Accounting information systems in a computer environment

Only study guide for

AIN1501

Authors:
Mr NJ Booyse
Ms C Leonard
Mr DJP Scott
Ms GM Viviers

Contributor:
Mrs A Mc Gee

Curriculum and learning development:
Ms M Madiope
Ms GNW Moleko

College of Economic and Management Sciences
School of Accounting Sciences
Department of Management Accounting

University of South Africa,
Pretoria

Printed and published by the
University of South Africa
Muckleneuk, Pretoria

AIN1501/1/2013–2019

98908480

3B2

New PRTOU-Style

CONTENTS

OVERVIEW

Welcome

During the last twenty years, there have been significant changes in the functioning and development of the business world and the economy. A dramatic increase in innovations and technology forced businesses to perform more professionally. Computers and other communication networks have been a driving force behind this shift and contributed much more than ever believed. It is difficult to imagine that, in just 20 years, processes changed from slow, manual and cumbersome to instantaneous, cutting-edge technology that is fast and reliable. This resulted in what we call the *new economy*, a term that is not yet well known. The *new economy* is based on these technologies and continuing to grow in importance. What exactly is the new economy? In its most basic form, it is a global state where communication technology creates global competition. It creates change so rapidly that many people refer to it as a revolution instead of an evolution.

To those of you who wish to enrich your minds, welcome to the AIN1501 module! As Henry Ford said, ''Anyone who stops learning is old, whether twenty or eighty. Anyone who keeps learning today is young. The greatest thing in life is to keep your mind young.''

Please note that successful completion of this module will not make you a computer specialist; it will rather ensure that you have good background knowledge of accounting systems in a computer environment. You will be able to use this background knowledge in your studies, whether you wish to become an accountant, an auditor, or a business specialist. This module is therefore a basic but important building block for other modules that you still have to master. The module is not practically oriented; however, it does give you the knowledge base you will need to deal with problems in later modules. In the following module, Practical accounting data processing (AIN2601), you will have the opportunity to apply the knowledge and skills you acquired in the AIN1501 module practically.

Because technology changes so rapidly, information technology is not a rigid or unchangeable area of study. It is therefore your duty as a student to ensure – after the successful completion of this module – that you keep up to date with the latest developments in the relevant field. Knowledge is only meaningful if it is relevant and up to date! As Richard Anthony de los Santos II said, ''In all the years I've lived, I have yet to stop learning''.

Before starting your studies, it is important that you take note of a few important matters that follow below.

General objectives of this module

Information in the global economy is instantaneous and easily accessible. This speeds up an organisation's business cycle and allows it to maximise profit in shorter periods. Technology result in that people use their brainpower significantly more than physical power, and this requires specific education and knowledge.

AIN1501 is intended for people who are interested in qualifying as accountants or management accountants, including students who are planning to register at SAICA or

CIMA. Students who are working towards a qualification in the field of information technology will also benefit from this module.

This module provides you with the theoretical knowledge needed to understand the fundamental aspects of computerised information systems in a business environment. The theoretical knowledge will enable you to function as a user, designer, or evaluator of accounting information systems in the workplace.

Lastly, the AIN1501 module provides you with the knowledge you need, to understand the computer principles and concepts concerned with information. It aims to make you aware of computers and information systems, with specific reference to their operation, the particular functions they can perform in the processing of accounting data and the associated risks and controls.

Prerequisites and co-requisites

Students who register for this module should be able to

- communicate effectively in the English language
- learn from predominantly written material
- communicate what they have learnt comprehensibly in the medium of instruction
- take responsibility for their own learning and progress with guided support

It is assumed that students have

- reading and comprehension skills to enable them to read questions and case studies, comprehend their content and follow a logical thought process
- the ability to apply the basic principles they have been exposed to in the tutorial matter to specific questions or case studies and to formulate an opinion or recommendation, or draw a conclusion from this application

Structure of this study guide and the module

The module is divided into five distinctive parts, each containing several topics. Topics are the main study areas in each part, and each topic is divided further into study units. You will find the outcomes, which you are required to achieve for each topic in this guide, at the beginning of each topic.

The parts of the course are described below.

PART 1

Explains the nature of information systems.

(Topic 1)

This topic introduces you to information, information systems and information strategy and it deals with the information system department.

PART 2

Explains the information technology infrastructure.

(Topics 2–3)

The second topic deals with information technology components and terminology, such as hardware and software, and the third topic explains computer networks and data communication.

PART 3

Describes the security and ethical risks associated with the use of computers in business and the controls that should be in place to minimise these risks.

(Topics 4–6)

This section deals firstly with the threats and secondly with the controls in a computerised environment. Topic 6 explains privacy and ethical matters.

PART 4

Explains the principles related to information system development.

(Topic 7)

This section deals with system development processes.

PART 5

Distinguishes between strategic information systems and their business applications. It also explains concepts of electronic commerce (e-commerce) and its risks.

(Topic 8–9)

The first section of this topic concentrates on the application of different strategic information systems and Topic 9 continues by discussing the threats and controls associated with e-commerce.

Content AIN1501 (figure 1)

Figure 1 below contains a schematic presentation of the content of the AIN1501 module.

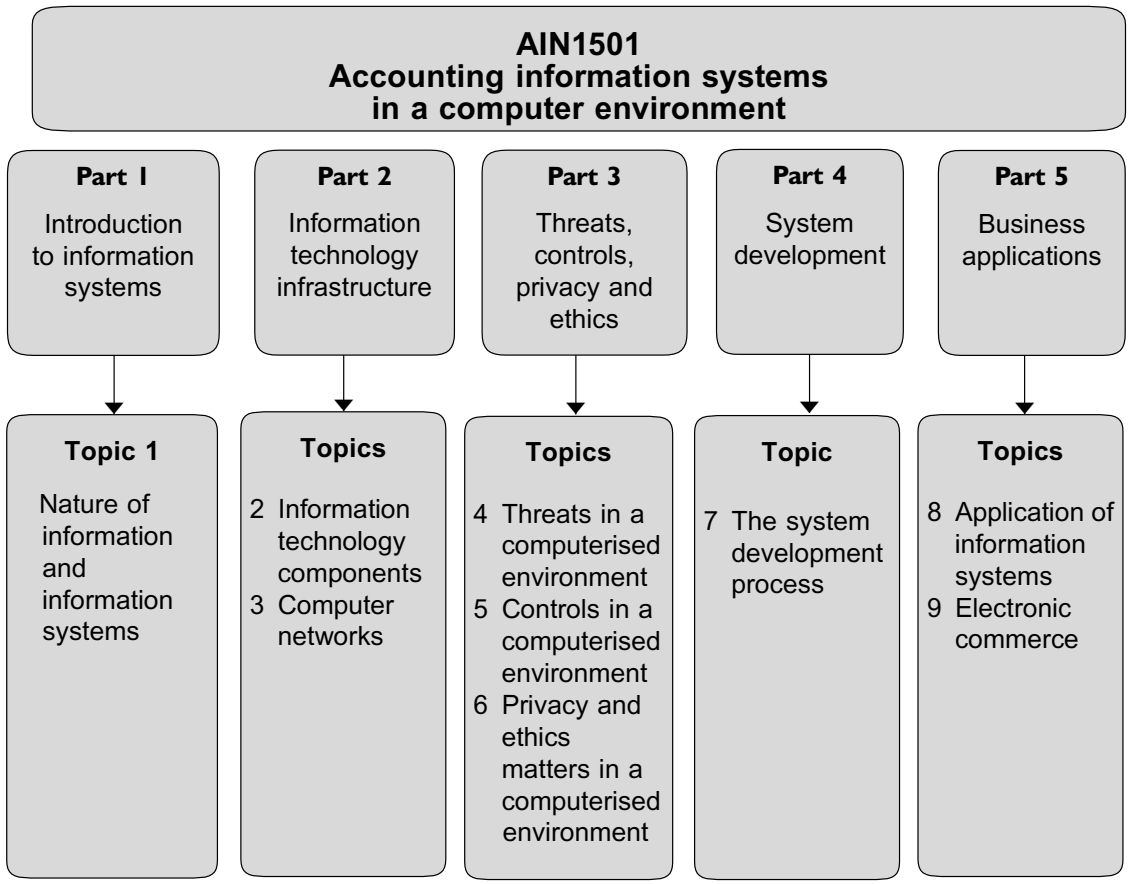


FIGURE 1: A schematic presentation of the content of the AIN1501 module

Study material and resources

Prescribed study material

The study guide – AIN1501 is the only prescribed study material for this module.

