors to now look at the operating system is that it provides more capabilities than it ever used to. It is in fact difficult to separate extra applications and utilities that are bundled into the operating system. For example with Microsoft XP you also get:

- Multimedia and video conferencing
- Collaboration tools
- Encryption
- Remote assistance so someone else can take over a computer
- Internet Information Services (IIS) to build web sites

Because Microsoft software is so widely used it becomes a target for hackers. While detailed analysis of the internal operation of the operating system is too detailed for most auditors it is important that the operating system now be considered a risk. Generally speaking the organization (and auditors) should regularly check with the operating system vendor and install the latest fixes and patches that are available.

II. Application Programs

As regards the application programs the controls should ensure that the integrity and reliability of the data is not compromised. After all this is a basic control objective. There will be many controls built into the language that is used to develop the application and also the way the application operates. For example if a variable is defined as numeric or a data field then users should not be able to put in text to that field.

There are some controls that the auditors may need to verify:

- Overflow or large numbers need to be handled correctly. Are the field types and character sizes large enough?
- Can a reasonableness test be applied? For example are the calculated invoice values within a standard range?
- Are there check totals that have been independently calculated?
- Do files have control totals on them that can be checked as processing progresses?
- Does the system handle rounding correctly? There is the famous fraud case of the programmer who stole all the small interest rounding.
- Is a log file produced?

In many cases the actual review and audit of the software will need to be undertaken with the assistance of a specialist IT auditor.
6. **Monitoring and surveillance techniques**

An important control has always been management supervision. In manual systems the document flow usually went up the chain of command and managers would see the work of their subordinates and hopefully identify any errors or problems.

At one extreme, as part of physical security, it is possible to install surveillance cameras. These are most likely to be a deterrent to thieves and could be installed in warehouses or other areas that contain valuable assets. More subtle is the use of IT systems to monitor user activity. There is a privacy issue here and local laws and regulations must be adhered to but it could be possible to track an employee’s movements especially if they use a magnetic and to enter various parts of the building.

More common is the tracking or monitoring of IT usage and data access. This may be in the form of a log file that records the user id, the time of access and the action that was taken. In many cases these logs are only used if something goes wrong and the organization is trying to trace the problem. These logs may be used to identify actions taken by staff accessing the system remotely or after hours.

It is possible or set alerts on a system so that if a particular event takes place someone is notified immediately. For example unauthorized access to the payroll system could trigger an alert that notifies and IT manager who could then identify the terminal and then check who is physically attempting the action.
Practice Questions

Q no 1) Even if the policy states that staff should behave ethically, how could you confirm that they are?

Q no 2) Categorise the following controls as preventative or detective:
1. encryption
2. setting file permissions
3. help facilities
4. batch control
5. audit trails
6. check digits
7. log files
8. printing internal tables

Q no 3) Users often complain about having to think about passwords and so will use easy to guess words. Describe ways of selecting an easy to remember but hard to guess password.

Q no 4) List the advantages of using batch controls over data entry.

Q no 5) A manager may review the log of data access to check why employees have accessed data. This manager’s access will also be logged in this report so how can you control what the manager may have been up to?

Q no 6) What classification scheme could be used in the Institute of Chartered Accountants?

Q no 7) Describe security procedures that could apply to contractors working at a secure site.

Q no 8) Describe the database controls that you may want to use to control a payroll clerk’s access to employee information.

Q no 9) Increasingly networks are using open systems or popular protocols rather than proprietary systems. Why can this be a security weakness?

Q no 10) Visit the Microsoft site and identify any updates for the current operating system.

Q no 11) What are the issues with an organisation monitoring employee’s e-mail?

Suggested Solution

Answer no 1
Students should consider:

- What does “behave ethically” mean?
- Once specific instances have been identified then controls become easier to identify.
- Log files may record what and when data was accessed and these may be checked to see that there were valid reasons for access.
- User behaviour may be observed by managers and peers.
• Other controls such as over-ride controls may identify users that over or under charge customers.

**Answer no 2**

<table>
<thead>
<tr>
<th>Control</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption</td>
<td>P</td>
</tr>
<tr>
<td>Setting file permissions</td>
<td>P</td>
</tr>
<tr>
<td>Help facilities</td>
<td>P</td>
</tr>
<tr>
<td>Batch control</td>
<td>D</td>
</tr>
<tr>
<td>Audit trails</td>
<td>D</td>
</tr>
<tr>
<td>Check digits</td>
<td>D</td>
</tr>
<tr>
<td>Log files</td>
<td>D</td>
</tr>
<tr>
<td>Printing internal tables</td>
<td>D</td>
</tr>
</tbody>
</table>

There may be discussion as to whether some of these controls such as Batch Controls are Preventative or Detective. Strictly speaking a Preventative control stops an error getting into the computer. The objective of the exercise is to get students thinking about various controls not precisely categorising them.

**Answer no 3**

The solution could suggest:

• A short statement about what the user likes, e.g. I like golf.
• This could be refined with special characters and upper and lower case, e.g. I/like/Golf.
• Initials of a favourite film e.g. Gone with the Wind = GWTW.
• A favourite saying, e.g. 2bornot2b.
• It is essential that the user never discloses the method they have chosen.

**Answer no 4**

The solution should cover:

• Provides control totals for verification at end of batch run.
• Controls completeness of entry.
• Provides independent figures for balancing file.
• Keeps like transactions together, which improve input process.
• Errors can be restricted to a relatively small batch of transactions.

**Answer no 5**

Solution should cover:

• This has been a problem with manual systems as well as IT systems.
• One solution is for a higher manager to review but this is often impractical since these managers are normally too busy.
• Managers are often controlled by budgets and overall performance. So long as they meet their target the organisation is happy with their performance and may even turn a blind eye to minor errors and security lapses.
• The only time that this information is ever reviewed may be during an audit.
• Exception reporting may be used but again this needs to be reviewed by a senior manager.

**Answer no 6**

The solution could suggest:
• Public
• Members only
• Staff and Members
• Staff only
• Executive staff only

**Answer no 7**
The solution should consider:

• Are contractors to be treated as employees or guests?
• They need access rights such as badges and key cards.
• Do they need to travel around to do their work?
• Security clearance may need to be checked.
• Will they be allowed out-of-hours access?
• Will they use their own PCs and what is the restriction on copying and removing data.
• Do they need user accounts on the system?
• Are they also working at competitive companies?
• Is there a contract that they need to sign?
• Who is to be held responsible for them?

**Answer no 8**
The solution should suggest:

• The clerk may be restricted in the employees that they can view, i.e. not senior managers.
• The clerk may not be able to see all information about employees but only that which they need to know.
• There may be restrictions on peers that the clerk can access.
• There may be restrictions on the data that can be printed out as opposed to being available on a screen.

**Answer no 9**
The solution should discuss:

• Open systems have to be very well documented and this may reveal security flaws.
• Since so many organisations use the open system there is a great deal of knowledge about the system and statistically there will be more knowledgeable people with criminal intent.
• The fact that so many organisations use the system makes it a worthwhile target.
• While these are all weaknesses, one strength is the fact that should a weakness be discovered it is usually fixed very quickly.

**Answer no 10**
There is no solution for this question other than to see what are the current security issues at the time of presenting the course. But for example, at the time of writing there was a security fix for IE version 6 posted at:

Answer no 11
The main issues are:

- Amount of privacy that an employee expects.
- Have employees been told that the mail will be monitored?
- Who will be doing it and what type of information is being sought?
- How will the organisation verify that mail comes from an employee and not from someone posing as the employee?
- What are the rules for e-mail and penalties?
- What about mail that uses third party organisations such as hotmail?
14 Business Continuity/Disaster Recovery Planning

<table>
<thead>
<tr>
<th>Topic List</th>
<th>Syllabus Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>13.1 Disaster and other Disruptive Events</td>
<td>2.8</td>
</tr>
<tr>
<td>13.2 Business Impact Analysis (BIA)</td>
<td>2.8</td>
</tr>
<tr>
<td>13.3 Selection of Recovery Strategies</td>
<td>2.8</td>
</tr>
<tr>
<td>13.4 Components of an Effective Business Continuity Plan</td>
<td>2.8</td>
</tr>
<tr>
<td>13.5 Media and Documentation Backup</td>
<td>2.8</td>
</tr>
<tr>
<td>13.6 Recovery/Continuity Plan Testing</td>
<td>2.8</td>
</tr>
</tbody>
</table>

INTRODUCTION

STUDY GUIDE


The purpose of business continuity/disaster recovery is to enable a business to continue operations in the event of a disruption and to survive a disastrous interruption to their information systems. Rigorous planning and commitment of resources is necessary to adequately plan for such an event. Business continuity planning (BCP) is a process designed to reduce the organization’s risk for an unexpected disruption of its critical functions, on matter whether these are manual or automated ones, and assure continuity of minimum level of services necessary for critical operations. This planning’s is primarily the responsibility of senior management, as they are entrusted with the safeguarding of both the assets of the company and the viability of the company. This plan is generally followed business units to get by while recovery is taking place. The plan should address all function and assets required to continue as a viable
organization. This includes continuity procedures determined necessary to survive and minimize business interruption. Additionally, disaster recovery planning (DRP) is generally the plan followed by IS to recover an IT processing facility, or by business units to recover an operational facility. The IS recovery plan must be consistent with and support the overall plan of the organization.

Overall the concept, business continuity is equal to the combination of disaster recovery planning plus continuity of business operations.

13.1 Disaster and Other Disruptive Events

Disasters are disruption that cause critical information resources to be inoperative for a period of time that adversely impacts business operations, which could be anything from several hours to several days, depending upon the criticality of the information resource. Most importantly, disaster require action to recover operational status, which in a worst-case scenario, would entail use of an alternate processing facility, where restoration of software and data files from offsite copies may be required. It is necessary that the alternate facility be available until the original information processing facility is restored.

Example of disasters of a catastrophic nature are earthquakes, floods, tornadoes, severe thunderstones, file, etc. Other disastrous events causing disruption may occur when expected services are no longer supplied to the company, such as electrical power, telecommunications, natural gas supply or other delivery services (which may or may not be related to a natural disaster).

Additionally, not all critical disruption in service are classified as a disaster but still are of a high-risk nature. For example, disruption in service is sometimes caused by system malfunctions, accidental file deletions, network denial of service intrusions and viruses. These events may require action to be taken to recover operational status in order to resume service. Such actions may necessitate restoration of hardware, software of data files. Therefore, a well defined risk-based classification systems need to be in effect to make a determination to initialize business continuity planning efforts.

A good business continuity plan will take into account all types of events impacting both critical information systems processing facilities and end user normal business operation functions. For worse case scenarios, short-term and long-term fallback strategies are required. For the short term, an alternate processing facility may be needed to satisfy immediate operational needs, as in the case of a major natural disaster. In the long-term a new permanent facility must be identified for disaster recovery and equipped to provide for continuation system processing services on a regular basis.

13.2 Business Impact Analysis (BIA)

Prior to developing the plan, the criticality of information resources (applications, data, networks, system software, facilities, etc.) that support an organization’s critical business process must be determined. This is done through a business impact analysis. With senior management support, both information systems processing and end user personnel should participate in this analysis. Their analysis should include all types of information resources and look beyond traditional information resources (i.e. mainframe operations) to possibly include in a business continuity/disaster recovery planning. For example, many end user groups have installed sophisticated LANs and desktop workstation that perform critical function on a daily basis.

The business impact analysis will consider the following questions:
• What are the critical information resources related to an organization’s critical business process?

This is the first consideration because disruption to an information resource is not a disaster in itself, unless it is related to a critical business process due to an information organization losing its revenue generating business due to an information system failure. Other example of potential critical business processes may include:

- Receiving payments
- Production
- Paying employees
- Advertising
- Dispatching of finished goods

Each process needs to be assessed to determine if it is critically. Indications of criticality for example would include:

- The process supports lives, or people’s health and safety
- Disruption of the process would cause a loss of income to the organization or exceptional costs that are unacceptable.
- The process is required to meet legal or statutory requirements

• What is the critical recovery time period for information resources in which business processing must resumed before significant or unacceptable losses are suffered?

The cost of recovery facilities, however reduces if they are required less urgently. There is a breakeven point where the impact of the disruption will begin to be greater than the cost of recovery. The length of this time period depends on the nature of the business being disrupted. For instance, financial institutions, such as banks and brokerage firms will usually have a much shorter critical recovery time period than manufacturing firms. Also, the time of year or day of week may effect the window of time for recovery. For example, a bank experiencing a major outage on Saturday at midnight has longer time in which to recover than on Monday at midnight, based on the assumption the bank is not processing on Sunday.

• What is system risk ranking?

This involves a determination of risk based upon impact derived from the critical recovery timer period as well as the likelihood that an adverse disruption will occur. Many organizations will use a risk of occurrence to determine a reasonable cost of being prepared. For example, they may determine that there is a 0.1 percent risk (or 1 in 1000) that over the next five years the organization will suffer a serious disruption. If the assessed impact might be US $ 10 million then the maximum reasonable cost of being prepared might be US $ 10 million x 0.1 percent US $10,000 over five years. From this risk-based analysis process, prioritizing critical systems can take place in developing recovery strategies. The risk ranking procedure should be performed in coordination with both information systems processing and end user personnel.


## 13.3 Selection of Recovery Strategies

From the priorities and timescales assessed through the business impact analysis:

- Establish the disaster recovery strategies for IT and other facilities
- Determine the business activities that could take place while the facilities are being recovered.

There will be various strategies for recovering critical information resources. The appropriate strategy is the one with a cost of an acceptable recovery time that is also reasonable compared to the impact and likelihood of occurrence as determined in business impact analysis. The cost of recovery is the cost of preparing for possible disruption (i.e., purchasing, maintaining and regularly testing redundant computers and maintaining alternate network routing, etc.) as back insurance will usually be lower, if there is a suitable plan.