Supplementary literature/additional reading

Check for additional enrichment material on MyUnisa (https://my.unisa.ac.za).

The bibliography at the end of the study guide gives a number of additional resources if you would like to read more about specific topics.

Assignments

The assignments are set out in Tutorial Letter 101, together with the necessary instructions. Your assignments should be submitted for marking by the due dates.

It is in your best interest to answer and submit as many assignments as possible, since

- they form an important, integral part of your studies
- you will not be allowed admission to the examination without submitting the compulsory assignment
- they facilitate preparation for the examination
- some assignments, as indicated in Tutorial Letter 101, are taken into account when calculating your year mark; the higher your year mark, the better chance you have of succeeding in the module

Critical success factors

Our aim in designing the study guide was to give you the best possible opportunity to master the knowledge, skills and values required by the discipline and the demands of professional practice. To discover what other support we offer you, please refer to Tutorial Letter 101.

To ensure that you are successful in your studies, we would advise you to do the following:

- Start as early as possible on your studies. We have found that students who start early have time to reflect on their studies and formulate their own informed opinions.
- Use your time sensibly.
- Work systematically through the contents of the study guide.
- Set realistic goals.
- Believe in yourself.

We have designed this module using the SAQA guidelines with regard to the notional hours you will need to work through the course material successfully. You will need at least 120 hours to read and study all the study material, do your assignments and prepare for the examination.

Research has shown that students who complete their assignments diligently are more likely to pass their examinations than those who do the minimum.

You will not be able to pass this module successfully if you only try to memorise detail. We suggest that you allow yourself enough time to read a chapter, use different techniques to summarise the content, and spend time reflecting on the issues and principles involved.

Study programme guideline

Part	Topic No	Topic	Hours
1	1	Nature of information and information systems	14
2	2	Information technology components	14
	3	Computer networks	10
Assignment 1			1
3	4	Threats in a computerised environment	10
	5	Controls in a computerised environment	6
	6	Privacy and ethical matters in a computerised environment	4
4	7	System development process	24
Assignment 2			1
5	8	Application of information systems	14
	9	Electronic commerce	10
Assignment 3			2
Review			8
Examination paper			2
Total hours			120

Teaching strategy

Our teaching role focuses on facilitating your learning experiences towards achieving specific outcomes. Furthermore, for each of the topics that comprise this module, the learning experiences were designed with the aim of enabling you to master the learning content at a predetermined competence level.

Meaning of words

Throughout this module, we communicate the learning outcomes and self-assessment criteria phrased in terms of what you should be able to do. This process involves the use of action words, which are typically verbs or phrases containing verbs that describe what is expected from the student in the learning activity. It is our objective to ensure that the words we use to indicate a requirement clearly state what you need to do. You should also ensure that you clearly understand the requirements conveyed by the range of words we use in the study material for this module.

We list below (in alphabetical order) examples of some of the action words that you will come across in this module, together with their meanings for the purposes of this module.

Action word	Meaning
Compare	Examine in order to observe resemblances, relationships and differences
Complete	Finish/add what is required
Define	State precisely the meaning/scope/total character; make clear (especially the outline); give a concise description of the distinguishing features
Describe	Give clearly the distinguishing details or essential characteristics
Determine	Decide; come to a conclusion/make a decision, include reasoning
Discuss	Examine/consider the opposing arguments
Draft	Prepare a preliminary version
Explain	Set out the meaning of something; clarify the meaning, provide supporting evidence; argue the truth of something
Identify	Establish by consideration, select, recognise
Illustrate	Explain, clarify by means of an example to illustrate the nature, meaning and importance of something (see *Explain*)
List	Record/item, record/itemise names or things belonging to a class
Mention/ Name/ State	Specify by name; cite names, characteristics, items, elements or facts
Record	Put in writing; set down for reference and retention
Summarise	Give a condensed version; state the key aspects
Tabulate	Arrange/organise in table form

Preparing for the examination

When commencing your studies, we recommend that you prepare a schedule, which allocates time to each study unit, leaving sufficient time for revision closer to the exam.

This study guide contains what you need to complete the module successfully.

We suggest the following study method:

- Work systematically through each topic.
- Read the learning outcomes of each topic in the study guide to accustom you with the aims of each of the nine topics.
- Evaluate yourself continuously by working through the self-assessment activities provided in the study guide.

When doing revision and preparing for the examination, it is recommended that you

- review each study unit thoroughly using your detailed summaries
- attempt to answer the assignments under exam conditions and compare your answers with the solutions provided
- attempt to provide comprehensive and meaningful answers to the additional problems and questions included at the end of the relevant chapters in your prescribed textbooks

The study programme on page XV serves as a guideline for your study programme for the year.

Examination technique

Comply with the examiner's requirements by

- carefully reading the instructions on the front page of the question paper
- providing relevant answers only
- presenting your answer in the correct format
- following the examiner's instructions carefully

Satisfy the examiner by

- handing in a neat answer book

Give your best by

- planning your answer carefully
- being aware of the time allocation for each question
- reading the question carefully and planning your answer (remember to answer what is required of you)
- answering the easier questions first
- not leaving the examination venue before the allocated time has elapsed

Conclusion

We recognise the increasing impact of computer technology in the day-to-day business activities of accountants. This module (AIN1501) and the next module (AIN2601) combine the theoretical and practical understanding of accounting with the ability to define and develop information systems that harmonise human and computer resources. Accountants are in a prime position to understand the main business activities of organisations and the information needs of individuals and groups both within and outside organisations. These two modules will give you a deeper and clearer understanding of the use of information technology in information systems and of the organisational and social impact of computers.

Since you are a student at a distance education institution, you should see this study guide as your lecturer, that is, we are transferring the knowledge to you through it. Enjoy your studies and remember, the sooner you tackle the work, the more time you will have to review before the exams.

Finally, we trust that you will enjoy this module.

All the best for your studies

Your AIN1501 lecturers

Accounting information systems in a computer environment (AIN1501)

MODULE PURPOSE

This module is intended for people who are interested in qualifying as accountants or management accountants, including students who are planning to register at SAICA or CIMA. Students who are working towards a qualification in the field of information technology will also benefit from this module.

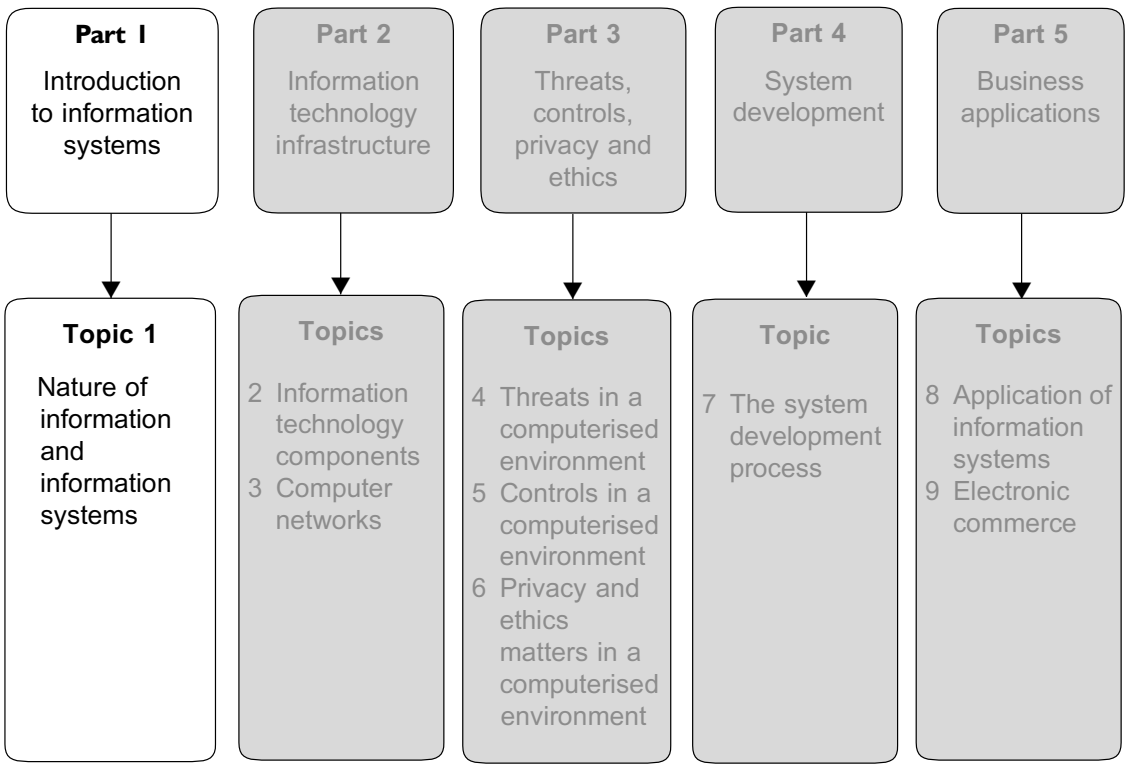
The aim of this module is to equip students with theoretical knowledge of the fundamental aspects of computerised information systems in a business environment, which will enable them to function as users, designers and evaluators of accounting information systems in the workplace.

Part 1 Introduction to information systems
Part 2 Information technology infrastructure
Part 3 Threats, controls, privacy and ethics
Part 4 System development
Part 5 Business applications

Introduction to information systems

PURPOSE

The purpose of part 1 is to assist you in developing an understanding of information and the need for information in organisations. In addition, you will be exposed to the nature of information systems and information strategy. This part is also intended to equip you with knowledge of the management of the information system department.



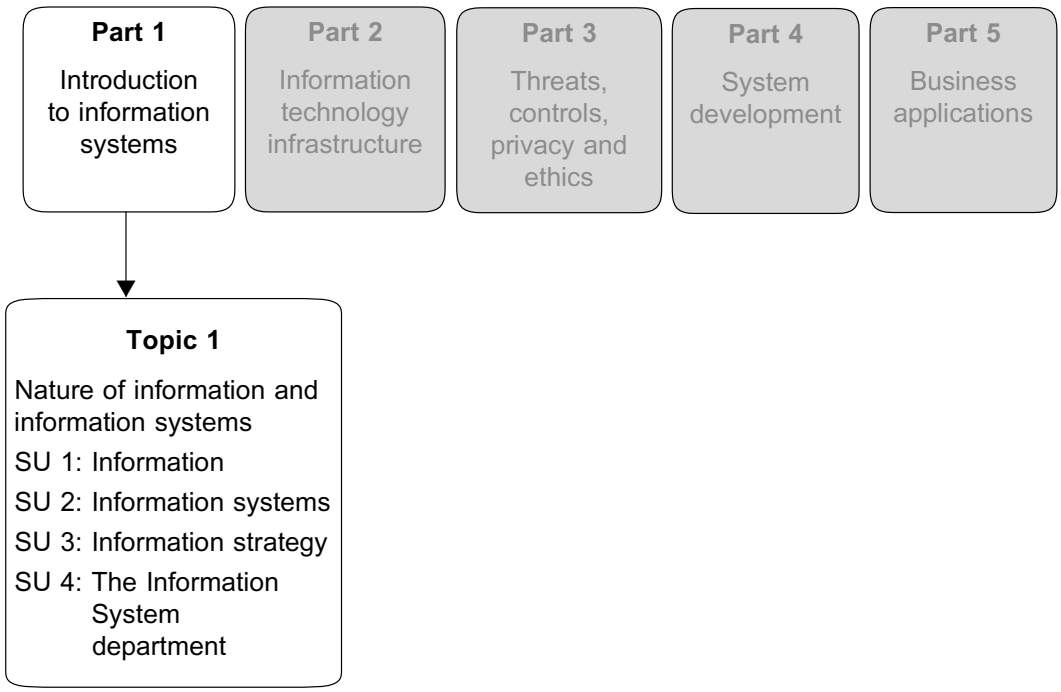
Nature of information and information systems

LEARNING OUTCOMES

After studying this topic, you should be able to

- define information and list the characteristics of information
- describe the uses and users of information in a business environment
- explain an information system and its role in an organisation
- define a computerised information system
- describe an accounting information system and the importance of having knowledge of accounting information systems
- explain an information strategy and its importance for the organisation
- describe the relationship between information, information system and information strategy
- explain concepts of the information system department

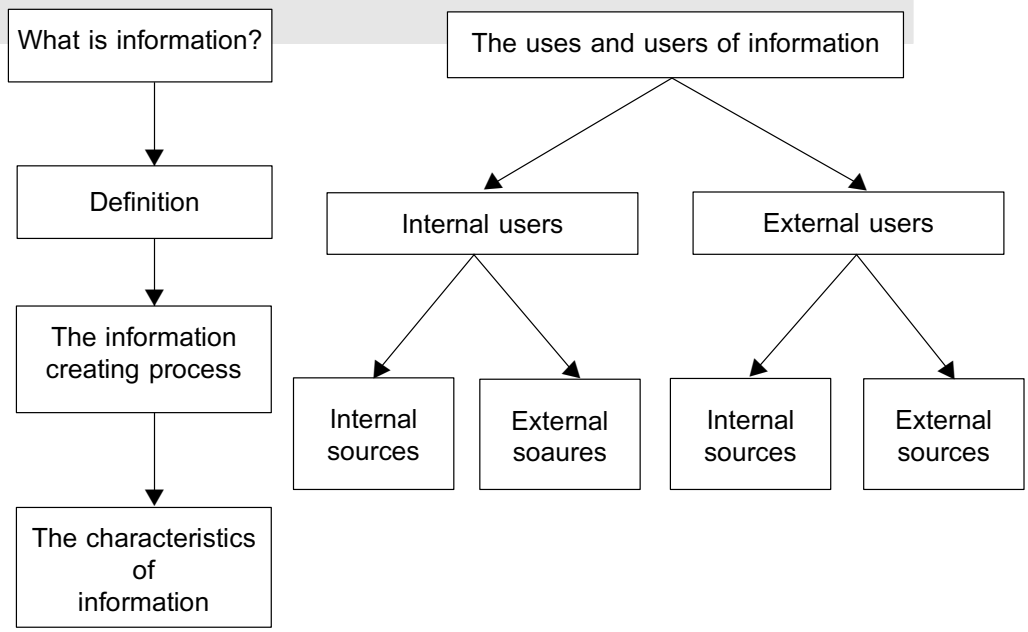
This topic consists of four study units



STUDY UNIT 1

Information

In this study unit



1 INTRODUCTION

We are living in the information age. Information is everywhere. The most obvious reason for processing data is to reduce uncertainty and therefore most organisations value information as a strategic asset. No organisation can function without information. It is one of the key elements in the support of any business process and forms the basis of an organisation's future planning and decisions. Understanding the impact of information on an organisation is crucial in running a successful business. Such an understanding helps managers to ensure that their organisation stays on track in a continuously changing environment.

In this study unit, we look at information, the characteristics of information and the uses and users of information.

2 WHAT IS INFORMATION?

To understand information it is important to look at the term ''data'' first.

*Data are the **raw material*** available for processing into information. Data consist of numbers, letters, audio and video data and relate to facts, events and transactions.

NOTE

The word *data* is actually the plural form of the word *datum.*

Information is a ***set of facts*** or ***data organised*** and processed in such a way that it provides additional value beyond that of the facts themselves. Information is derived from data or raw facts that represent real-world elements, as illustrated in the following table:

In other words, information is ***data*** that have been ***processed*** in such a way as to be meaningful to the person who receives it. This information provides knowledge that leads the user to make decisions.

In a business environment, the creation of information for decision-making can be illustrated as follows:

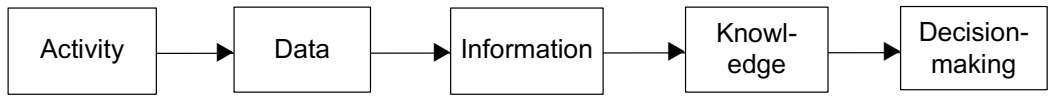


FIGURE 1.1: The creation of information

Example

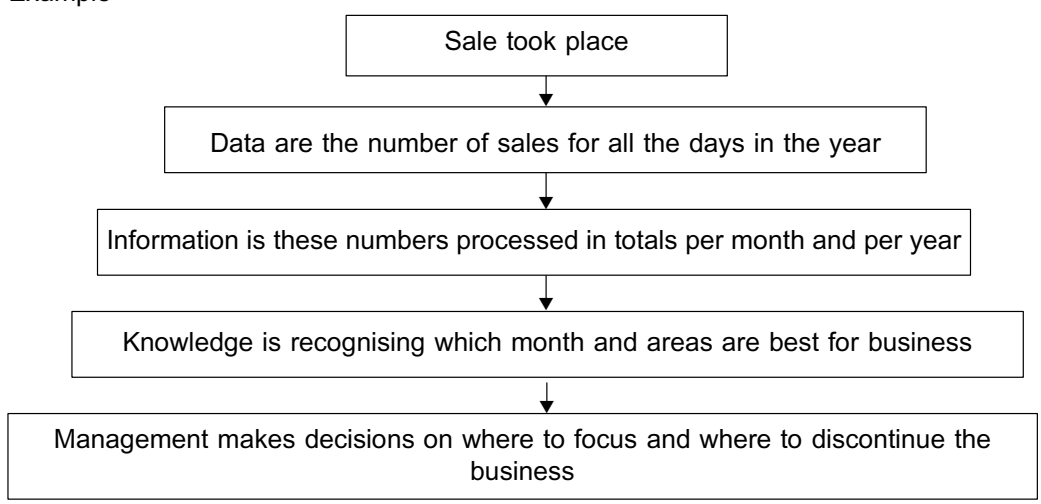


FIGURE 1.2: The creation of information (example)