Generally each IT platform that runs an application supporting a critical business function will need a recovery strategy. There are many strategies. The most appropriate alternative in terms of speed to recover and recovery cost should be selected based on the relative risk level identified in the business impact analysis. For large mainframe and network facility operations, strategies based on the risk level identified for recovery to select from would include developing:

- Duplicate information processing facilities
- Hot sites
- Warm sites
- Cold sites
- Reciprocal arrangements with other companies

As data and software are required for these strategies, special arrangements need to be considered for their backup to removable media and their safe, secure storage offsite.

Additionally part of the recovery of IT facilities will involve telecommunications for which the strategies usually considered include:

- Network redundancy
- Alternative routing
- Diverse routing
- Long haul network diversity
- Protection of the local loop
- Voice recovery

These strategies are discussed in more detail later in this chapter.

Having developed a strategy for the recovery of sufficient IT facilities to support critical business processes, it is critical the strategies for these functions get by until all facilities are restored and therefore may include:

- Doing nothing until recovery facilities ready
Using manual procedures
- Focusing on the most important customers, suppliers, products, etc.
- Using PC based systems to capture data for later processing or to perform simple local processing

13.3.1 Other Issues in Plan Development

The personnel who must react to the disaster scenarios are those responsible for the most critical resources. Therefore, management and user involvement is vital to the success of the business continuity plan. User management involvement is essential to the identification of critical systems and their associated critical recovery times and the specification of needed resources. The three major divisions that require involvement in the formulation of the business continuity plan are support services, business operations, and information processing support.

Because the underlying purpose of business continuity planning is the resumption of business operations, it is essential to consider the entire organization, not just information systems processing services, when developing the plan. Where a uniform business continuity plan does not exist for the entire organization, the plan for information system processing should be extended to include planning for all divisions and units that are dependent upon information systems processing functions. Data processing plans must extend to the user areas to cover the sources of information, transmitted of data to the information system processing department and delivery and deployment of processed results to the user.

When formulating the plan, the following items should be included:

- A list of staff required to maintain critical business functions in the short, medium and long term
- The configuration of building facilities, desks, chairs, telephones, etc, required to maintain critical business functions in the short, medium and long term

13.4 Components of an Effective Business Continuity Plan

For the planning, implementation, and evaluation phase of the business continuity plan the following should be agreed upon:

- The goals/requirement/products for each phase
- Alternate facilities to perform tasks and operations
- Critical information resources to deploy (e.g., data and systems)
- Persons responsible for completion
- Available resources to aid in deployment (including human)
- Scheduling of activities with priorities established

Most business continuity plans are created as procedures which accommodate systems, user and network recovery strategies. Copies of the plan should be kept offsite, possibly that at the homes of key decision making personnel.

Components of this plan include
1. **Key Decision-making Personnel**

   The plan should contain a notification directory of key decision-making IS and end user personnel required to initiate and carry out recovery efforts. This is usually a telephone directory of people who should be notified in the event of a disaster or catastrophe.

   This directory should contain the following information:
   
   - Prioritized contacts, that is, who gets called first
   - Primary and emergency telephone numbers and address for each critical contact person. These will usually be key team leaders responsible for contacting the members of their team
   - Phone numbers and address for representatives of equipment and software vendors
   - Phone numbers of contacts within companies that have been designated to provide supply and equipment service
   - Phone numbers of contact person at recovery facilities, including hot site representatives or predefined network communication reporting services
   - Phone numbers of contact person at offsite media storage facilities and the contact persons within the company who are authorized to retrieve from the offsite facility
   - Phone numbers of insurance company agents
   - Phone numbers of contact’s at contract personnel services

2. **Backup of Required Supplies**

   The plan should contain all supplies necessary for the communication of normal business activities in the recovery effort. This includes detailed up-to-date hardcopy procedures that can be easily followed by contract personnel who are unfamiliar with standard operations. Also, a supply of special forms such as check stock, invoice forms and order forms should be secured at an offsite location.

   If the data entry function is dependent on certain hardware devices and/or software programs, these programs and equipment should be provided at the hot site including specialized EDI (electronic data interchange) equipment and programs.

3. **Organization And Assignment of Responsibilities**

   The plan should contain the teams with their assigned responsibilities in the event of a disaster. To implement the strategies that have been developed for business recovery, key decision making IS and user personnel should be identified. These individuals usually lead teams that have been created in response to a critical function or task defined in the plan, depending on the size of the business operation, these teams may be designated as single person positions.
The involvement of the following teams depends on the level of the disruption of service and the types of assets lost or damaged. It is good idea to develop a matrix on the correction between the teams to participate and the estimated recovery effort/level of disruption.

- **Emergency action team** - The first response team. They are designated fire wardens and back-up crews, whose function is to deal with fires or other emergency response scenarios. One of their primary function is the orderly evacuation of personnel and the securing of human life.

- **Damage assessment team** - Assesses the extent of damage following the disaster. The team should be comprised of individuals who have the ability to assess damage and estimate the time required to recover operations at the affected site. This team should include staff skilled in the use of testing equipment, knowledgeable about systems and networks and trained in applicable safety regulations and procedures. In addition, they have the responsibility of identifying possible causes of the disaster and their impact on damage and predictable downtime.

- **Emergency management team** - Responsible for coordinating the activities of all other recovery teams and handles key decision-making. They determine activation of the business continuity plan. Other functions entail arranging the finances of the recovery, handling legal matters evolving from the disaster and handling relations and media inquiries.

- **Offsite storage team** - Responsible for obtaining, packaging and shipping media and records to the recovery facilities, as well as establishing and overseeing an offsite storage schedule for information created during operations at the recovery site.

- **Software team** - Responsible for restoring systems packs, loading and testing operating systems software and resolving systems level problems.

- **Application team** - Travels to the system recovery site and restores user packs and application programs on the backup system. As the recovery progresses, this team may have the responsibility of monitoring application performance and database integrity.

- **Security team** - Continually monitors the security of systems and communication links, resolves any security conflicts that impede the expeditious recovery of the system, and assures the proper installation and functioning of the security software package.

- **Emergency operations team** - Consists of shift operators and shift supervisors who will reside at the system recovery site and manage system operations during the entirety of the disaster and recovery projects. Another responsibility might be coordinating hardware installation, if a hot site or other equipment-ready facility has not been designated as the recovery center.

- **Network recovery team** - Responsible for rerouting wide area voice and data communications traffic, reestablishing host network control and access at the system recovery site, providing ongoing support for data communications and overseeing communication integrity.

- **Communication team** - Travels to the recovery site where they work in conjunction with the remote network recovery team to establish a user/system network. This team also is responsible for soliciting and installing communication hardware at the recovery site and working with local exchange carriers and gateway vendors in the rerouting of local service and gateway access.

- **Transportation team** - Serves as a facilities team to locate a recovery site if one has not been predetermined and is responsible for coordinating the transport of company employees to a distant recovery site. They also may assist in contacting employees to inform them of new work locations and scheduling and arranging employee lodgings.

- **User hardware team** - Locates and coordinates the delivery and installation of user terminals, printers, typewriters, photocopiers and other necessary equipment. This team also offers support to the communication team and to any hardware and facilities salvage efforts.
• **Data preparation and records team**—Working from terminals installed at the user recovery site updates the applications database. This team also oversees contract data entry personnel and assists records salvage efforts in acquiring primary documents and other input information sources.

• **Administrative support team**—Provides clerical support to the other teams and serves as a message center for the user recovery site. This team also may control accounting and payroll functions as well as ongoing facilities management.

• **Supplies team**—Supports the efforts of the user hardware team by contacting vendors and coordinating logistics for an ongoing supply of necessary office and computer supplies.

• **Salvage team**—Manages the relocation project. This team also makes a more detailed assessment of the damage to the facilities and equipment than was performed initially; provides the emergency management team with the information required to determine whether planning should be directed towards reconstruction or relocation; provides information necessary for filling insurance claims (insurance is the primary source of funding for the recovery efforts) and coordinates the efforts necessary for immediate records salvage, such as restoring paper documents and electronic media.

• **Relocation team**—Coordinates the process of moving from the hot site to a new location or to the restored original location. This involves relocating the information systems processing operations, communication traffic and user operations. This team also monitors the transition to normal service levels.

4. **Telecommunication Network**

The plan should contain the organization’s telecommunication networks. Today telecommunication networks are key to business process in both large and small organizations therefore the procedures to ensure continuous telecommunication capabilities should be given a high priority. Telecommunication networks are susceptible to the same natural disasters as data centers, but also are vulnerable to several disastrous events unique to telecommunications. These include central switching office disasters, cable cuts, communication software glitches and errors, security breaches connected to hacking (phone hackers are known as phreakers) and a host of other human mishaps. It is the responsibility of the organization and not the local exchange carriers to ensure constant communication capabilities. The local exchange carrier is not responsible for providing backup services, through many do back up main components within their systems. Therefore, the organization should make provisions for backing up its own telecommunication facilities.

To maintain critical business processes, the information processing facilities business continuity plan should provide for adequate telecommunication capabilities. Telecommunication capabilities to consider include telephone voice circuits, wide area networks (connections to distributed data center), local area networks (wrong group PC connections) and third party electronic data interchange provides. The critical capacity requirements should be identified for the various thresholds of outage for each telecommunications capability, such as 2 hours, 8 hours or 24 hours. Uninterruptible power supplies should be sufficient to provide backup to the telecommunication equipment, as well as the computer equipment.

The methods of providing telecommunications continuity are:

• **Redundancy**—Involves providing extra capacity with a plan to use the surplus capacity should normal primary transmission capability not be available, in the case of a LAN, a second cable could be installed through an alternate route for use in the event the primary cable is damaged.

• **Alternative Routing**—The method of routing information via on alternate medium such its copper cable or fiber optics. This involves use of different networks, circuits or end points should be normal network be unavailable. Most local carriers are deploying counter rotating
fiver optic rings. These rings have fiber optic cables that transmit information in two different directions and in separate cable sheaths for increased protection. Currently, these ring connect through one central switching office. However, future expansion of the rings may incorporate a second central office in the circuit. Some carriers are offering alternate routes to different points of presence or alternate central offices. Other examples include a dialup circuit, as an alternative to dedicated circuits, a cellular phone and microwave communication, as an alternative of land circuits, as an alternative to electronic transmissions.

- **Diverse routing**—The method of routing traffic through split cable facilities or duplicate cable facilities. This can be accomplished with different and/or duplicate cable sheaths. If different cable sheaths are used, the cable may be in the same conduit and therefore subject to the same interruptions as the cable it backing up. The communication service subscriber can duplicate the facilities by having alternative routes, although the entrance to and from the customer premises may be in the same conduit. The subscriber can obtain diverse routing and alternate routing form the local carrier, including dual entrance facilities. However, acquiring this type of access is time-consuming and costly. Most carrier provide facilities for alternate and diverse routing, although the majority of services are transmitted over terrestrial media. These cable facilities are usually located in the ground or basement. Ground-based facilities are at great risk due to the aging infrastructures of cities. In addition, cable-based facilities usually share room with mechanical and electrical systems that can impose great risks due to human error and disastrous events.

- **Long haul network diversity**—Many recovery facilities vendors have provided diverse long distance network availability utilizing TI circuits among the major long-distance carriers. This ensure long-distance access should any one carrier experience a network failure. Several of the major carriers have now installed automatic re-routing software and redundant lines that provide instantaneous recovery should a break in their lines occur. The IS auditor should verify that the recovery facility has these vital telecommunications capabilities.

- **Last mile circuit protection**—Many recovery facilities provide a redundant combination of local carrier Tis microwave and/or coaxial cable access to the local communications loop. This enables the facility to have access during a local carrier communication disaster. Alternative local carrier routing is also utilized.

- **Voice recovery**—With many service, financial and retail industries dependent on voice communication, redundant cabling and alternative routing should be provided for voice communication lines as well as data communications lines.

### 5. Insurance

The plan should contain key information of the organization insurance. The information systems processing insurance policy is usually a multi peril policy designed to provide various types of IS coverage. Its should be modularly constructed so that it can be adapted to the insured’s particular IS environment.

- **Is equipment and facilities**—Provides coverage of physical damage to the information processing facility and owned equipment. (Insurance of lease equipment should be obtained when the lessee is responsible for hazard coverage.) The IS auditor is cautioned to review these policies since many policies are only obligated to replace nonrestorable equipment with “like kind and quality” not necessarily with new equipment by the same vendor as the damage equipment.

- **Media (software) reconstruction**—Covers damage to IS media that is the property of the insured and for which the insured may be liable. Insurance is available for on-premises, off-premises or in-transit situations and covers the actual reproduction cost of the property. Considerations in determining the amount of coverage needed are programming costs to reproduce the media damaged, backup expenses and physical replacement of media devices, such as tapes, cartridges and disks.

- **Extra expenses**—Designed to cover the extra costs of continuing operations following damage or destruction at the information processing facility. The amount of extra expense...
insurance needed is based on the availability and cost of backup facilities and operations. Extra expense can also cover the loss of net profits caused by computer media damage. This provides reimbursement for monetary losses resulting from suspension of operations. Coverage would be if the information processing facilities were on the sixth floor and the first five floors were burned out. In this case, operations would be interrupted even though the information processing facility remained unaffected.

- **Business interruption**—Covers the loss of profit due to the disruption of the activity of the company caused by any malfunction of the IS organization.

- **Valuable papers and records**—Cover actual cash value of valuable papers and records (not defined as media) on the insured’s premises against direct physical loss or damage.

- **Errors and omissions**—Provides legal liability protection in the event that the professional practitioner, commits an act, error or omission that results in financial loss to a client. This insurance was originally designed for service bureaus but is now available from several insurance companies for protection systems analysts, software designers, programmers, consultant and other IS personnel.

- **Fidelity coverage**—Usually takes the form of bankers blanket bonds, excess fidelity insurance and commercial blanket bonds, and covers loss from dishonest or fraudulent acts by employees. This type of coverage is prevalent in financial institution operating their own information processing facility.