The characteristics of information

When using information for decision-making purposes, it should comply with the characteristics described in the table below:

Characteristics	Explanation
Accurate	Information should be without any errors. Inaccurate data entered into a process will provide inaccurate information. Information should be checked to ensure correctness.
Accessible	Information should be easily available to users in order to meet their needs.
Up-to-date information	Information needs to include the latest possible information and recording time of data should be minimised.

Characteristics	Explanation
Detail information	Some users may need details of all events while others need a summary. Information should contain all the important facts, but no more than are necessary.
Flexibility	Information is flexible if it is usable for more than one purpose.
Relevance of information	Information should be relevant to the needs of the users.
Cost-effectiveness	The value of information should always be balanced with the cost of producing the information.
Reliability	Information is reliable if one can depend on it. Reliability depends on the source of information. A rumour is not reliable.
Timely	Information should be delivered when it is needed.
Format of information	Information should not be overly complex and should be supplied in the required format. Too much information or information in the wrong format leads to difficulty in determining what is important.

3 THE USES AND USERS OF INFORMATION

The users of information can be both internal and external users. These users of information, both internal and external, first need to be identified before decisions on information needs can be made. Such users need information in order to perform a specific task or make specific decisions.

Internal users may need information for future planning and forecasting, for measuring performance or for control in the organisation or about specific processes. External users, such as investors or financiers, may need information on the performance of the organisation for possible future investment, while clients may need information on products and services.

This can be illustrated as follows:

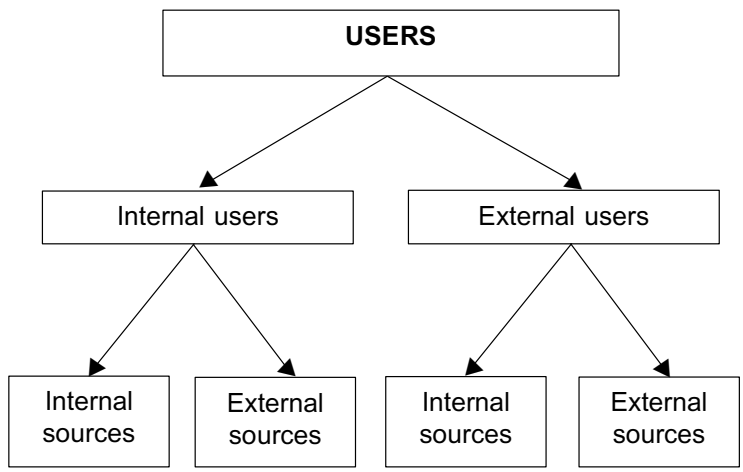


FIGURE 1.3: The uses and users of information

3.1 Internal users

Internal users use information to assist them in performing their daily tasks. This information can be from an *internal or an external source*. The following examples will explain the use of these two types of information source.

3.1.1 Examples of internal users and the information needed by them are the following:

Management: To coordinate the activities of the organisation, to do future planning, to make important decisions based on the information, to measure performance and control activities. Managers need *internal* information about their budgets and products in order to carry out their financial planning and make informed decisions. They also need *external* forecasting information on the economy, as well as on interest and exchange rates.

Financial managers: Financial managers need information on the financial performance of the organisation in order to make decisions on cash flow and financing. Hence, management financial statements are an internal source of information. Financial managers also need external information on possible sources of finance in order to make financing decisions.

Production managers: Internal information on sales quantities and sales forecasting is needed to control and plan the production process. Production managers use *external* information on new technology and production processes to improve the performance of the department.

Staff managers: Staff managers use *internal* information on qualifications needed and salary levels. *External* information on employees and their qualifications should also be available to place employees in appropriate jobs.

Marketing managers: *Internal* information needed relates to products, target markets and prices in order to make decisions on possible promotions and advertising methods. *External* information on the different media to use for advertising and their tariffs is needed, as well as on general market conditions, the economy and competitors.

Sales managers: *Internal* information is needed on production costs and all overhead costs in order to make decisions on sales prices. *External* information on clients and their spending patterns is used to approach the clients and determine opening times for retail outlets.

Purchase manager: *Internal* information is necessary on the quantity of the various products or raw material needed by the production department. The purchase manager also needs *external* information on suppliers and prices in order to make informed decisions on the best quality and prices.

Employees: Employees need to have *internal* information on the sustainability of the organisation for job security reasons and *external* information on labour laws and unions.

3.2 External users

Users outside the organisation may also need information from internal and external sources for various reasons. Financial statements form one of the most important sources of information in this regard.

3.2.1 Examples of external users and the information they need, from internal or external sources, are the following:

Shareholders: Shareholders need to make informed decisions on whether to hold or extend their investment or to look at other investments. In order to make these decisions they need *internal* information on the financial and overall performance of the organisation and *external* information from other organisations.

Suppliers: Suppliers need *internal* information on the sustainability and creditworthiness of the organisation for future planning and on products and services in order to supply

the organisation with excellent service. *External* information on creditworthiness is available from references and credit bureaus.

Customers: Customers need *internal* information about products and services in order to make decisions on what and where to buy. They also need information on things like discount, interest rates and payment terms, and whether finance is available or not. Customers can use *external* information on the products and services of different suppliers for comparison purposes.

Financial institutions: In order to supply finance, financial institutions need *internal* financial information to determine the creditworthiness of the organisation. This creditworthiness can also be evaluated from *external* sources, such as references and credit bureaus.

Government: The most important need for information by the government is for use by the South African Revenue Services (SARS). SARS needs *internal* financial information to determine the tax liability of the organisation. On the other hand, it also needs information from *external* sources like banks and other organisations to obtain information on the organisation's earnings. Payroll, taxes and employees' retirement fund deductions are also reported to SARS.

Possible future employees: Future employees need access to *internal* information on the sustainability of the organisation for job-security reasons and *external* information on labour laws and unions. Information from external sources, such as the published financial statements, can also help a job applicant to determine the sustainability of the possible future employer.

Activity 1.1

Visit one of the following:

- an administration department of a business
- the management of a business
- the owner of a business
- any employed person you know

Try to obtain answers to the following questions:

- What personal information from your employees do you use in your business and why do you need this information?
- What information on your sales do you use and for what purpose?
- What information do you try to obtain on your competitors and why do you need it?

---

4 SUMMARY

Information is a key resource within the organisation and forms the basis of decisions made by internal users such as management and external users such as customers and suppliers. It is essential to keep the characteristics of information in mind when collecting information and to ensure that the information obtained is useful.

''Information is a necessary resource, produced by information systems and is a key building block to the management and decision-making in any organisation'' (Van Wyk

2006:1). In the next study unit (study unit 2), you will deal which the role played by information systems and computerised information systems in organisations.

Self-assessment

a. Briefly define the term ‘‘information’’ from a business perspective.

b. Define the term ‘‘data’’.

c. List and describe ten inherent characteristics that determine the value and relevancy of information for specific users in a specific situation.

d. Name and describe five internal users and five external users of information in an organisation.

e. Draw a diagram to illustrate the process of creating information.

f. Application question:

SPCE

SPCE is a manufacturing organisation that manufactures specialist portable communication equipment. In recent years, the development of new technology such as wireless mobile telephones, infrared thermal imaging and global positioning has allowed competitors to create new products. The market for such equipment has – at the same time – grown significantly in the private and public sectors. Accordingly, SPCE recognised that its market share is decreasing and that it does not know as much about its competitors and the needs of its clients as it should.

Required:

As the management accountant of SPCE, you are required to advise the board on what internal and external information it needs in order to solve the problem that SPCE is facing.

Assessment feedback

Your answer to the application question above could have included the following:

The following internal information is needed:

- Information on sales quantities and sales forecasting of SPCE is needed to control and plan the production process and to determine whether the production department can keep up with possible changes in the market in order to retain market share.
- Information on staff qualifications and salary levels will help to evaluate employees’ skills and to compare them with those of the competitors. Do they have the skills to make the new and better products?
- Information on products, target markets and prices to make decisions on possible promotions and advertisement methods.
- Information on the quantity of the various products or raw material.
- Information on creditworthiness of the organisation for future planning and the development of possible new products and services in order to supply customers with excellent service.
- Information on the manufacturing equipment.

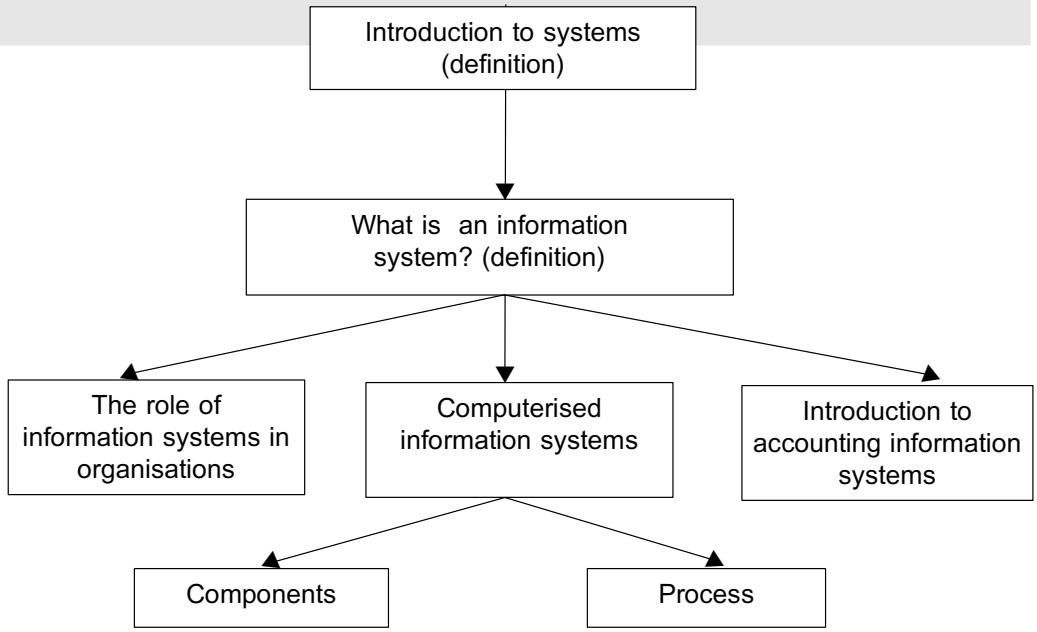
The following external information is needed:

- Information on competitors' products and services to compare them with SPCE's products.
- Information on potential financiers in order to make financing decisions on possible technology upgrades.
- External information on new technology and production processes to improve competition.
- Information on different marketing strategies and the cost involved.
- Information on clients and their spending patterns in order to approach clients and determine possible opening hours for SPCE wholesale/retail outlets.
- Information on suppliers and prices in order to make informed decisions on suppliers in terms of cutting costs and prices.
- Information on regulations applicable to cell phones, infrared equipment and global positioning system (GPSs), amongst others.

STUDY UNIT 2

Information systems

In this study unit



1 INTRODUCTION

In the previous unit, we looked at the information used in almost all organisations. Organisations use information systems to manage their information, to reduce uncertainties and costs and to increase revenues and service delivery.

Organisations make decisions on a daily basis and need planning to implement such decisions. In order to plan, knowledge of resources, time scales for implementation and possible outcomes is needed. This knowledge comes from the information provided by information systems.

Systems form part of our daily lives. The school system, which you have moved through, is possibly the most important system you have experienced. A world with no systems would be a disorganised place. In this study unit, you will learn more about information systems, and the role played by information systems and computerised information systems.

2 WHAT IS A SYSTEM?

A *system* is ***a set of two*** or more ***components*** that serve a ***common purpose and interact*** to ***achieve a common goal***. A system consists of subsystems or elements that perform specific functions supporting the larger system (Romney & Steinbart 2009:26).

The components of a system and the relationship among them can be explained as follows:

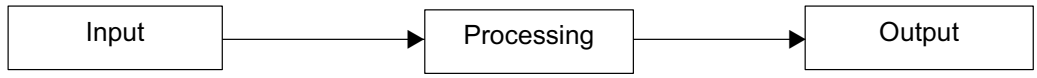


FIGURE 2.1: The components of a system

3 OPEN OR CLOSED SYSTEMS

Systems operate within their environment. Some systems have no effect on their environment and do not affect the environment within which they operate.

A system that is ***isolated*** from its ***environment*** is called a *closed system*. An example would be an automatic washing machine, where the dirty clothes, washing powder and knowledge are the input and the processing stage of the washing cycle would be the selection of a suitable programme and the operating of the machine. The clean clothes are the output.

An *open system* ***interacts*** with its environment. The environment affects it and it, in turn, ***affects its environment***.

Most business systems are open systems. For example, a purchasing system, where the purchase order requests comprise the input. The processing stage consists of identifying the items and the quantities that should be ordered and the output comprises placing the order with preferred suppliers. Feedback includes the communication of order dates, quantities and delivery dates to the department that placed the order.

This system is an open system and the external environment affects the system, for instance suppliers' prices, the transportation of items and the availability of items to an organisation.

4 SYSTEM PERFORMANCE MEASUREMENT

A system need to be properly managed and controlled, like any other function in the organisation. To ensure that the information system adds value and supports the organisation the quality must be monitored.

System performance measurement is the ***monitoring*** of the working of the system to ensure it is effective, fulfil its responsibility and ***make the contribution*** it is supposed to make.

System performance can be measured as follows:

- *Effectiveness.* This is a measurement of the outcomes against a predetermined level of output. It measures the extent to which the information system meets its goals.

- *Efficiency.* This measures outputs against inputs to determine the rate of output over input.
- *Performance standards.* This is a set of specific performance expectations for the information system. Observable activities explain how the job should be done. The performance standards document explains the results that are expected for satisfactory performance of the system.

A *system variable* is the ***quantity or item*** that can be ***controlled*** by the decision maker. The price a company charges for its products is a system variable because it can be controlled by the company and they can decide to change the price.

A *system parameter* is a ***value or quantity*** that cannot be ***internally controlled***, meaning it cannot be changed by a decision-maker in the company. An example is the cost of raw material, as the supplier determines this cost.

5 WHAT IS AN INFORMATION SYSTEM?

An *information system* is an ***organised way of collecting, processing, managing and reporting information for informed decision-making*** to achieve goals (Romney & Steinbart 2009:809).

An information system is a set of interrelated elements or components that collect (input), manipulate (process) and disseminate (output) data and information, and provide a feedback mechanism to meet an objective. ***Input*** refers to the act of gathering and capturing raw data. It can be a manual or automated process but, regardless of the method used, the accuracy of the input is critical in order to achieve the desired output. ***Processing*** involves the conversion or transformation of data into useful outputs while the term ***output*** refers to the production of useful information, usually in the form of documents and reports. The term ***feedback*** refers to the output used to make changes to input or processing activities.

6 THE ROLE OF INFORMATION SYSTEMS IN ORGANISATIONS

Information systems are the heartbeat of any organisation. According to BPP-LM-CIMA E1 (2009:54), information systems assist organisations with the following functions:

- **Planning**

For long-term (strategic) planning, management needs historic information on annual profit to determine growth. Information on the needs of consumers is also required to enable management to set realistic objectives. Information on available resources, markets, possible outcomes of scenarios, suppliers and lots more is needed to do short-term (operational) planning. Information systems provide this information and assist with the daily tasks of management.

> You will learn more about strategic and operational planning in Principles of management accounting (MAC2601) and Principles of strategy, risk & financial management techniques (MAC2602).

- **Recording transactions**

Transactions are recorded to use as evidence, thus meeting legal requirements and to assess profitability. An information system is used to capture and process these transactions.

> You will learn more about the practical application of this in Practical accounting data processing (AIN2601).

- **Decision-making**

One of management's daily tasks is to make decisions and choose between alternatives. If relevant information is available, it will reduce uncertainties and support the decision maker in selecting an option. An information system supports the decisions taken by management.