- **Media transportation**—Provides coverage for potential loss or damage to media in transit to off-premises information processing facilities. Transit coverage wording in the policy usually specific that all documents must be timed or otherwise copied. When the policy does not specially state that data be filmed prior to being transported and the work is not filmed, management should obtain from the insurance carrier a letter that specifically describes the carrier’s position and coverage in the event data are destroyed.

6. **Recovery Alternatives**

Lengthier and more costly outages, particularly disasters that impair the primary physical facility, require offsite backup alternatives.

The types of offsite backup hardware facilities available are:

I. **Hot Site**

They are fully configured and ready to operate within several hours. The equipment and systems software must be compatible with the primary installation being backed up. The only additional needs are staff, programs, data files and documentation.

Costs associated with the use of a third party hot site are usually but are often cost justify for critical applications. When properly planned, insurance coverage will usually offset the costs incurred for using this type of facility. Costs include a basic subscription cost, monthly fee, activation costs for when the site is used for an actual emergency and hourly or daily use charges. Pricing structures vary between vendors. Some hot site supplies impose a high activation fee in order to discourage the frivolous use of the facility. Other vendors have no activation fee and encourage the use of the facility for non-disaster purpose such as overload processing.

The hot site is intended for emergency operation of a limited time period and not for long-term extended use. Long-term use would impair the protection of other subscribers. Therefore, the hot site should be viewed as a means of accomplishing the continuation of essential operations for a period of up to several
weeks following a disaster or major emergency further plans are still necessary to provide for subsequent operations.

Components of the disaster recovery plan for network connectivity to a hot site over a public-switched network should address such issues as redundancy and maintaining sufficient capacity on diverse paths to carry a rerouted path. It should also provide for late night access routing through different central offices, so no single point of failure can disable the entire network.

II. Warm Sites

They are partially configured with network connections and selected peripheral equipment, such as disk drives, tape drives and controller, but without the main computer. Sometimes a warm site is equipped with a less powerful CPU than the one generally use. The assumption behind the warm site concept is that the computer can usually be obtained quickly for emergency installation (provided it is a widely used model) and, since the computer is the most expensive unit, such an arrangement is less totally than a hot site. After the installation of the needed components the site can be ready for service within hours, however the location and installation of the CPU and other missing units could take several days or weeks.

III. Cold Sites

They have only the basic environment (electrical wiring, air conditioning, flooring, etc.) to operate an information processing facility. The cold site is ready to receive equipment but does not offer any components at the site in advance of the need. Activation of the site may take several weeks.

IV. Duplicate Information Processing Facilities

They are dedicated self-developed recovery sites that back up critical applications. They can range in form a standby hot site to a reciprocal agreement with another company installation. The assumption is that there are fewer problems in coordinating compatibility and availability in the case of duplicate information processing facility sites. However larger organizations may experience problems similar to those encountered by reciprocal agreements between unrelated companies. This is particularly true whenever departmental or divisional information processing facilities are managed separately or hostile in-house political jealousies exist. Several principle must be in place to ensure the viability of this approach.

The site chosen should be subject to the same natural disaster(s) as the original (primary) site:  
There must be coordination of hardware/software strategies. A reasonable degree of compatibility must exist to serve as basis for backup. 
Recourse availability must be assured. The workloads of the sites must monitored to ensure that availability for emergency backup use would not be impaired. 
Regular testing is necessary. Even though duplicate sites are under common ownership and even if the sites are under the same management, tasting of the backup operation is necessary.

V. Reciprocal Agreements

They are between two or more organizations with similar equipment or applications. under the typical agreement, participants promise to provide computer time to each other when an emergency arises.

Advantages
• Low cost
• May be the only option available because of unavailable hot sites due to unique vendor equipment.

Disadvantages
• Usually not enforceable
• Differences in equipment configuration often necessitate program changes to operate effectively
• Unmodified changes in workloads or equipment configuration render the agreement limited or useless

Critical question to cover in a Reciprocal Agreement
• How much time will be available at the host computer site?
• What facilities and equipment will be available?
• Will staff assistance be provided?
• How quickly can access be gained to the host recovery facility?
• Can data and voice communication links be established at the host site?
• How long can the emergency operation continue?
• How frequently can the system be tested for compatibility?
• How will confidentiality of data be maintained?
• What type of security will be afforded for information systems operations and data?
• How much advance notice is required for using the facility?
• Are there certain times of the year, month, etc. when the partner’s facility are not available?

VI. Procuring Alternative Hardware

There are several alternatives available for securing backup hardware and physical facilities.

• **Vendor or Third Party**—Hardware vendors are usually the best source for replacement equipment. However, this may often involve a waiting period that is not acceptable for critical operations. It is unlikely that any vendor will guarantee specific reaction to a crisis. Vendor arrangements are best utilized when planning to move from a hot site to a warm or cold site. The arrangements should be planned in advance. Another source of equipment replacement is the used hardware market. This market can supply critical components or entire systems on relatively short notice, often at a savings. These dealer relationships should be cultivated well in advance of the actual emergency.

• **Off the-shelf**—Such components are readily available from the inventory of suppliers on short notice and with minimum need for special arrangements. To make use of this approach, several strategies must be utilized, including:
  • Avoiding use of unusual and hard-to-get equipment
  • Regularly updating equipment to keep current
  • Maintaining software compatibility to permit operation of newer equipment
VII. Offsite Libraries

Because it is desirable to ensure that the profit-seeking activities of a business (including the IS operations in its supportive role) are not interrupted in the event of a disaster, secondary storage media (usually tape reels, tape cartridges, removable hard disks or cassettes) are used to store programs and associated data for backup purposes. These tapes or other secondary storage media are stored in one or more physical facility (referred to as offsite libraries) based on availability of time and perceived business interruption risk. It is the offsite librarian’s responsibility to maintain a perpetual inventory of the contents of these libraries, to control access to library media and to rotate media between various libraries as applicable.

13.5 Media and Documentation Backup

A crucial element of a business continuity onsite or offsite recovery plan is the availability of adequate data. Availability of important data and documentation, including offsite storage of such backup data and documentation, is a prerequisite for any type of recovery plan.

Copies of data taken for offsite backup must be given the same level of security as the original files. The offsite facility and transportation arrangements must therefore meet the security requirements for the most sensitive class of data on the backup media.

13.5.1 Periodic Backup Procedures

Both data and software files should be backed up on a periodic basis. The time period in which to schedule the backup may differ per application program or software system. For instance, certain application systems that run on a monthly basis in which master or transaction files are updated will require that the backup be scheduled after the monthly production run.

Scheduling the periods backup can often be accomplished via an automated tape management system and automated job scheduling software. Automating the backup procedures will prevent any missed backup cycles due to operator errors.

Backup for data and software must allow for the continuing occurrence of change. A copy of the file or record as of some point in time is retained for backup purposes. All changes or transactions that occur during the interval between the copy and the current time also are retimed.

Consideration for establishing file backup schedules:

- Frequency of backup cycle and depth of retention generations must be determined for each data file.
- Backup strategy must anticipate failure at any step of the processing cycle.
- Master files should be retained at appropriate intervals such as the end of an updating procedure to provide synchronization between files and system.
- Transaction files should be presented to coincide with master files, so a prior generation of a master file can be brought completely up to date to recreate a current master file.
• Real-time files require special backup techniques, such as duplicate logging of transactions use of before and/or after images of master records time stamping of transactions and communication simulation.

• Database management systems (DBMS) require specialized backup usually provided as an integral feature of the DBMS.

• File descriptions need to be maintained to coincide with each version of a file that is retained for DBMS systems this may entail keeping separate versions of data dictionaries.

• It may be necessary to secure the license to use certain vendor software at an alternate site: this should be arranged in advance of the need.

• Backup for software must include object code and source code libraries and provisions for maintaining program patches on a current basis at all backup locations. Likewise, any documentation required for the consistent and continual operation of the business should be preserved in an offsite backup facility. This includes source documents required for restoration of the production database. As with data files, the offsite copies should be kept up to date to ensure their usefulness.

13.6 Recovery/Continuity Plan Testing

Most business continuity test fall short of a full-scale test of all operational portions of the corporation. This should not preclude performing full or partial testing because one of the purposes of the business continuity test is to determine how well the plan works or which portions of the plan need improvement.

The test should be scheduled during a time that will minimize disruptions to normal operations. Weekends are generally a good time to conduct tests. It is important that the key recovery team members be involved in the test process and allotted the necessary time to put their full effort into it.

The test should address all critical components and simulate actual prime time processing conditions, even if it is a confronted in off hours.

Specifications

The test should strive to accomplish the following tasks:

• Verity the completeness and precision of the business continuity plan.

• The performance of the personnel involved in the exercise.

• Appraise the ** and awareness non-business continuity team members.

• Evaluate the coordination among the business continuity team and external *** and suppliers

• Measure the ability and capacity of the backup site to perform prescribed processing.

• Assess the vital records retrieval capability.

• Evaluate the state and quantity of equipment and supplies that have been relocated to the recovery site.

• Measure the overall performance of operational and information systems processing activities related to maintaining the business entity.

Test Execution

To perform testing each of the following test phases should be completed:
• Pretest- The set of actions necessary to set the stage for the actual test. This ranges from placing tables in the proper operations recovery area to transporting and installing backup telephone equipment. These activities are outside the realm of those that would take place in the case of a real emergency, in which here is not forewarning of the event and therefore no time to take preparatory actions.

• Test-This is the real action of the business continuity test. Actual operational activates are executed to test the specific objectives of the business continuity plan. Data entry telephone calls, information systems processing, handing orders and movement of personnel,
14. Case Studies

14.1 Approach to answering scenarios

The suggested approach to the scenario questions is:

(a) Read the first paragraph of the scenario so you obtain an idea of the context of the scenario and the industry being used as an example.
(b) Read the question requirements
(c) Start to produce an essay plan, using the requirements as a structure for the plan and noting down the areas of knowledge that will be used
(d) Read through the scenario information in detail, noting on the plan relevant parts of the scenario that can be used to support the knowledge you will be including in your answer
(e) Check through the plan and order the comments made into the order for your answer
(f) Write out the answer – referring back to the scenario and question requirements as necessary to ensure you keep “on track” with the answer
(g) Cross out comments in the answer plan as they are transferred onto your answer to avoid making the same point twice
(h) If there is time, read through your answer, brushing up on spelling and any grammatical errors if you can

The purpose of these scenarios is not to produce a full answer, so you may want to eliminate sections 6 to 8 of the general plan above. However, you should be able to produce an essay plan, noting areas such as SWOT analysis or sections in the value chain that will be relevant to a full essay.

14.1.1 Using the scenarios

When you are ready, read through a scenario and produce an answer according to the procedure suggested above. Then compare this answer with the activity solution and identify which points you managed to include – and any that you missed. Finding the points missed will help you broaden your knowledge and see where additional comments can be made in similar answers next time.

Don’t do all the scenarios at the same time, but stagger these throughout the remainder of your studies to provide a change from learning. However, you will still be learning, but now how to apply your knowledge to specific situations!

14.2 Police Force of IRP

The management committee of the police force of IRP is responsible for the maintenance of law and order for a region of 1,600 square miles. The region has six major cities and a population of 3,000,000. IRP maintains its headquarters in the capital city of the region, and has branches in each of the five other cities.

The mission statement of the police force is to 'provide a quality service to the residents in the region by containing levels of crime to a minimum, and by maintaining an acceptable crime detection rate'.

The objectives of the force include:
(a) a crime detection rate of 40% (40 out of 100 crimes solved within 6 months).
(b) increasing public confidence in the police force by 2% per annum.

The actual detection rate is running at around 25%, and public confidence in the police force has fallen steadily for the last three years.

Specific information technology (IT) objectives formulated this year include:

(a) information should be sent to headquarters (HQ) from the regional centres within 10 minutes of a police officer reaching the scene of a crime.
(b) there will be an annual review and update of the IT system of IRP.

These objectives have yet to be reflected in the computer systems of IRP, as explained below.

The system

IRP's current computer system was last reviewed and upgraded five years ago. Each office has a Local Area Network (LAN) with personal computers, printers, file servers and a backup unit.

Communication between each location is by floppy disk each evening. Each of the five regional centres copies the day's information regarding crimes onto a floppy disk. This is sent by courier to the HQ where the main files are updated the next morning. Information is then available to police officers by telephoning the HQ during the day in normal office hours when staff are available to answer queries. Each week a copy of the HQ database is taken and sent to each of the regional centres, and the regional systems are updated with this information.

New crime details are entered onto the regional computer when police officers return to the police station, although this may not be until the end of their work shift, which can be up to 10 hours after an initial call-out to a crime. Each police officer uses a police car when he/she is on duty.

IRP employs 18 programmers to maintain and upgrade its software systems. Hardware and off-the-shelf software are purchased from a third-party vendor. The vendor also has extensive training and programming facilities that are not at present used by IRP.

Shortcomings

At a recent meeting between IRP and its third-party supplier, the supplier provided IRP with information concerning the shortcomings of IRP's computer systems:

(a) there is no long-term strategy
(b) there did not appear to be any project management skills within IRP for the continued upgrading of the computer systems
(c) IRP appeared to be unable to make up its mind regarding the computer system that it required. This has resulted in a large number of incompatible systems being purchased; even if regional centres were networked, they would have difficulty communicating with each other
(d) IRP always wants 'something for nothing' i.e., it is not willing to fund the IT infrastructure that it actually needs.

As a result of this meeting, IRP is actively reviewing its IT systems, and is considering outsourcing its main IT developments. IRP has therefore approached three companies and asked them to provide quotes for the development of its IT systems.
14.3 **Suggested Solution**

Outsourcing can be used to fill a skills shortage gap; for one-off projects; for consultancy etc. The following are areas where outsourcing could be used to IRP’s advantage:

**IT strategy**

Once the strategic framework has been established, stability is introduced which engenders the execution of long-term plans. At this stage the introduction of a third party would make a useful contribution. Consultants who are specialists in this field would be in a good position to develop the IT strategy and would have access to the many tools and techniques available to assist in this task.