> You will learn more about the information required to make decisions in Principles of management accounting (MAC2601) and Principles of strategy, risk & financial management techniques (MAC2602).

- **Control and performance measurement**

Plans and objectives are put in place to enable management to measure performance. Management must ensure that plans are executed and the objectives are met. Information on the different business units and the business as a whole is required to control and monitor performance and to take corrective action.

> You will learn more about management's role in decision-making in Principles of management accounting (MAC2601).

7 COMPUTERISED INFORMATION SYSTEMS

People can use a computerised information system to gain access to meaningful information. An example of a computerised information system is an ATM machine.

> A *computerised information* system is a set of ***hardware, software, telecommunication, people*** and ***procedures*** that is used to ***collect, store*** and ***process data into information***.

A computerised information system consists of different components.

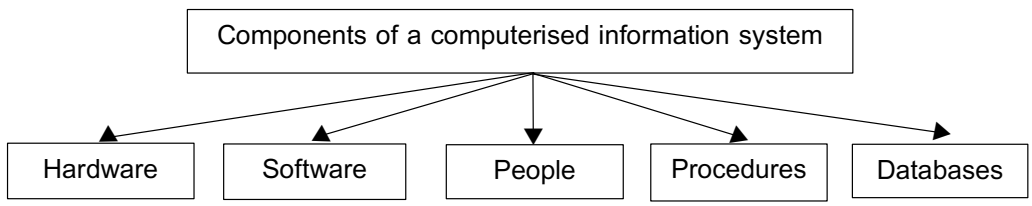


FIGURE 2.2: The components of a computerised information system

- Hardware

  (Discussed in detail in part 2, topic 2, study unit 5)

- Software

  (Discussed in detail in part 2, topic 2, study unit 6)

- Telecommunication, networks and the internet

  (Discussed in detail in part 2, topic 3, study unit 7, 8 and 9)

- People

  People need to interact with the computer to enter data and retrieve information.

  People run, manage and maintain a system and are the most important element in a computerised information system.

- Procedures

  Policies, methods, rules and strategies for using the system are necessary to ensure order and control.

  Poorly developed and inadequate implementation of procedures will waste time or result in wrong decisions.

- Databases

  A database comprises facts and information, organised and stored in two or more related data files.

  A database contains information on sales, purchases, inventories, employees, customers and much more.

A computerised information system process

The following diagram illustrates the computerised information system process and the relationship between the different stages:

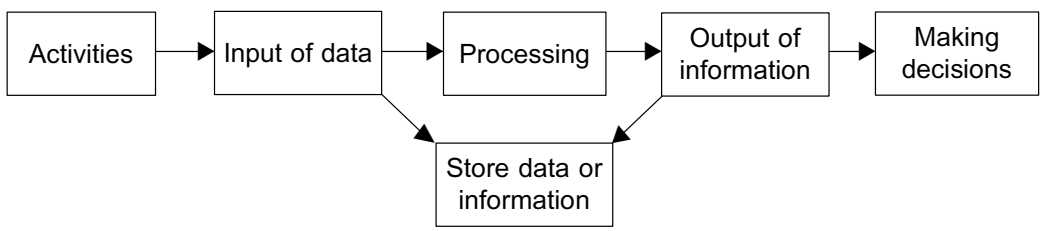


FIGURE 2.3: The computerised information system process

8 ACCOUNTING INFORMATION SYSTEM (AIS)

8.1 Definition

An accounting information system ***collects, records, stores*** and ***processes financial data*** to supply information for decision makers.

8.2 Why study an accounting information system?

A career in accounting or auditing will challenge you to evaluate the reliability and accuracy of the information from an accounting information system (AIS). In order to do

so you will need to understand the development, operation and control of the system and be able to identify the strengths and weaknesses of the system.

Activity 2.1

Why will an organisation have an advantage over its competitors if its information system can produce information about sales figures, product availability and client requirements faster than its competitors can?

Feedback

For long-term (strategic) planning, management needs information on future sales to determine the growth in the market. This enables management to make faster provision for financing possible production expansion, while competitors do not have the information yet.

Current product information enables management to plan possible improved products and new products to satisfy the needs of customers before competitors recognise the gap in the market.

Timely information on customers' needs enables management to plan accordingly. Getting this information before competitors, can enable the organisation to become market leaders.

---

9 SUMMARY

Information produced by information systems, forms the basis for major day-to-day decisions. People and organisations use information systems to help them achieve their goals. To use information systems effectively, it is essential for individuals to understand them in order to perform their daily tasks.

Computerised information systems are essential for today's organisations as they process information more accurately and much faster. That is also the reason why an accounting information system have become an important component of any successful business.

The next study unit (study unit 3) deals with organisational strategy to manage information effectively.

Self-assessment

a. Define a *system.*
b. Draw a diagram to illustrate the relationship between the components of a system.
c. Briefly discuss the performance measurement of an information system.
d. Briefly describe an information system.
e. Name and describe the role of information systems in organisations.
f. Define a *computerised information system.*
g. Name the six stages of the computerised information process. (You can use a diagram to illustrate your answer.)

h. Name the components of a computerised information system.

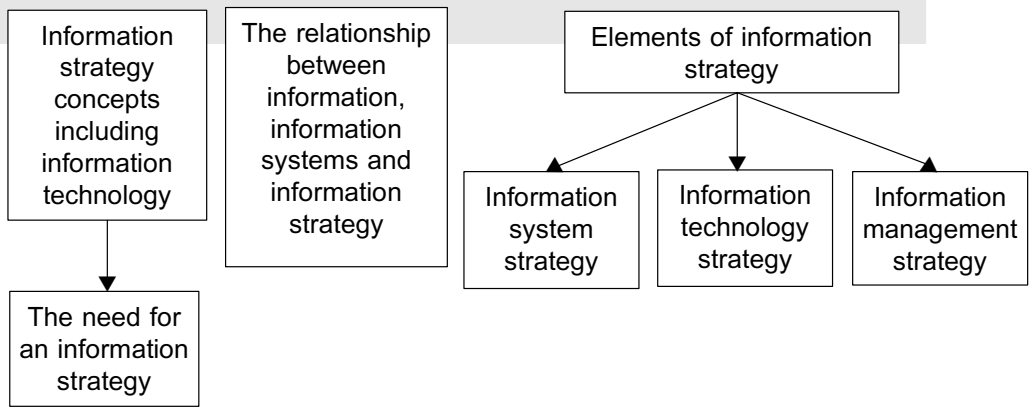
i. Define an *accounting information system.*

j. Briefly explain why the study of accounting information systems is important for future accountants and auditors.

STUDY UNIT 3

Information strategy

In this study unit



1 INTRODUCTION

An information system is a tool (asset) used in an organisation. In the absence of proper management and control, the information system could easily become more of a liability than an asset to the organisation.

In the first two study units of this topic, we dealt with information and information system. In this section, we will provide you with information to help you to obtain a better understanding of the term *information strategy* and its relationship to the previous two terms.

2 WHAT IS AN INFORMATION STRATEGY?

An information strategy refers to our ***decisions or plan on how to use*** the available information, ***how to collect*** more relevant, useful information and ***how to use the information technology*** to manage the process.

In order to gain a better understanding of this definition we need to look at the meaning of the term ''information technology''.

Information technology refers to the ***processing of data***, using ***electronic systems*** (computer systems) and all ***communication links*** and ***software*** that go with it.

Revisit the definitions for the terms ‘‘information’’ and ‘‘information system’’ in the previous study units.

3 THE RELATIONSHIP BETWEEN INFORMATION, INFORMATION SYSTEM AND INFORMATION STRATEGY

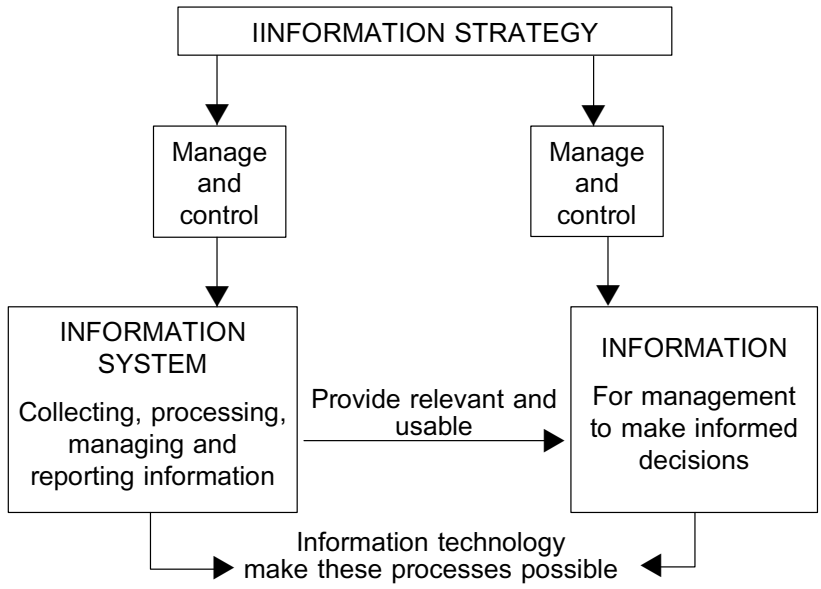


FIGURE 3.1: The relationship between information, information system and information strategy

For a thorough understanding, we need to differentiate between

- information
- the way it is collected, processed and stored
- the plan to manage and control information and an information system

An information system provides management with relevant and usable ***information***. Management can now use this information to make ***informed decisions***. In order for an information system to be effective and ***information to be managed properly***, organisations need a plan on how to manage their information and information systems. This plan is the ***information strategy***. ***Information technology*** enables these processes and makes them fast and efficient.

4 INFORMATION STRATEGY

The information strategy should be in line with the overall strategy of the organisation and support the organisation’s strategic plan. Information strategy refers to the overall plan an organisation has to create and develop its information system (BPP-LM-CIMA (P3), 2009, p. 258).

BPP-LM-CIMA E2 (2009:228) divided information strategy into three elements:

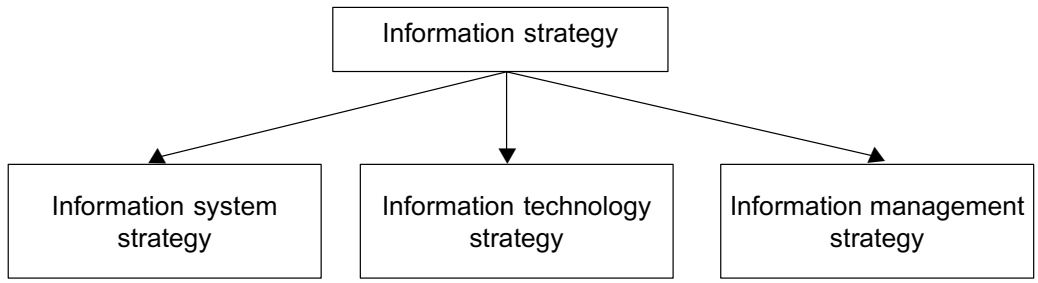


FIGURE 3.2: The three elements of information strategy

- The *information system strategy* is a long-term plan for system in order to provide information to support business strategy.
- The *information technology strategy* entails selecting, operating and managing the technology elements of the information system strategy.
- The *information management strategy* refers to the people involved in the use of information technology and these people's roles. It deals with the relationships between them and with the management process needed to use information technology.

5 BENEFITS OF AN INFORMATION STRATEGY

- An information system contributes to the achievement of goal congruence between the information system's objectives and the organisation's objectives.
- Information strategies ensure that the required information is acquired, retained and shared with all stakeholders.
- Information strategies minimise development and maintenance costs, which are expensive.
- Organisations are more likely to create a sustainable competitive advantage.
- Information strategies ensure better quality information and therefore better decisions by management.

Activity 3.1

Visit the management or the owner of one of your local companies or businesses and try to get a look at their information strategy. Ask them the following questions:

a. Do you have an information strategy (a plan to manage your information and information system)?
b. Do you think such a strategy is necessary; and if so, why?

6 SUMMARY

Owing to rapid developments in the field of information technology, an information strategy should be managed effectively and management should plan carefully ways in which to handle the information system. Such a plan is known as an information strategy. Information technology assists organisations with the management of information, the information system and the information systems' strategy.

An organisation that does not have an information system strategy is like a rowing boat adrift on a big ocean. By drawing up a proper strategy for the organisation's information system, the capital and other resources invested can be used to the organisation, its customers and stakeholders' advantage.

The next study unit (study unit 4) will discuss the management of the information system department in detail before we elaborate more on the components of a computerised information system in part 2.

Self-assessment

a. Explain the terms:
   - information technology
   - information strategy

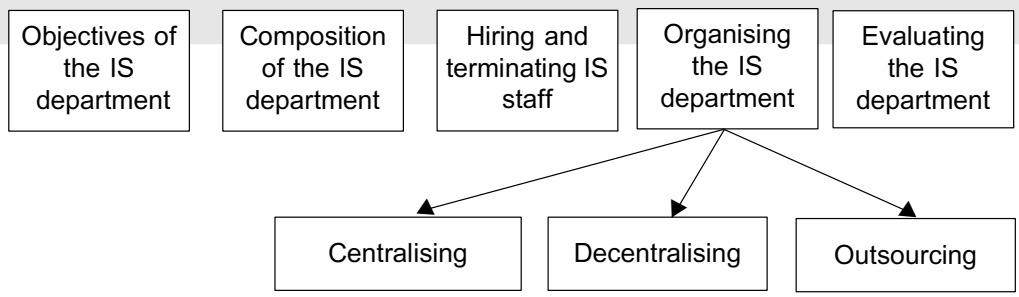
b. Name and explain the three elements of the information strategy.

c. Explain the need for an information strategy.

STUDY UNIT 4

The Information System (IS) department

In this study unit



1 INTRODUCTION

As you will know by now, information is no longer only a nice to have, but rather a necessity in the business environment, enabling users to make sensible decisions. Accessible, accurate, complete, economical, flexible, relevant, reliable, secure, simple, timely and verifiable information plays a vital role in preventing financial losses, increasing shareholder wealth and maintaining a competitive advantage in the marketplace.

In this study unit, we will talk about the establishment of an efficient information system (IS) department as a method to provide users with useful information.

2 INFORMATION SYSTEM DEPARTMENT

The information system (IS) department is a **support function** within the organisation. This department plays a vital role in that it ***aids in providing information*** in an ***accurate, functional format*** by forming the backbone of the information system. The IS department's role can broadly be described as ***ensuring*** that the ***information system is operating efficiently*** on a day-to-day basis and is ***maintained and upgraded*** when appropriate.

2.1 Objectives of the IS department

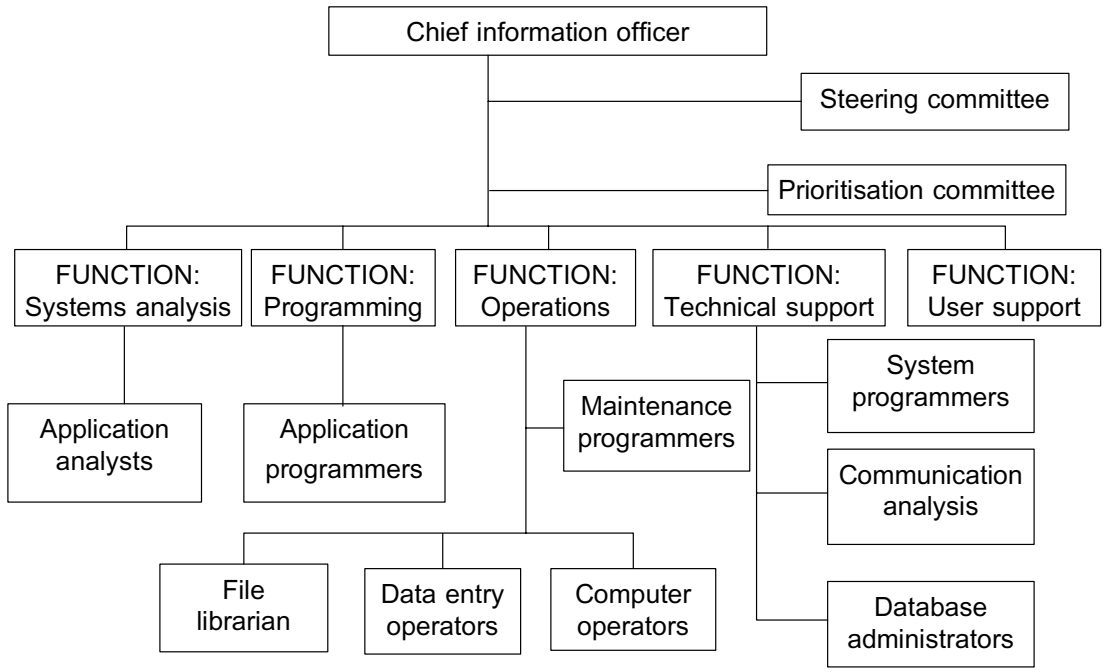
Before we venture into the composition of an IS department, it will be a good starting point to first have a look at the objectives of the IS department.