The result would be an all-embracing, robust, long-term strategy to alleviate the deficiency that there is no long-term strategy.

**Skills shortage**

An IT department can be expensive to support and maintain, particularly if there is a requirement to keep it up-to-date.

New technologies, new applications, new techniques are continually being introduced; this means that existing staff constantly have to learn new techniques and new packages.

Sometimes the amount of work fluctuates. For example, the systems and networks staff may be very stretched while a new system is being installed succeeded by a period of under-utilisation. Also, there is a requirement for project management skills to continually upgrade the computer systems that are not present in IRP.

These deficiencies can be mitigated if the work is outsourced. Typically the amount of knowledge IT staff need to retain is forever increasing; therefore, it is increasingly difficult to be an 'expert' in more than one or two areas. The advantage of outsourcing is that IRP can benefit from the expertise of an individual for a short period without having to invest in that expertise in the long-term.

The most cost effective means of outsourcing this area may be to use the services of FM.

**Compatibility**

IRP have experienced a development in the IT area lacking in direction or strategy, resulting in a melange of incompatible equipment. Taking this route, due to lack of vision and/or experience, can be an expensive mistake. It is useful for organisations to ask from time to time ‘what business are we in?’ and concentrate on what it is. In IRP’s case, they are in the business of crime detection and prevention; to become involved in maintaining IT systems may be viewed as deviating from their main objectives. A service level agreement (SLA) with a third party may be a more economical route to satisfying their continuing IT requirements; this third party is better placed to handle changes to system requirements and annual reviews.
**Value for money**

By outsourcing, a particular service is being bought and clearly specified in a contract, and as a result IRP can expect better value for money. Because IRP are aware they are being charged for a specific service they will ensure that it is provided at the agreed price and within the agreed time period; it is within IRP’s interests to ensure this is the case. The third party is equally aware that he has to perform his part of the contract and failure to do so at the agreed price and within the agreed time period will almost certainly attract financial penalties. The third party will also be enjoying the economies of scale resulting from operating a large-scale enterprise, which can be passed on to IRP.

IRP may wish to select an FM used by other police forces. To gain the greatest benefit from outsourcing, an appropriate FM should be selected. One that has in-depth experience of the problems and procedures of police work would be in a stronger position to provide an economical and appropriate solution to IRP’s IT needs.

The potential risks to IRP from outsourcing the development and operation of its IT systems would include the following:

- Dependency on the supplier to operate and maintain a mission-critical application
- Loss of confidentiality of very sensitive data
- Difficult contract terms may lead to dispute and contractual arguments
- Length of contract (being locked into a deal that can’t be cancelled)
- Lost expertise, as IT staff no longer work within IRP (though there is little evidence of this at present)
- Earl’s systems audit grid:

<table>
<thead>
<tr>
<th>Business value</th>
<th>Divest</th>
<th>Re-assess</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>High</strong></td>
<td></td>
<td><strong>Renew</strong></td>
</tr>
<tr>
<td><strong>Low</strong></td>
<td></td>
<td>Maintain / enhance</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Strategic importance of planned Information Systems</th>
<th><strong>Turnaround</strong></th>
<th>Strategic</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Low</strong></td>
<td>Support</td>
<td>Factory</td>
</tr>
<tr>
<td>Low</td>
<td>High</td>
<td></td>
</tr>
</tbody>
</table>

(a) McFarlan’s strategic grid
14.4 Nasar Inc

You are a consultant who has been appointed to assist the financial controller to implement a new personal Computer (PC) based financial accounting system selected by the Mr Khan, Managing Director of Nasar Inc (Nasar) and also owner of the company. You have also been asked to help the company develop a strategic plan.

Nasar was established 2 years ago as a computer distributor, specialising in the sale of notebook and laptop computers and a full range of accessories e.g. carrying cases, docking stations. At the time the company was set up, Mr. Khan believed there would be enormous growth in this area and the growth of his company has confirmed this. Nasar now consists of 5 retail branch offices in large regional towns and a warehouse and head office function in Karachi. During the last year, Mr. Kahn has begun to sell through dealers in smaller towns.

Mr. Khan has encouraged the branch stores to operate autonomously. Individual stores have local computer systems to handle customer orders, customer tracking, marketing etc. Sales are normally for cash or credit card, although there has been an increase in orders for specialty notebook computers that are then billed to corporate customers. Dealers place their orders with head office.

Head office keeps track of the dealer orders and fulfilment processes.

Summary financial data in provided below:

<table>
<thead>
<tr>
<th>YEAR ENDED</th>
<th>SALES (Rs)</th>
<th>GROSS MARGIN (Rs)</th>
<th>STOCKHOLDING (Rs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>31/12/1999</td>
<td>225,000</td>
<td>51,750</td>
<td>49,000</td>
</tr>
<tr>
<td>31/12/2000</td>
<td>4,650,000</td>
<td>930,000</td>
<td>850,000</td>
</tr>
<tr>
<td>31/12/2001</td>
<td>16,440,000</td>
<td>2,350,000</td>
<td>3,750,000</td>
</tr>
</tbody>
</table>

In your initial meeting with Mr. Khan and the Financial Controller, Mr. Addit, the provided an overview of the company. Here is an extract from the meeting notes:

As you can see from our figures, the past 3 years have been extremely successful for Nasar. In a highly competitive industry, we have been able to capture a high proportion of the market, largely due to our ability to deliver specialist notebooks to our customers without lengthy delays. With the current high demand, manufacturers have been unable to supply sufficient stocks to meet industry demands. However we have overcome this by ordering products from our suppliers based on expected demands of our customers and by close liaison with our suppliers to monitor delivery times.

The business has now grown to the extent that we need more computerised controls than those provided by our existing PC based cashbook system. With increasing sales volumes, we have a larger volume of outstanding customer accounts and higher stock levels. Also the risk of obsolescence in our industry means that we cannot afford to let our stock holdings get out of hand.

Another issue is that our competition is increasing. Other sellers of PCs are beginning to move into the notebook market and together with the improved production capabilities of manufacturers this is pressuring us to reduce our prices. We need to look at promoting IT more as a strategic weapon rather than an administrative tool.

As you know, we have purchased the Cashit Accounting software package at a cost of Rs 10,000. It is a multi-user system that comprises the following modules:
• General Ledger  
• Account Receivable  
• Accounts Payable  
• Inventory Control  
• Cashbook

i) Identify 3 key critical success factors (CSFs) for the business and explain why each of these is critical.

ii) What sort of information is required to monitor the performance of Nasar against the CSFs.

iii) List 3 ways in which IT can play a more strategic role for Nasar and provide real or hypothetical examples from various industries. Identify how each way listed might relate to this company

iv) Describe how IT plans should be developed in relation to this organisation's business plan.

v) Given the current situation in the organisations there is a need to centralise customer information for use in national marketing. Which areas would you want to investigate further to determine their impact on the IT strategic plan?

vi) You are invited to speak for approximately an hour at a meeting of the branch managers and major dealers to explain the IT Strategic Plan. Develop an agenda for the meeting and explain how you would run the meeting. Consider what issues you think the managers might raise and describe how you would handle these in the session.

14.5 Suggested Solution

i) CSFs should be directly related to the material in the question and could include:
   • Purchasing policy. The ability of the company to purchase notebook computers so that they can deliver them to customers more quickly than their competitors
   • Debtor Control. Cash flow is important especially given the high stock value. Mechanisms need to be in place to collect revenue as soon as possible.
   • Stock Control. In an industry with a sustained downward pricing pressure, it is critical that slow moving stock is quickly identified and converted to cash.
   • Pricing control, the pricing pressure from competitors will result in decreased margins (evidenced by decreasing Gross Profit margin in the figures supplied). Margins on stock items need to be closely monitored.

ii) The sort of information that should be in place to monitor these would be:
   • Purchase order information including costs, outstanding orders, expected delivery dates and forecast sales.
   • Debtors information including cash receipts, orders taken and projected sales.
   • Stock information including % turnover of items, stock items not sold for a certain period and holding times.
   • Detailed sales information would be required including sales by region, salesman and period, discounts given and difference between buy-in and selling price.
iii) There are many ways in which IT could play a more strategic role for Nasar. These include:

As a competitive tool

1. Provide field staff with effective methods of gathering information e.g. using mobile technologies such as laptops and hand-held computers. Dealers with hand-held computers could provide almost instant access to obsolete or slow stock to negotiate deals with priority customers and move the stock.

2. Provide effective methods for tracking stock items and performing stock takes more easily e.g. introduce bar-coding and scanning technologies. Picking stock in the warehouse could be more timely with bar-codes and scanning technologies. More frequent stock control could move some of the potentially obsolete stock.

3. Provide a collaborative computing environment to help staff across all department share information e.g. e-mail, and other groupware. By allowing staff in the retail branches and warehouse and head office to communicate and have access to important stock and customer information for better services.

4. Investigate integrated systems that will provide more information for targeting customer types and special customers e.g. CRM systems. Brining all system together will overcome some inefficacies in each branch looking after its own systems and it will provide head office with better management information for decision-making.

To re-engineer business processes

5. Rationalise systems and allow staff to share facilities e.g. use the same order and customer management information systems and processes. AC RM or ERP system would necessitate a review of business processes and rationalisation of duplicated processes at remote branches and head office.

6. Provide tools to re-engineer processes and determine effects e.g. CASE tools. By providing a selection of the tools available to management, Nasar will facilitate better analysis and design of information systems.

7. Provide the ability to capture cost information about current processes to determine where there are inefficiencies e.g. investigate activity-based costing.

8. Provide the facilities to automate current manual processes e.g. robotics for picking orders in warehouse.

For inter-organisational linking

1. Provide direct access to supplier systems for ordering and tracking delivery of orders e.g. EDI systems. Many suppliers now use networks and communications software to enable direct access to suppliers systems. This would enable Nasar buyers access to better information and faster order fulfilment.

2. Provide timely information to partners e.g. extranet and collaborative tools.

IV) The student should be able to relate the development of an IT Strategic Plan to Nasar in terms of the major players and issues to be covered. The key to being able to work with the business on the Strategic Planning is that the company has identified using “IT more as a strategic weapon than an administrative tool”.

The company will need to develop its business strategy first in consultation with IT. Once the business knows its goals and objectives, then it can begin to develop and look at the strategic use of IT. IT Strategic planning should identify opportunities that can then be tested against the Business plan and revised until they are aligned.
Armed with the IT Strategic Plan, the IT Manager will then be able to address the IT planning issues, develop priorities for IT acquisitions and systems, and address the operation’s strategy.

14.6 JHG

Background

JHG has 256 branches in 26 different countries worldwide including the USA and the UK, in most European capitals, and in Kuala Lumpur, Colombo and Johannesburg. The company offers specialist financial services to multi-national companies including audit and assurance advice, systems analysis and systems assurance. The company employs in excess of 21,000 people. The company was formed in July 20X8 from the merger of firms within the 26 countries. The aim of the merger was to provide international companies with a standard service, no matter in which country they were located.

Use of software

Prior to the merger, the independent firms that now belong to the JHG Company established and maintained their own computer hardware and software systems to support their work. As part of the post-merger integration, an international committee of senior Board members from each country has been working on producing software that can be used by all branches of the company, regardless of the country in which they are operating. Amalgamating and rationalising the system development departments currently maintained within each country will achieve substantial cost savings for the company, as a whole.

Writing this software commenced in December 20X8 with the objective of implementing the new system during July 20X9, just prior to the busiest months from the point-of-view of the amount of work being undertaken. Because of the relatively short timescale for writing the software, three software development centres were established in London, San Francisco and Kuala Lumpur. The aim was to speed up the writing of the software by transferring the work between the three different time zones to achieve virtually 24-hour working.

Once the software is implemented, employees will easily be able to share work, including confidential client information, because they will be using the same system. This will help to provide an enhanced service to JHG’s international clients. The client data refers to individual client companies and some of their employees by name.

Additional project information

Reports produced in early March 20X9 indicated that the development was proceeding well. Development deadlines were being achieved and the software writers in the three locations had adapted well to the working arrangements.

Key milestones still to be achieved included:

- July 20X9 - Confirmation of hardware and software requirements to run the new software
- August 20X9 - User input regarding the acceptability of the system
- September 20X9 - Release of software and implementation in each country
- January 20X0 - Full training material and user guides available
Where the particular laws of any country are not fully accommodated by the software, minor amendments will be required on a national level. This local tailoring will take place towards the end of August 20X9.

Current situation - 27 May 20X9

The international team of software writers, being quite pleased with the software written to date, decided to release an example of one of the main information screens to be displayed in the system. The team is particularly proud of the innovative use of navigation icons and the inclusion of flower pictures on-screen to provide a more relaxed working environment. However, the project is falling considerably behind schedule. The international Board is considering two alternatives:

(a) cancelling the implementation in 20X9; or
(b) asking all branches to use the international version of the software this year, which will mean postponing any local tailoring of the software until the year 20X0.

Neither option is particularly acceptable, and the Board has yet to make its final decision on this matter.

Requirement

*Produce a brief SWOT analysis for the Information System of JHG.*

14.6.1 Suggested Solution

SWOT analysis

**Strengths**

Large organisation with an international network of branches

**Weaknesses**

May be too complex for existing communications systems
Current information systems in various locations are inconsistent and may be incompatible
Project falling behind schedule
Programmers concentrating on content rather than user needs

**Opportunities**

Significant cost savings, improved service levels (and efficiency improvements) available from integrated software
24-hour software development available due to global nature of the business

**Threats**

System may fail due to loss of confidence, late delivery or lack of user acceptance
14.7 Reedit Publications

Reedit is a publisher of children’s and educational textbooks. It is planning to upgrade its use of technology including greater automation of its head office and production facilities. Currently it operates production facilities at 3 of the regional centres focussing on children’s books while the remaining centres focus on educational textbooks.

In the past, the company’s technology has been developed in a somewhat ad-hoc manner. Fast growth has meant that systems have been developed in reaction to problems rather than in any planned manner.

The following briefly summarize the company’s information architecture:

Technology. The company runs 2 mid-range computers that have significant capacity and performance issues at present. The processing load on the hardware is very high and this is causing bottlenecks with memory and disk activity.

Network. Local Area Networks (LANS) are in place at the head office, each of the 5 regional distribution centres and in several other locations. Most of the factories have terminal connections with a few stand-alone desktop PCs. A WAN is in place connecting each of the major regional centres.

Applications. Reedit purchased a software package for accounting some years ago. The software also provides some functions for sales, manufacturing and distribution areas. The applications have been heavily modified with a few specialized systems development for forecasting and analysis. Several projects are underway at present to improve the existing systems.

Data. A well-known database is being used as recommended by the software vendor.

IT Organization structure. Two teams are in place with separate IT managers. One team is in the production facilities and includes 10 staff to support the production plant as well as the regional distribution centres. The other team is in the Head office. This team, comprising 5 people, supports the WAN and desktop as well as the centralized systems.

The Executive management of Reedit recently announced it is going to change the business approach from a regional basis to offer products at a national level (i.e. all product lines available nationally) plus extend its range into educational games.

The company has been working on its business strategy and the overall approach includes setting its Corporate Mission Statement/Vision and then establishing the broad objectives and strategies by product line. Business Managers will determine specific plans to achieve the corporate mission. The IT managers have been asked to participate in the process.
You are a consultant assigned to help Reedit Publications (Reedit) prepare its Information Technology Strategic Plan.

i) Explain how the proposed restructuring could affect the current information architecture.

ii) The table below outlines some of the tasks in the overall Business Strategic Planning Framework. Using the table, identify and explain the IT Strategic Planning tasks that need to be considered within this framework. (NOTE that not every row of the table needs to be used.

iii) Identify the use of an IT Strategic Plan for Reedit. What information from the IT Strategy document could also be included as separate sections within the Business Strategy document? What sections from the IT Strategic Plan would you recommend are excluded from the Business Strategic Plan and form part of a separate IT document?

<table>
<thead>
<tr>
<th>Stage</th>
<th>Purpose</th>
<th>Process</th>
<th>Deliverables</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vision</td>
<td>Set Business mission statement and vision</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strategy</td>
<td>Set broad business objectives and strategies</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Implementation</td>
<td>Set specific business strategies.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

14.7.1 Suggested Solution.

i) The proposed restructuring could affect current IT architecture in many ways including:

Technology. Capacity and performance are already an issue. Adding to processing and expanding products lines will impact this and place heavy demands on the systems. The IT implications are to look for adding memory, and disk storage capacity or to evaluate an overall upgrade to the system. More strategically there might be better production control systems that will necessitate a move to client/server architecture.

Network. Local Area Networks must be standardised and able to connect all centres. Greater automation linking all centres might necessitate a review of the entire network. More strategically, an investigation into the Internet, intranets and other network solutions might prove fruitful and require more focus on security issues such as encryption and firewalls.
Applications. IT is unknown how the systems are currently structured but to move to a national product line will require a review of the systems. Can they handle the new expanded product line? Can they handle the new accounting controls and systems? Will they still be appropriate for a new architecture and will they be able to support the centres over a network?

Data. Although no details are given, this area must be reviewed as part of the overall architecture. How does the database relate to the other systems? What sorts of users require access? Should it be integrated across the organization and with all systems? Strategically it might be appropriate to look at an ERP system to integrate all systems and provide improved information for management decision-making.

IT Organization structure. This is the area that will have the most impact. With 2 IT managers and various locations, the issue of staff skills and performance will be key. Identifying the location of the IT department and the roles of the 2 current managers will need to be handled carefully. Understanding the resources needed and the skills needed for the new architecture will be crucial.

ii) Typically IT strategic planning is done as a separate exercise however this is changing and the biggest issue today is how to align the business Strategic Plan with The IT Strategic Plan. Student’s answers will vary for this questions and there is no one correct solution.

What we are looking for is an understanding that the strategic business plan underpins and drives the IT strategy. IT is not a technical document and should be high level.

Suggested solution is:

<table>
<thead>
<tr>
<th>Stage</th>
<th>Purpose</th>
<th>Process</th>
<th>Deliverables</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vision</td>
<td>Set Business mission statement and vision</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT Purpose and Vision</td>
<td>To gain a shared understanding of the IT Direction within the business.</td>
<td>Describe the desired state of IT within the business – including the IT Dept and the rest of the organisation</td>
<td>Brief IT direction.</td>
</tr>
<tr>
<td>Strategy</td>
<td>Set broad business objectives and strategies</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Understanding the current IT environment</td>
<td>Complete and inventory and assessment of all systems and infrastructure</td>
<td>Systems overview</td>
<td>Systems assessment</td>
</tr>
<tr>
<td>Identify technology trends that could impact the business</td>
<td>Review literature, attend trade shows, and contract consultant’s report about technologies that impact the</td>
<td>List of key factors and key technologies</td>
<td></td>
</tr>
</tbody>
</table>
### Establish IT objectives and Strategies

Identify key business areas that need to be supported and critical success factors

### Summary of IT objectives

<table>
<thead>
<tr>
<th>Implementation</th>
<th>Set specific business strategies.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Specify IT strategies and evaluate key business areas</td>
</tr>
<tr>
<td></td>
<td>Project summaries linked to specific business strategies</td>
</tr>
<tr>
<td></td>
<td>Develop a high-level IT Architecture</td>
</tr>
<tr>
<td></td>
<td>Application Architecture</td>
</tr>
<tr>
<td></td>
<td>Technology Architecture</td>
</tr>
<tr>
<td></td>
<td>IS Organization structure</td>
</tr>
</tbody>
</table>

### iii) The IT Strategic Plan for Reedit should provide a framework that supports future IT decisions about projects, budgets, and resources. The document also provides a communication tool to IT staff and the rest of the organization about the direction, priorities and resources issues for IT.

Sections of the IT Strategic Plan that should be included in the Business Strategic Plan are:

- Current IT assessment including overall assessment, status and issues relevant to Reedit
- IT Strategy containing an outline of the proposed projects in terms of the business and product strategies that they support. This could also include a high-level information architecture and plan for IT projects.
- IT Strategy Implementation Plan highlighting dependencies, transition issues and opportunity factors.
- Sections that would not be included in the Business Plan are:
  - Project Descriptions giving brief scope, name, dependences, critical success factors
  - Information Architecture models that are more technical in nature e.g. network architecture and data architecture
14.8 MQS Ltd

Introduction and decision making structure

MQS Ltd produces specialised industrial chemicals to individual customer orders. Each order is treated as a separate project under the control of three distinct management tiers:

The production managers who are responsible for the making of the product, although they have no control over the input mix or the quality of input used. Each product is made from a large number of chemicals and is very sensitive to any change in the quality of the inputs. To maintain a high quality of output, frequent adjustments are required to the input product mix. These adjustments alleviate any fall in quality caused by changes in the quality of the inputs.

The senior managers who work in the company's main office. The senior managers collate and produce weekly management reports on the progress of projects for which they are responsible. The reports recommend actions to the chief accountant although he must authorise these decisions before they can be implemented.

The chief accountant who approves changes to the costing of projects, and the quality of inputs and the input mix used.

Order and production process

Each customer order takes four months to complete from the initial receipt of the order at MQS Ltd. The order and production process involves four stages, each stage taking approximately one month. Each stage is followed in sequential order with no time overlap.

Quotation: Drafting of a detailed quotation and input requirements listing for agreement with the customer. Only 1% of orders are cancelled during this time, and an initial input requirement can be available in as little as two days, including pricing from standard price lists issued by suppliers.

Material ordering: A price enquiry is sent to three suppliers, who each return a firm quote including quantity discounts not available on standard price lists. A quote has to be accepted by the chief accountant before the approved purchase order can be raised, and goods delivered from the supplier. Goods are ordered from one of three competing suppliers. The order is given to the supplier with the lowest quote. Goods are then available ex-stock. MQS Ltd employs a staff of 10 to negotiate prices and saves on average £25,000 per annum in the process, compared to the standard price offered on trade price lists.

Production: Production itself takes about one week. Quality control checks take about three weeks.

Packaging and shipping: Specialised containers for the delivery of the goods are ordered. Two weeks later these containers are delivered, and the goods are checked into the container. Another week is taken up in organising a specialist courier firm to collect and deliver the goods.

MQS Ltd is considering whether to implement a business change (business process re-engineering project) for its ordering and production process.
Requirement

Explain how time could be saved within the order and production process by re-engineering it. Provide a detailed estimate of the new production time from the receipt of order from the customer to the delivery of the finished goods.

14.8.1 Suggested Solution.

Currently the time taken to service an order is four months.

Time could be saved within the order and production process as follows:

- After receiving an order, an initial input requirement can be available in two days and requirements agree with the customer within a week. Currently this stage takes one month.

- Following negotiation, orders for delivery of ex-stock should be placed with suppliers to Just-in-Time delivery within the same week. Having set up arrangements with the suppliers, the requirements for expensive and time-consuming negotiations for each order placed is eliminated.

- In week 2, production and quality control can commence, and the delivery container can be ordered. Quality control can continue into the following two-week period while awaiting delivery of the container. The delivery time and the time taken to undertake quality control should also be investigated for potential savings in time.

- During week 4, while carriage is being organised with the specialist courier, the goods can be checked into the container.

Following the above process, the new production time could be reduced to about five weeks. Further time may be saved by investigating procedures further e.g., whether spare containers could be kept on site; reducing the delivery time of the container, the time taken to carry out quality control etc. As well as reducing the production time, other savings such as staff costs, have also been made.

14.9 ARG

Background

ARG is an international airline operator, based in a central European country. It maintains a fleet of approximately 350 aircraft, and its core activity is to provide passenger and freight services to over 200 destinations worldwide.

ARG maintains offices in each country to which its aircraft fly. Each office provides the following services:

- information provision on the airline services offered by ARG, including flight times and destinations serviced by ARG, and
- access to ARG's passenger and freight booking system for customers who wish to book either passenger or freight carriage services with ARG.
Each office also has access to ARG's confidential internal data systems that provide information on aircraft location, servicing history and the company's personnel. The latter includes salary details as well as staff locations.

**Systems specification**

To support its core business activity, ARG recently invested in a high-speed international WAN. This system enabled ARG to transfer large volumes of data relating to its operations between its 200 offices worldwide with a minimum of delay. The systems specification for the new ARG system was quite rigorous. The specification included the following requirements:

- the basic infrastructure of the WAN, including such items as the cabling and communication hardware, had to have an expected life of 10 years,
- computer chips and other similar system elements had to be upgradeable as technology improved, and
- the entire system had to be easily upgradeable with a fixed capital amount being allocated for this upgrade each year. System upgrades were not to exceed this capital amount under any circumstances.

ARG also assumed that its WAN infrastructure and its core business as an international airline operator would remain unchanged for the next 10 years.

Very few equipment suppliers were willing to provide this level of commitment to the system. Finally, a small but financially stable company called AP Ltd successfully tendered for the contract, even though some of AP Ltd's systems were not industry standard.

**Systems implementation**

The actual systems changeover and implementation were performed with few problems. The staff at ARG were using the new system efficiently within one week of implementation.

It should be noted that the Board of ARG made the decision to invest in the WAN on the basis that the company must be at the forefront of the use of technology to support its core business activities. This strategy is seen as being essential to produce a sustainable competitive advantage in the airline industry.

**Post-implementation review**

In the three months since the system was installed, ARG has seen significant increases in productivity and levels of customer service. The investment has therefore been judged to be a success.

During the post-implementation review of the system, it was found that the WAN had considerable excess capacity to take additional network traffic. ARG's initial forecast showed that it would use only one third of the capacity of the network in its first two years of operation. Even optimistic forecasts of network traffic growth indicate that this excess capacity would not be used by ARG for at least another 7 years. The Board of ARG therefore asked the IT Director to consider ways of providing additional revenue to the company from this excess capacity.

After detailed consideration of the problem, the IT Director reported back to the Board. The main proposal was to make this excess capacity available to other companies which required a WAN but either did not have the money, or the strategy to build a WAN for themselves. Should the proposal be accepted/ then it is expected that these other companies would require

- a guarantee of the level of service that they can expect from ARG, including access rights to the WAN and delivery times of information across the network,
• Internet access to transfer data to customers and receive information back from customers,
guarantee of security of data both from non-ARG WAN users and from the staff of ARG itself.

Requirement

*Produce a brief PEST analysis for ARG, concentrating on those issues that directly affect the*
*Information System of the organisation.*

*Briefly outline the steps that the IT director would have to take in developing a business case for*
*his proposal.*

14.9.1 Suggested Solution.

PEST analysis

Political

• Different countries may have different legal restrictions relating to information systems

Economic

• The airline industry is highly competitive

Social

• Airline customers are demanding more information regarding consumer products, and will expect
real-time information
• Users are becoming more technologically-aware (and therefore less tolerant of poor systems
performance)

Technological

• High speed data transmission is available from WAN providers and through the Internet
• Technology is changing too quickly to assume that systems infrastructure will remain unchanged
for a long period

Business case development

The steps that the IT director would have to undertake would be as follows:

Where we are

Beginning the business case with a critical appraisal of the current position of the system will allow the
Board to understand the problems and issues that led to the investment proposal.

Where we want to be

Having clear objectives for the investment will lead to four clear benefits:

The board can decide whether achievement of the objectives justifies the scale of the investment.
The Board can decide whether the proposal is goal congruent with the strategy of ARG.
The objectives can be used as the basis for a framework of performance measurement and control during the project (if it is agreed).

The objectives can be used as the basis for a post-investment audit, once the project is completed.

**Going to get there**

This stage outlines the scope of the investment, and may break it down into a detailed series of steps or ‘work packages’. This will give the Board a clearer view of exactly what is involved in the project, and allow them to judge the degree of business disruption likely to be involved.

**Justification**

The justification stage of the business case will give the Board the detailed information that they need to make their decision whether to proceed with the investment. It will summarise the preceding stages, and seek to show that the business benefits of the investment outweigh the business costs.

---

**14.10 TEP PLC**

**Background**

TEP plc runs a theme park offering a wide range of activities including rides, shows and parades. The rides vary from 'thrill' rides, where visitors sit in vehicles that travel around a hilly track at high speed, to slow electric-powered cars in which children can drive around. Visitors pay an entrance fee, which gives them unlimited access for one day to the park's activities. The average entry price is £16 and the park received 2.6 million visitors in 1997. It employs about 6,000 staff for about 9 months of the year: the park closes during a season of poor weather.

It is considered to be the most popular park in the country in which it operates, although in recent years it has tended to attract more young adults and fewer families with younger children. Market research undertaken by TEP plc indicates that families tend to avoid the park because there are very few attractions for children below the age of 10. Many of the technologically advanced rides built by TEP plc have age and height restrictions, making them unsuitable for young children.

The objectives of TEP plc are to

- maintain net profit margins at 10%, and
- offer the most technologically up-to-date rides.

The company has met these objectives during its last seven years of operation. However, a number of other parks have opened in recent years, offering similar state-of-the-art attractions and rides. These parks have placed considerable competitive pressure on TEP plc. The main area of competition between the parks is in providing the most technologically advanced ride possible, whilst at the same time making the ride sufficiently attractive for customers to want to return to the park to go on the ride again. As a result of this competition, the average cost of providing a new ride is £6 million with annual maintenance costs running at 10% of this amount.

**Current information systems**

The theme park's information system was installed seven years ago and has received only minor modifications since then. It concentrates on collecting information concerning:
• customers entering the park, including cash collection and banking (payment is accepted by cash and credit cards)
• stock and sales control of the retail outlets, and
• the numbers of customers using each ride.

The Directors' Executive Information System was also installed seven years ago. The EIS is linked to the park's information system, providing the ability to view the daily totals from this system. In the early 1990s, this was considered to be the only data that the Directors required from the computer systems. The Directors now hardly ever use the EIS.

Both the EIS and the park information system are backed up daily with the backup disks being kept in a fireproof safe in the ticket office on site.

Although there are plans to advertise the park on the World Wide Web, the project has been delayed.

**Investment decision in 20X8**

After a substantial review of the theme park market, TEP plc has identified what it considers to be a new area where competitive advantage can be obtained. At present, all the theme parks in the country only offer facilities at the park itself. The board of TEP plc believes that the company should

• build a modern hotel within the park offering accommodation for families with children,
• offer a complete holiday package to customers including travel arrangements, accommodation at the hotel, special offers like early entry to the park and souvenirs such as special mugs,
• provide more shows and rides suitable for younger children to encourage more families to visit the park, and
• purchase a specialist travel agency to provide the holiday package service.

The cost of this investment would be in the region of £6 million, although the hotel would not be operational until the 20X9 season.

If the investment is undertaken, it is expected that the travel agency will be able to

• access the new hotel's computer system to book accommodation via an Internet connection
• provide details of special events directly from TEP plc's theme park Web Site, and
• provide an on-line booking and payments system through its own Web Site for customers who prefer using the Internet to book their holiday.

If the hotel investment is made, then no new ride would be produced in 20X8. The policy of building one new ride per year would be re-introduced in 20X9.

As an alternative, TEP plc could continue its present policy of investing in one major new ride each year. This would help it maintain its position of being the most technologically advanced park in the country. The ride under consideration is a virtual reality simulator of a spaceship crashing into one of Saturn's moons. It will cost £6.2 million to develop and build. So far, no other theme park has considered using Virtual Reality on such a large scale.

The Board must choose between these two investment decisions by the end of June this year.
Requirement

Explain the features of an improved EIS that would assist the directors of TEP plc in the strategic management of the business.

Briefly explain how data warehousing and data mining could be used by TEP plc to improve the profitability of their business.

Briefly explain how IT could help TEP plc to decide between the investment alternatives, and suggest any limitations to its use in this context.

14.10.1 Suggested Solution.

EIS features

The current Executive Information System (EIS) is seven years old and can allow the directors to view daily totals from the theme park's information systems. However, the system is hardly ever used because of its limited functionality. The changes that need to be made include the full provision of facilities that a modern EIS now tends to provide. This would consist of

- easy to use, screen-based systems with mouse, icons and touch-screen facilities, giving easy access to data;
- presentational aids, by pictorial or graphical means, so that information can be conveyed without too many trivial choices of scale, colour and layout. The EIS should be able to provide information pictorially, and in an easy-to-use format, so that the directors can overlay the trend information from one variable on top of another to check for correlation etc.
- summary level data, captured from the organisation’s main systems, which might involve integrating the executive’s desktop micro with the organisation’s mainframe;
- a facility that allows the executive to drill down from higher to lower levels of information;
- data manipulation facilities such as comparison with budget or prior year data and external information that can be superimposed onto the organisation’s information e.g., sales forecasts with information from the Meteorological Office about the weather;
- tools for analysis, including ratio analysis, forecasts, what if analysis and trends;
- a template system that allows the same type of data e.g., sales figures, to be presented in the same format, irrespective of changes in the volume of information required.
- a broad range of both internal and external data as well as the ability to drill down to the detailed transactions.

Data warehousing and data mining

TEP has access to a large volume of data about the performance and history of their business, plus data relating to the demographics and spending of visitors. Data warehousing involves setting up a central corporate database in which all or most of the organisation’s data will be held. This data will then be made
available to all authorised users via their workstation. This would allow staff to analyse data relating to the business and use it to model the likely impact of major investments such as those suggested (see below).

Data mining means extracting data from multiple data sources by means of interactive and analytical software tools that allow the miner to specify search parameters and are capable of identifying trends and relationships within and between data sets.

Data mining involves the application by the software of a number of different analytical approaches:

- Identifying ‘clusters’ of useful and significant data in the midst of a useless or irrelevant mass;
- Summarising data to show overall patterns that may be hidden if data is viewed at the detailed level;
- Creating and learning classification rules that can make sense of patterns in data;
- Finding possible dependencies between apparently unrelated data sets, using correlation and regression tools; and
- Detecting anomalies in patterns of data that may signify events or occurrences that are important to the decision-maker.

Data mining packages not only provide the analytical tools required for data analysis, but also ‘learn’ from the process of mining and become more powerful the more they are used. Decision-makers find that data mining packages turn them into ‘experts’, without having to learn how the analytical tools actually work.

The use of data mining software on a data warehouse at TEP would allow the managers to identify opportunities to exploit the behaviour of the organisation and its customers to improve revenues and reduce costs.

**Using IT for investment appraisal**

Having obtained all of the relevant data from the data warehouse, the decision makers in TEP would be able to use computer-based modelling packages (often based on spreadsheets) to evaluate the cash flow and business impact of the investment proposals under different sets of assumptions. This would improve the decision making process and allow managers to understand the risks and opportunities of each option.

### 14.11 DS LTD's

DS Ltd's main activity is the delivery of parcels. It aims to deliver parcels within 24 hours of collection to any place in the country in which it operates. It maintains 27 distribution warehouses - one in each of the major population centres of the country. Each warehouse has a fleet of delivery vans as well as warehouse, administrative and distribution staff. The company's head office is located in the capital city.

**Current computer system**

DS Ltd's current computer system is described below:

The main network is a Wide Area Network (WAN) with each distribution warehouse being linked to a central database via a dedicated landline. Each warehouse itself runs a Local Area Network (LAN) with a central minicomputer maintaining up-to-date files for that location.

The central database is updated from each warehouse every three hours on average. Update is hindered by the low baud rate of the data transmission equipment. At the same time that the central database is updated, the LAN at each warehouse receives the current copy of the database. There are 27 sites and about 6 minutes' processing data transmission time is required per site for full update of the database.
Input at each warehouse is by keyboard and VDU to the local database. Data are validated on input. Errors normally occur when packages are received from other warehouses, within a 50-kilometre radius, before the local database has been updated to receive details of those packages in transit.

**Treatment of packages**

Each package in the system is treated as follows:

When the package is collected from the dispatch point, the customer signs a three-part package receipt set to confirm the collection of the package. One part of this receipt is attached to the package, the customer retains the top copy and the van driver the third copy. The package is taken to the local warehouse where the package receipt slip is checked against the list of expected collections for that day. Any non-collections are noted and investigated by 11.00 am the following day.

The destination for the package, taken from the package receipt slip, is entered into the company's computer. The computer works out the optimum method of transferring the package to the warehouse that is closest to the delivery address. It then prints out a transfer list showing the proposed shipping methods and estimated timings for that package. The transfer list is attached to the package. Each transfer list has a unique reference number on it; this reference number will be input to the computer system at various stages throughout the journey of the package. This will assist the company in ascertaining where individual packages are located.

Each transfer list is read manually and the package placed on the appropriate lorry for forwarding to the distribution warehouse from which the package will be delivered to the customer. Where the package is routed via more than one warehouse, the package will be placed on the lorry for the intermediate warehouse for onward transmission to the final warehouse.

Upon receipt at each distribution warehouse, packages are again sorted using the transfer list attached to each package. Packages for other distribution warehouses are forwarded, whilst packages for local delivery are further sorted by hand into area codes for the city. The driver is given packages for his own area code, and is then expected to deliver the packages after organising his own route.

Customers sign for packages upon delivery. The goods delivery note is left with the customer, and a copy is taken back to the warehouse where details are input to the computer.

Packages are tracked through the system at each warehouse. The unique transfer list code is input to the computer as each package is dispatched or arrives at the warehouse. The computer master files are updated every three hours with this information.

The company is actively investigating the use of hand-held bar-code readers as an input device, which will be linked to a computer terminal located in each of the company's vehicles.
**Requirements**

Identify and explain the possible sources of competitive advantage that DS Ltd might obtain from the use of bar coded data capture and vehicle-based terminals.

If the system of bar codes and vehicle-based terminals were to be adopted, briefly outline opportunities to use the Internet to gain a further competitive advantage.

Briefly explain how a decision to invest in bar coded data capture and vehicle-based terminals would be affected by the corporate strategy of DS Ltd.

Briefly explain how the Value Chain of DS Ltd would be affected by an investment in bar coded data capture and vehicle-based terminals.

**14.11.1 Suggested Solution.**

**Competitive advantage**

*Cost leadership*

The proposed use of bar coded data capture and vehicle-based terminals may lead to a reduction in staff numbers required for the input and processing of data. This may allow DS to reduce the cost (and perhaps the price) of their services.

*Differentiation*

Their customers may see the use of technology by DS as adding value to the service by making it more efficient and effective.

*Focus*

Improved information flows should allow DS to provide a more personalised service, particularly to their large, regular customers.

**Use of the Internet**

Once the investment is made in bar coded data capture and vehicle-based terminals, DS could choose to give large customers the option to track their parcels on the Internet. This would involve the customers gaining access to the information systems of DS, but would improve service levels (and therefore differentiation) still further.

**Corporate strategy and IT investment**
DS will have to decide whether such a large IT investment, with the opportunity to obtain a competitive advantage from it, fits in with their overall corporate strategy. We have no information about the company’s strategy, but the fact that they are actively investigating the opportunity suggests that they are likely to invest. There is a risk that customers may perceive the change as reducing the ‘personal service’ element of the business, but this is unlikely. However, the investment should be considered by the organisation’s strategic decision makers before it proceeds.

(a) Value chain

<table>
<thead>
<tr>
<th>Firm Infrastructure</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Human Resource Management</td>
<td>Autom.</td>
</tr>
<tr>
<td>Technology Development</td>
<td></td>
</tr>
<tr>
<td>Procurement</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Inbound Logistics</th>
<th>Operations</th>
<th>Outbound Logistics</th>
<th>Sales &amp; Marketing</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Better utilisation of staff and vehicles</td>
<td>Improved on-time delivery of parcels</td>
<td>Internet-based enquiry system for customers?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

14.12 **Veemax**

Veemax manufactures and distributes solar power systems for homes and are recognised overseas as being leaders in their field. The company deals directly with home builders and some residential architects but plan to develop larger systems for office buildings and hotels.

Veemax has separately managed data centres in 4 large towns across Pakistan. There are 3 types of hardware platforms in use by the company. Veemax recently acquired new hardware the head office based on an expected life of 5 years. Applications are mainly purchased, fairly old and undocumented, with some modifications made for the business requirements in each town. Each data centre is responsible for all local IT Functions, and involves systems analysts, business analysts, computer operations staff and user support representatives. Network communications is arranged in a coordinated manner across the data centres.

The proposed investigation needs to assess the cost, benefit and ability of two or three IT operating alternates. A management committee consisting of the business managers and IT managers for each town will approve the recommendation.

You have been asked by Veemax to propose consulting services to help assess the future operating alternatives for its data centres, based on outsourcing and centralisation options.
i) **Prepare a presentation to the Veemax management committee that outlines the alternatives you propose to investigate and your initial reasoning. Describe the areas/factors you will investigate to help Veemax assess each of the alternatives.**

ii) **Provide a list of the IT functions that Veemax could separately outsource.**

### 14.12.1 Suggested Solution

This question is designed to assess the student’s understanding of centralised processing versus distributed and the issues involved with each.

i) We would expect the students’ to identify 3 alternatives including:

- Centralise data centres
- Outsource data centres
- Combination of outsourced and centralised data centres e.g. retaining the most critical functions and outsourcing the less critical ones.

The factors that the student should assess includes:

**Cost of each option.**

- Centralisation costs that need to be taken into consideration include environment and infrastructure costs, maintenance costs, administration, support costs, technology obsolescence costs, data communications costs, software license costs and data recovery/redundancy costs.
- The outsourcing option will incur many of the above factors and will also depend on contracting arrangements. These must include support, location of work and support, ownership of applications that will be used and how the deal is structured.
- Transition, conversion and long-term costs likely should also be investigated.

**Infrastructure.**

- Requirements that need to be assessed include the space required for the data centres, the network and communications links, staffing and the IT organisation itself. These considerations all have important implications for Veemax. For example, consider the business continuity issues concerned with providing a satisfactory response time to the centres.

**Applications.**

- Consider the impact on applications in each option if there are regional differences, or if there are licensing implications of choosing a centralised system and if all requirements are the same for each centre.
- Considerations should also look at the longer-term requirements of Veemax and if the option chosen will impact on the strategy or future choices.

**Hardware.**

- Centralised and decentralised systems will mean different capacity and performance issues. Also need to consider life expectancy of equipment and whether it fits in with Veemax’ strategic direction.

**Business**

- The impact on business service must be assessed. What is best to serve the customers? How will the business units be co-coordinated if the systems are outsourced? What impact will this have on budgets? How much training and re-training will be needed for each option?

ii) **Outsourced Services**
Almost all the current IT Services could be outsourced from planning to support. Recommendation to management should consider:

- What systems and activities are strategic to the company’s business?
- How much will outsourcing save the company?
- Does the company have access to the necessary skills and knowledge?
- Will outsourcing help support the company’s future directions?

While there isn’t a great deal of information available for making this decision, the student should have a sufficient understanding of outsourcing to be able to identify some of the more common outsourcing options that might suit Veemax including:

- Centralised data centre
- Operate the data centre
- Maintain current applications
- Develop future systems
- Operate the network
- Provide user support
- Provide PC and system support
- Handle systems administration functions.

14.13 **Patak’s Fine Silks**

Patak’s Fine Silks manufactures silk for the fashion industry. Patak’s has been operating for over 15 years and it now commands a healthy 30% of the local market. Its systems work well although the IT Manager has repeatedly requested additional funds to upgrade the equipment and systems that are running near capacity.

The company has just been sold and the new owner is looking to make the company more profitable and undertake an expansion program to raise its profile. Patak’s new owner is extremely interested in the opportunities that ecommerce could offer the company and wants the Board to support him in pursuing such a strategy. The Board comprises 12 members, 8 members who have served more than 3 years and 4 new members.

You are the IT Manager and the new owner has asked you to prepare a presentation to the Board on the opportunities and risks of adopting an ecommerce strategy and what the company might do about it.

You may use PowerPoint but include the notes you might use to guide you through the presentation.

Would you provide any handout? Why or why not? If so include these in your answer.

14.13.1 **Suggested Solution.**

The questions seeks to test if the student can distil a lot of information into a meaningful, short presentation on a real IT issue with a specific audience in mind. Even though there is no provision for the students to present their answers, the answers submitted should demonstrate an understanding of the use of PowerPoint to present the facts and back that up with the written words.
Students’ answers will vary but the format and presentation should be well structured to suit the intended audience of senior management level. We would expect slides to contain no more than 6 – 8 dot points, be clear and follow a standard template.

- Handouts would be advisable for this presentation as the new owner seeks to obtain support from the Board. Handouts will provide the Board members with material that they can refer to on an ongoing basis.
- The student’s should assume no, or limited, knowledge at Board level about ecommerce and the latest technologies. A suggested outline for the presentation follows:
- Agenda – tell them what you are going to cover in the presentation.
- Current IT System – it would be a good idea to set the scene for the new Board members in terms of the current architecture and issues. This should be high level only but should highlight that something must be done even if the Board decides not to proceed with an ecommerce strategy.
- What is ecommerce? Introduce the topic and explain what it means. Use examples where possible.
- Terms and technologies. Provide a high level introduction of some of the new terms they might not have heard about e.g. website, extranet. A handout of definitions might prove useful to the Board members.
- What are the advantages?
- What are the risks?
- Next Steps – present some alternatives for taking the next step for example it would be necessary to undertake a Strategic Planning exercise to establish the framework for an ecommerce strategy.

Questions

The answer on benefits and risks should include some of the following considerations.

Advantages

- Competition. New markets are available through ecommerce technologies such as website which has global reach and it also permits targeted marketing.
- Wider audiences. Traditional marketing for Patak’s is confined to the local market. Ecommerce technologies will allow Patak’s to expand its customer base regionally, nationally and globally. A Website will extend its reach to a potentially broad audience.
- Cost effective marketing channels. Extranets will allow Patak’s to form closer relationships with manufacturers and designers and thus establish multiple marketing channels quite cheaply.
- Innovative marketing. New technologies allow more meaningful material to be produced e.g. streaming videos to demonstrate the product or detailed catalogues complete with pictures and price lists.
- Cost Reduction. Many ecommerce technologies allow streamlining of the supply chain, new cost-effective alliances and more effective warehousing and delivery modes. Consider the cost reduction effect of technologies enabling virtual warehousing – producing goods only when orders are received and avoiding costly inventory collections.

Risks

There are many risks associated with ecommerce and the IT risks may be categorised into 3 areas.

- IT Infrastructure risks. These risks relate to the hardware and infrastructure that is required to keep systems accessible and operational to support the business. Risks can arise from
unauthorised access, physical loss of equipment, inadequate emergency plans, improper disclosure of information or inadequate encryption.

- **IT application risk.** Most of these risks are the same as the traditional risks of IT applications including bugs and errors, inadequate testing, inadequate integration of systems, inadequate reconciliation, lack of audit trails and lack of version control of programs.

- **IT Business process risks** include transaction data not transmitted efficiently or completely to accounting systems, backup systems only addressing the ebusiness processes, design and implementation of interfaces not appropriate, and controls applied to one process without regard to the entire process.

Other risks include legal risks e.g. privacy, confidentiality and regulatory issues that may differ from one country to another e.g. textile standards.

14.14 **Controls**

You are the Computer Audit Manager of GGG Limited (GGG). The company manufactures and distributes ceramic tiles throughout Asia. The company is in the processes of restructuring its operations and implementing a new financial system called BIGSYS. The new system includes modules for sales orders, accounts receivable, purchase orders, accounts payable, fixed assets, general ledger and financial statements as well as a report writer.

In the past, a lot of company time and money was spent on non-value added reporting. Extensive reporting requirements have been imposed by head office and the branch sites have also tailored some of their accounting systems to fit their own internal and external reporting needs. The changes are typically made by one of the in-house programmers very quickly as part of their daily support duties. This has led to information that is not used and information that is not comparable between the different branches. Further, there is a lack of confidence in the accuracy of information from the current systems unless double-checked or additional manual controls are established. The external auditors have chosen not to rely on system controls in a few areas such as inventory and accounts receivable.

Users are provided access to all the current system modules and are cross-trained in different areas to allow for extra help during busy periods or when key staff are away due to illness or annual leave. There continues to be pressure to better leverage employees including extensive empowerment of management and staff at all levels.

The new financial system is being used to help establish more cost-effective and consistent financial processes across the business. The system will provide for a more distributed computing environment and additional features will be available such as remote access, Internet access and integrated system controls.

A project team has been formed to:

- set-up and configure the system parameters to satisfy GGG’s requirements based on the business needs and industry best practices;
- tailor, where critical, the new system primarily in the sales order and reporting areas; and
- complete data conversions and establish interfaces with a few other systems such as the payroll and manufacturing systems.
Required

a) Prepare a brief overview to management outlining internal audit’s proposed involvement in the security, audit and control design and implementation work for the new financial system. The overview should include explanations about the:

i) current control environment and business plans that could give rise to added control risks;

ii) key outcomes and benefits from internal audit’s involvement in the control work; and

iii) control work approach including scope and key steps.

b) Outline the topics that need to be addressed in an information security policy for GGG. This should not be just a list of security mechanisms but rather a structure for preparing a security policy document for GGG. Describe in more detail the key security policy matters that need to be addressed regarding GGG’s future use of the Internet including topics related to scope, requirements and responsibilities.

14.14.1 Suggested Solution

The following lists key issues and principles associated with this question:
As with any consultant or resource’s involvement in a system project, management need to understand the value of involving audit staff to proactively assist in the control design and implementation work for new systems. Early involvement of control specialists will help ensure that the new systems will be implemented with an integrated set of controls, avoiding a subsequent “band aid” approach.

An Information Security Policy is provided to confirm the company’s security goal, clarify rights and responsibilities, provide guidance / requirements and rely on employees’ common sense and good judgement.

1. Potential Problem Areas
The following lists possible problems candidates may encounter with this case study:

- Many candidates should be comfortable with this question if they have an audit background and this may result in solutions focusing more on control techniques (e.g., input, process and output control methods) rather than the control design risks, benefits and approach.

- Some candidates may focus on audit’s role being more of an adviser, quality assurance or monitor. This is considered less effective than active involvement although such roles can also be included.

- Information security topics may be focused on particular security mechanisms (e.g., password control, user access validation) and exclude key matters related to purpose, scope and enforcement processes. Candidates were specifically instructed that the solution “should not be just a list of security mechanisms but rather a structure for preparing a Security Policy document for GGG”.

a) Solution Summary - Control Design

It is well established that appropriate (internal) audit involvement in system development can contribute significantly to a successful system development or implementation project. The following is a brief overview outlining Internal Audit’s proposed involvement in the security, audit and control design work for the new system.

i) BACKGROUND – CURRENT CONTROL ENVIRONMENT
The following summarises the current control environment of GGG:

**Security** - need to strengthen security regarding system access, segregation of duties, remote access and Internet access. Users are multi-skilled and that can be a good thing. However, it is important to maintain reasonable segregation of duties. The fact that controls are poor, users can get changes made and there are will be extensive report writing features which could give cause for concern.

**System Development and Maintenance** - need to establish more rigorous / standardised approaches for program changes including testing. GGG has allowed an autonomous method of working that may have advantages in ensuring that staff and managers feel that they have control of their domains but this can cause problems when trying to tailor packages. The definition of user requirements will have to embrace multiple and diverse needs and there could be disagreement between what Head Office (HO) wants and what the branches need. If the user requirements are allowed to evolve the project will never end. Requests for changes need to be evaluated in the light of a cost benefit.

**System Controls** - need to enhance system controls to ensure information accuracy and reduce need for double-checking or additional manual controls. However, this needs to be balanced with the need for automated controls and reports to have a clear purpose. As a general rule controls and information that cannot be acted on or used to help achieve the business goals are not required. As well, users may not design sufficient controls themselves due to lack of experience thus leading to inaccurate or incomplete data.

**Audit Controls** - need to enhance controls in systems to allow for greater audit reliance such as for inventory and accounts receivable. External auditors have not relied on controls and this would indicate that they are non-existent or not functioning. While there is no evidence that the systems are producing inaccurate data, such as a qualified audit report, it is not an acceptable situation. It may be that external audit costs are higher because of the additional work performed.

The following business plans of GGG that could give rise to added control risks:

- **Greater distributed computing** - e.g., possibly lack of data synchronisation between branches, loss of traditional audit trails and significant increase in number of users
- **Reorganisation of business** - e.g., possibly employee roles will be unclear
- **Pressure to leverage employees and staff empowerment** - e.g. possibly lack of duties segregation
- **Interfaces** - e.g., possibly poor data integrity between systems

**OUTCOMES AND BENEFITS**

- **Controls** - help ensure that the processes and systems being established are well controlled, auditable and secure rather than an “add-on”. This includes:
  - completeness
  - accuracy
  - authorisation/confidentiality
  - timeliness
  - validity
  - pertinence
  - consistency
  - presentation / disclosure
CASE STUDIES

availability/continuity

• Practical - strive for an appropriate balance between satisfying control objectives and users’ needs. Internal audit staff should have greater external experience in control design to help apply best practices.

• Integrated - early involvement of control specialists will help ensure that the new systems will be implemented with an integrated set of controls, avoiding a subsequent “band aid” approach. This allows for simplified and more precise efficient controls as well as greater technology flexibility that is not restricted by burdensome “add-on” controls.

• Assurance - provide audit assurance and the implementation of reliable functionality, controls, audit trails and security will help save audit and operation time and costs (e.g., by automating controls). Internal Audit should be able to consider the “big picture” and have a more independent corporate interest to help ensure realistic expectations and benefits realisation.

• Other - general benefits not directly associated with the controls design could include Internal Audit’s more direct access to management, ability to act as an arbitrator, help ensure adequate documentation and ability to carry out quality assurance if necessary.

(iii) APPROACH

• Scope - The scope of Internal Audit’s involvement is as follows:

  Activities - the controls, audit trails and security work cover both the business processes and computer systems excluding the interface system such as payroll and manufacturing.

  Teamwork - the Internal Audit representatives will work closely with representatives from the project team to define, document and implement the controls and will keep management well informed on the work status.

  Best Practices - controls will be established based on researched best practices. Sources of the best practices will be confirmed early in the project.

  System Reviews - excludes post-implementation audit reviews of the processes, interfaces and controls (both manual and automated) in the live environment that would be performed as part of separate audit assignments, as appropriate.

• Steps - the controls design work will include the following steps (candidates may provide other approaches and further details):

  Plan the Assignment - to assess the best design approach and support needs. This includes identifying the required resources from Internal Audit.

  Conduct Controls Workshop (or meetings) - to gain understanding and support of the project team.

  Define Control Objectives, Integrity Requirements and Integrity Techniques - for high and medium risk areas within each business process. This will include evaluating inherent risk and control risk of the project by carrying out a risk assessment exercise. As well, a review of the systems development and program maintenance policies and procedures is required with improvements to be proposed.

  Support Process Teams in the Configuration of Security, Controls and Audit Trails - including interfaces and data conversion.

  Support Testing of Controls and Security - as part of planned systems test activities.

Additional Discussion Questions

• What types of controls could be considered early that would be less likely to be considered after the system is implemented?
• Why could management resist audit’s involvement in the project, opting just for the post-implementation review approach?

b) Solution Summary - Security Policy
Security policies will primarily focus on the security characteristics of the company’s principal computer platforms or the perceived security risks which if not managed could cause significant loss or inconvenience to the business. The following outline suggests topics that need to be addressed in the Information Security Policy for GGG. The actual format would be dependent on the company’s current format for policies.

SCOPE AND RESPONSIBILITIES
• **Purpose** - state overall purpose such as to help protect company information assets including systems that are to be used for business purposes only. Overall, the policy is provided to confirm the security goal, clarify rights and responsibilities, provide guidance / requirements and rely on employees’ common sense and good judgement.

• **Staff Covered** - state the policy applies to all employees (full-time and part-time), contractors, suppliers, customers, service providers and other parties with approved access to company information assets.

• **Information Sources** - state information sources covered under the policy such as intellectual, electronic and hard copy (written and printed).

• **Information Assets** - state company information asset covered under the policy such as hardware and applications.

• **Staff Responsibilities** - state overall responsibilities of staff such as protecting company data and personal computers, keeping passwords confidential and reporting any security risks or possible breaches.

• **Security Roles and Responsibilities** - state key responsibilities for enforcing the security policy such as security function, information and system owners, departmental responsibilities (e.g., audit, human resources, media relations).

• **Related Regulations and Terms** - reference related regulations and employment terms that are applicable in conjunction with the security policy such as ethics, data protection, privacy, and confidentiality agreement.

• **Compliance** - state ramifications of security breach such as failure to comply will result in disciplinary action, including possible termination and legal actions.

REQUIREMENTS / GUIDANCE
• **Base Security** - state the security policies such as those related to access, data protection, and asset protection. The policies should:

  not be fixed to hardware or software currently in use.

  be a balance between excessive coverage and being too generic.

  focus on security risks rather than listing the type of security techniques and tools used.

  state the reason for a security requirement and examples of inappropriate use to help clarify each security requirement.
Base security areas to be considered in addressing the risks include:
- firewalls;
- anti-virus tools;
- access control;
- enhanced user authentication;
- encryption;
- physical security; and
- disaster recovery plans.

- **Security Risk Management** - state process for assessing and managing security risk such as identifying information assets, assessing threats, and defining actions (e.g., accept risk levels, transfer risks, mitigate risks with controls, or avoid risks).

- **Feedback/Escalation Procedures** - outline incident reporting approach, as well as follow-up requirements and resolution criteria.

Note - Candidates may provide more details on the types of base security topics to be covered for GGG such as remote access, new user accounts, password protection, firewall protection, etc.

**INTERNET USE**

The following describe the key security policy matters that relate to GGG’s future use of the Internet:

- **Data Security Procedures** - policies need to be established regarding the protection of data from GGG’s systems that could be accessed through the Internet. For example:
  - Establish firewall protection over modem or LAN access;
  - Encrypt sensitive information being transmitted over the Internet;
  - Require use of virus protection software (set company standard) and keep employees aware of the virus risks associated with downloading data or systems from the Internet;
  - Prevent or restrict use of trusted network relationships (i.e., require unique passwords);
  - Limit or control powerful network management features;
  - Prevent access ability using command line instructions;
  - Disabling system-default accounts;
  - Require use of passwords that are not easily guessed (e.g., 6-8 alphanumeric characters);
  - Restrict number of invalid log-in attempts to help prevent the password guessing;
  - Restrict display of company information or system help until a user is authenticated;
  - Record security violations for subsequent review and follow-up; and
  - Monitor security and immediately correct any weaknesses that become known.

- **System Access and Use Protection** - policies need to be established regarding who and how access will be provided to the company systems through the Internet. For example:
  - Qualifications and/or approval process for employee user access to/from the Internet. Who should have access? Is all staff to be allowed access or just a few?
• Qualifications and/or approval process for external user access to GGG’s financial systems from the Internet. GGG may provide customers with access to systems such as order entry, inventory and accounts receivable. The extent of information they are given access to must be restricted and the prior data security procedures must be adhered to.

• When is access allowed? Is access restricted to business hours? Can staff access the Internet through the company system from home?

• Types of remote access allowed.

• External facilities to be allowed access internally.

• Which software is to be used? Will GGG standardise on one product only?

• What is Internet access to be used for? Can orders be placed to suppliers or from customers?

• What is it not to be used for?

• **Secure E-mail Use** - policies need to be established regarding the use of e-mail. A separate e-mail policy may exist for GGG and should be referred to and extended to cover Internet e-mail. For example:

  • E-mail is to be used for business use although incidental personal use is acceptable bearing in mind the company owns the e-mail account. Incidental personal use could be further defined to exclude advertising, chain letters and offensive material including humour and images.

  • Business judgement and ethics need to be applied regarding what information is e-mailed over the Internet. The company may wish to further define what sensitive information cannot be sent over the Internet or must be encrypted.

  • Classes of e-mail may be established with related security requirements (e.g., casual, official, sensitive, graphics and audio, copyright material, non-business related).

  • Some company representation in e-mail or user groups may need to include disclaimer notices to say that comments are those of the individual.

**Additional Discussion Questions**

• How much of security protection is common sense and does this need to be stated in a policy?

• How long should a Security Policy be?
A

Abnormal job termination reports · 159
ACCESS CONTROL SOFTWARE · 383
Accounting for IS costs · 185
accounting rate of return · 25
ACS · 329
Active monitors · 381
Active X · 126
Administration - IT · 342
Analytic Applications · 201
Analytical decisions · 27
Anthony · 76
antivirus software · 381
Application areas · 102
Applications architecture · 61
applications portfolio · 83
ARPANET · 121
Assumptions · 102
Audit Guideline · 277
Audit Guidelines · 293
AUDIT PROCESS · 294
Authentication · 127, 145
Availability · 304
AvantGo Mobile Sales · 205

B

Baan · 221
Batch Processing · 36
Bespoke software · 358
Boot viruses · 125
Boston Consulting Group (BCG) · 100
Bottom up planning · 69
Budgeting · 306
Bulletin boards · 122
Business information strategy · 56
business model · 138
Business objectives · 101
Business strategy · 51
Business System Planning (BSP) · 58
business systems planning · 74
Business to Business Models · 142
Business to Consumer Models · 139

C

Call-back buttons · 122
Campaign Management · 200
Centralisation - of IS department · 349
Centrally planned · 62
check digits · 334
Clickstreams · 131
COBIT · 271
COBIT Framework · 277
Collaborative Computing · 166
Command level end-users · 177
Communications architecture · 60
Competitive advantage · 92
COMPETITIVE ADVANTAGE · 92
Componentisation · 225
Computer Aided Design · 33
Computer Crime Exposures · 382
Computer operations · 156
Computer Society of Pakistan · 165
computer supported co-operative work · 167
Computing architecture · 60
Confidentiality · 301
Console logs · 159
Contact Center · 199
Contagion · 78
Control · 78
Control Objectives · 304
Controls Frameworks · 269
Controls Over Viruses · 380
cookie · 131
Copyright law · 355
Copyright, Designs & Patents Act 1988 · 356
Corporate strategy · 51
COSO · 272
Cost Benefit Analysis · 182
Cost of information · 24
Cost-leadership · 93
Critical success factors · 75, 106, 107, 216
Critical Success Factors · 289
CRM · 3, 94, 95, 139, 141, 197, 199, 200, 201, 202, 203
CRM Suite Suppliers · 202
Cross charging · 189
Cryptography · 127
CSA · 73
CSF Analysis · 76
current situation analysis (CSA) · 78
Customer relationship management · 94
Customer Relationship Management · 197
Customer-Centric Intelligence Applications · 200
Customer-Facing Applications · 199
Customer-Touching Applications · 200

D

Data Administration · 79
Data administrator · 343
data analysts · 344
Data architecture · 61
Data Entry Personnel · 157
Data Mapping · 204
Data processing programmers · 178
Data security · 376
Data sources for CSF · 75
data warehousing · 41, 201
Data Warehousing · 201
database administrator · 343
decentralisation (of IS department) · 348
Decision Making · 26
Decision Support System · 31
Decision support systems · 31
Decision-making · 23
**Default passwords** · 124
**deletion checks** · 334
Dial-back security · 127
**Differentiation** · 93
Difficulties with outsourcing · 171
Digital Signature · 145
discounted cash flow · 25
Distributed Systems · 168
Dot-Com E-tailers · 141

**E**

Earl M · 82
Earl on planning · 70
**Earl’s Grid** · 78, 80
E-business models · 138
E-cash · 147
E-Checks · 148
Eclectic (mixed) planning · 70
ECML · 145
e-commerce · 226
EDI · 95, 119, 129, 133, 146, 149, 150, 227
Electronic cash · 144
Electronic Commerce · 128
Electronic Data Interchange · 133, 166, 169
Electronic marketing · 130
E-Marketplaces · 142
Encryption · 127
Encryption of data · 328
End User Computing · 176
**End-User support personnel** · 177
Enterprise analysis · 74, 106
Enterprise resource planning · 211
Enterprise Resource Planning · 94
Environmental Analysis · 73, 84
Environmental control · 323
Ergonomic · 321
E-supply chain · 227
E-tailers · 141
E-Wallets · 148
Executive Information System (EIS) · 449
Executive summary · 102
Executive support system (ESS) · 30
Executive Support Systems · 30
**existence checks** · 334
Expert systems · 37
Expert Systems · 36
Explicit knowledge · 38
**External analysis** · 85

**F**

Field Service Automation · 200
**firewalls** · 123
Firewalls · 127
**Focus** · 93

**format checks** · 334
four principles of privacy · 165
Fraud and data theft · 328
Free market · 62
**Frequently-Asked Questions** · 122
Functional support personnel · 177

**G**

General protective measures · 335
generic framework for developing an IS strategy · 63
Generic strategies · 92
Goals · 102
Griffiths · 182

**H**

Hacking · 124, 354
Help desk · 344
**Heuristic decisions** · 27
high-level controls · 285
Hoax Viruses · 126
HOW WEBTRUST WORKS · 299

**I**

Implementation · 102
implementing an ERP · 215
inbound logistics · 94
Information
value · 22
Information centre · 344
Information engineering (IE) · 57
Information Engineering Methodology · 58
**Information Management** · 26
INFORMATION SYSTEM · 28
Information systems · 106, 247
Information systems – value of · 184
Information Systems (IS) strategy · 55
Information Systems Department · 340
Information Systems Project (ISP) · 58
Initiation · 78
Input/Output Control Function · 157
Insourcing · 170
Integration · 79
Integrators · 133
**Integrity checkers** · 382
intellectual capital · 38
internal rate of return · 25
Internet · 121
investment appraisal methods · 25
Investment workstation · 34
IS / Business strategy alignment · 97
IS costs · 182
IS functionality strategy · 56
IS Operations · 155
IS Operations Staffing · 163
IS/IT strategy · 57
ISDN · 123
IT governance · 248, 250, 254, 283, 290, 293
IT Operation Strategy · 155
IT strategy · 53
Ives and Gordon · 41

J

J.D. Edwards · 219
Job Accounting · 160
Job Rerun Report · 159
Joint venture/strategic alliance sourcing · 170

K

key encapsulation · 128
key recovery · 128
Key Recovery Agent · 128
Knowledge Work Systems · 33
Knowledge Workers · 33

L

Leading edge · 62
Lights Out Operations · 156
linear programming · 27

M

Macro Viruses · 126
Maintenance · 102
Management Guidelines · 277, 286
Management Information Systems · 30
Maturity · 79
Maturity Model · 287, 288, 293
McFarlan · 54, 81, 99
McFarlan and McKenney · 83
McKenney · 81
Micro Payment · 146
Mobile devices and SFA · 205
Monopoly · 62
Moriarty and Swartz · 95
Multipartite viruses: · 125
Multiple/selective sourcing · 170

N

Natural disasters · 330
Navigator System Series · 58
Necessary evil · 63
net present value · 25
network analysis · 27
New entrants · 90
Nolan’s stage Model · 78
Non-programming end-user · 177

O

Office Automation Systems · 34
Online Banking · 147
On-Line Privacy · 301
On-line processing · 36
Operational information · 20, 77
Operational level information systems · 28
Operational personnel · 345
Operations · 102
Operator Assisted Operations · 156
Operator problem reports · 159
Operator work schedules · 159
Opportunities and Threats · 84
Oracle · 219
Organisational costs · 183
Organisational structure · 102
outbound logistics · 94
Output distribution reports · 159
Outsourcing · 228

P

Parson Generic IS strategies · 61
Parson, G · 98
payback method · 25
PeopleSoft · 219
Peppard · 83, 95
PEST · 52, 84, 85, 106
Polymorphic viruses · 126
Portals · 141
Porter · 54
Porter's five forces model · 90
Porter's value chain · 93
Privacy · 165
private key · 127
Problem Management · 161
Process and Domains · 272
Program Change Control · 162
Program viruses: · 125
Programming level end-users · 177
public key · 127

Q

Quality Assurance · 162

R

Rational Model · 52
Recharges at cost · 188
Recharges at mark-up · 189
Repetitive Strain Injury · 321
Reporting · 201
Supply chain process management · 208
Support/Help Desk · 163
SWOT · 52, 73, 86, 107
System development staff · 344
Systems' architecture · 59

T

Tacit knowledge · 37
Tactical information · 20, 77
Tactical level information systems · 28
Technology costs · 182
The Computer Misuse Act 1990 · 354
The Data Protection Act 1998 · 353
The data protection principles · 353
Threats to the organisation · 320
Top down planning · 69
Total outsourcing · 170
Transaction Integrity · 303
Transaction processing systems · 36
Transaction Processing Systems · 35
Trojans · 126
Trust Services · 300, 301

U

Unauthorised access · 329
Uninterruptible Power Supply · 330
Unstructured decisions · 26
Unstructured decisions · 27
User support staff · 343

V

VALUE OF INFORMATION · 22
virtual company · 133
Virtual reality · 33
Virtual Reality Modelling Language · 34
Virtual Supply Chain · 133
Viruses · 125, 329, 355

W

Ward and Griffiths · 95
Ward, J · 56, 97
Warwick · 80
WebTrust program · 299
Where We Are · 64
Where We Want To Be · 65
Where We Were? · 64
Worms · 126