The objectives of an organisation's IS department include:

- developing an IS strategy that aligns IS goals with the organisation's goals
- monitoring return on investments in IS
- setting standards for the purchase and use of hardware and software
- constantly seeking new ways to meet the needs of internal users
- implementing measures to ensure that planned benefits from system solutions are actually realised
- minimising database redundancy and increasing the reusability of a system by integrating information system architecture
- providing technical assistance to ensure that there is an efficient link between the IS department and the rest of the organisation.

2.2 Composition of the IS department

The structure of the IS department will vary depending on the size and nature of the organisation, but every organisation that processes transactions using a computerised information system will definitely have an IS department in place. A typical IS departmental structure in a large organisation will feature a number of key elements, by assigning tasks and responsibilities based on function. The five major functions include system analysis, programming, operations, technical support and user support. In a medium sized or smaller organisation there might not be a clear distinction between these functions, as IS activities may be consolidated depending on IS staff availability. A larger organisation will typically consist of a number of business functions, for example sales, production, reporting to the board of directors, with departments and departmental managers reporting to business unit managers. Figure 4.1 below illustrates a typical IS department in a large organisation:



Source: Adapted from Bodnar & Hopwood (2004:11)

FIGURE 4.1: A typical IS department in a large organisation

- The IS department is led by the *chief information officer (CIO)* and assisted by the steering committee in an advisory capacity. The CIO either will report at director level, or to a senior financial officer such as a controller, depending on the organisation's IS budget.

- The *steering committee* provides a platform for managers of other business functions in the organisation to provide input on IS policies, procedures and budgets based on the individual needs of the business units, such as manufacturing or administration. This committee operates on a strategic level. The committee consists of senior management, IS department staff and IS users from other business functions in the organisation. They provide user feedback in order to constantly improve the efficiency of the IS department. The committee will assist the IS department in making decisions on the information system used in the organisation and in planned system development projects. The committee also monitors the progress and success of system development projects. One way of monitoring the IS department is to give a member of the internal audit function a seat on the committee.
- The *prioritisation committee* ensures the effectiveness and efficiency of daily IS operations. This committee differs from the steering committee in its composition and the level on which it operates. Where the steering committee consists of higher-level management and focuses on strategy and mission, the prioritisation committee consists of departmental managers and staff in the IS department. The focus here is on the day-to-day running of the information system in order to ensure the smooth operation of business. Decisions made at prioritisation committee meetings will typically include plans of action for allocating limited IS resources. Accountants or financial managers will be given an opportunity to serve on this committee in order to obtain an understanding of the way financial data are converted into useful information to ensure reasonable financial reporting.
- The *system analysis function* is not only responsible for identifying problems by means of questionnaires, interviews and observation, but also for asking the question as to what the information system needs to do to overcome the problems. This function will pinpoint weaknesses in the existing system, which can only be rectified by designing a new computer processing system to satisfy user needs.
- The *programming function* works closely with the analysis function to ensure that the system designed by the system analysts is implemented to produce the programs that are needed. Programmers will focus on purchasing suitable programs, modifying existing programs, or developing new system.
- The *operations function* concentrates on the efficiency of the IS function. Data operators are involved in the day-to-day operation of the IS function by maintaining IS equipment, preparing data to be presented in a usable format to the computer system, running local area networks (LAN) or websites for the organisation and scheduling system maintenance.
- The *technical support function* specialises in a number of areas. This function advises on expensive hardware and software acquisitions, provides database administration support and maintains the web administration function. This function focuses on the support of IS staff.
- The *user support function* operates the helpdesk for service end users in the form of technical assistance, trouble shooting, equipment and software decisions and giving end users the opportunity to make suggestions or comment on the efficiency of the IS function. The function presents user training to optimise the use of the information system. The manager of the user support function works closely with the CIO to decide how the computing needs of end users will be met.

2.3 Hiring and terminating IS staff

Although a lot of time could have been spent on planning the structure of the IS function and documenting IS policies and procedures, the ultimate success of the IS function depends on the quality and motivation of the organisation's IS staff.

Invest time and money on conducting interviews and even background checks to appoint

the most suitable staff and provide effective training programmes to fill possible knowledge gaps and keep staff up to date and equipped for user assistance.

It is also very important to maintain healthy staff relations and to follow the correct procedures when terminating employment. A disgruntled employee can cause a lot of damage to the IS by leaking confidential information or hacking into the system.

Activity 4.1

If you were to conduct an interview with an IS department applicant, what would you take into consideration when deciding whether he/she would be appointed, for example what types of question would you ask, what kind of background checks would you perform? (Hint: Click on the links below for some good ideas.)

- http://www.glassdoor.com/Interview/information-technology-interview-questions-SRCH_KO0,22.htm
- http://www.blueskyinterviews.co.uk/interview-questions-for-IT

2.4 Organising the IS department

There are different ways for organising an IS department. Accordingly, the organisation could centralise, decentralise or outsource the IS department. The organisation will need to consider the most efficient way to organise the IS department.

2.5 Centralisation of an IS department

A *centralised* IT department means that ***IS staff and functions*** are situated in a ***single location*** such as the head office.

Advantages	Disadvantages
Duplication of certain IT functions is reduced.	A single fault in the system at head office level will affect every regional office in the organisation.
Files will be more secure.	Regional offices are less self-sufficient and may hesitate to make decisions as they are relying on head office.
Head office has better control over daily IS operations.	Important operational time may be wasted at regional level, as they might have to wait for IT services and help from head office.
Economies of scale may be available when buying IS equipment.	
There is optimal utilisation of IS capital as IS staff are in a centralised location and more funds are available to obtain IS expertise	

2.6 Decentralisation of the IS department

A *decentralised* IS department means that ***IS staff and functions*** are ***distributed throughout the organisation***, with every regional office or business unit usually having its own IS department.

Advantages	Disadvantages
IS staff will be conscious of IS and business needs on a regional level.	It is harder to control the IS department.
Every office is more independent.	As offices are independent, it might result in a lack of coordination between departments.
Every office has quicker access to IS assistance.	The risk of tasks, functions and data duplication may exist.
IS cost/overhead allocations are more accurate.	

2.7 Outsourcing the IS department

The IS function does not necessarily need to be performed by a department within the organisation itself. IS functions can also be outsourced to an external service provider and monitored by means of a service level agreement. The responsibility for maintaining the service level agreement can be assigned to an individual within the organisation.

Refer to study unit 13 for a discussion of outsourcing.

Activity 4.2

Is your office supported by an in-house (on the premises) IS department or is the IS department located at the head office (central point). Why do you think this is the case? If you are not currently employed, ask someone who is, about his or her organisation.

3 EVALUATING THE IS DEPARTMENT

The IS department needs to be evaluated to determine the cost versus benefit impact regarding the investment in the IS department.

The IT department's efficiency can be evaluated by, for example, answering the following questions:

- Did user computer literacy increase?
- Are the IS staff more aware of business matters?
- Did user groups' level of participation increase?
- To what extent are users making use of the IS support function?
- How successful was the implementation of new system?
- Are IS applications focusing on business?

- Did the response time to user complaints decrease?
- Did system downtime decrease?

The ideal situation would be to answer yes to all the questions above. If that is not the case, action plans should be designed, implemented and monitored to ensure improvement of weak areas.

4 SUMMARY

The structure and organisation of the IS department is determined by the nature and size of the organisation. This study unit described the typical structure of an IS department in a large organisation and how it can be evaluated. We also looked at centralisation, decentralisation and outsourcing as options for the IS department and the pros and cons to consider in making a decision on which to use.

The next part (Part 2) deals with the components of a computerised information system in more detail.

Self-assessment

a. Briefly describe the role of the steering committee.
b. List five questions to be asked when evaluating an IS department.
c. List three ways in which to organise an IS department.
d. Briefly describe the advantages and disadvantages of centralising an IS department.
e. Briefly describe the advantages and disadvantages of decentralising an IS department.
f. Application question:

   ABC Ltd is an audit firm with its head office in Johannesburg. It also has an office in four of the biggest cities of South Africa; that is Durban, Port Elizabeth, Cape Town and Pretoria. On average, every office employs fifty trainee accountants, each one equipped with a laptop. Would you recommend centralising or decentralising the IS department?

Assessment feedback

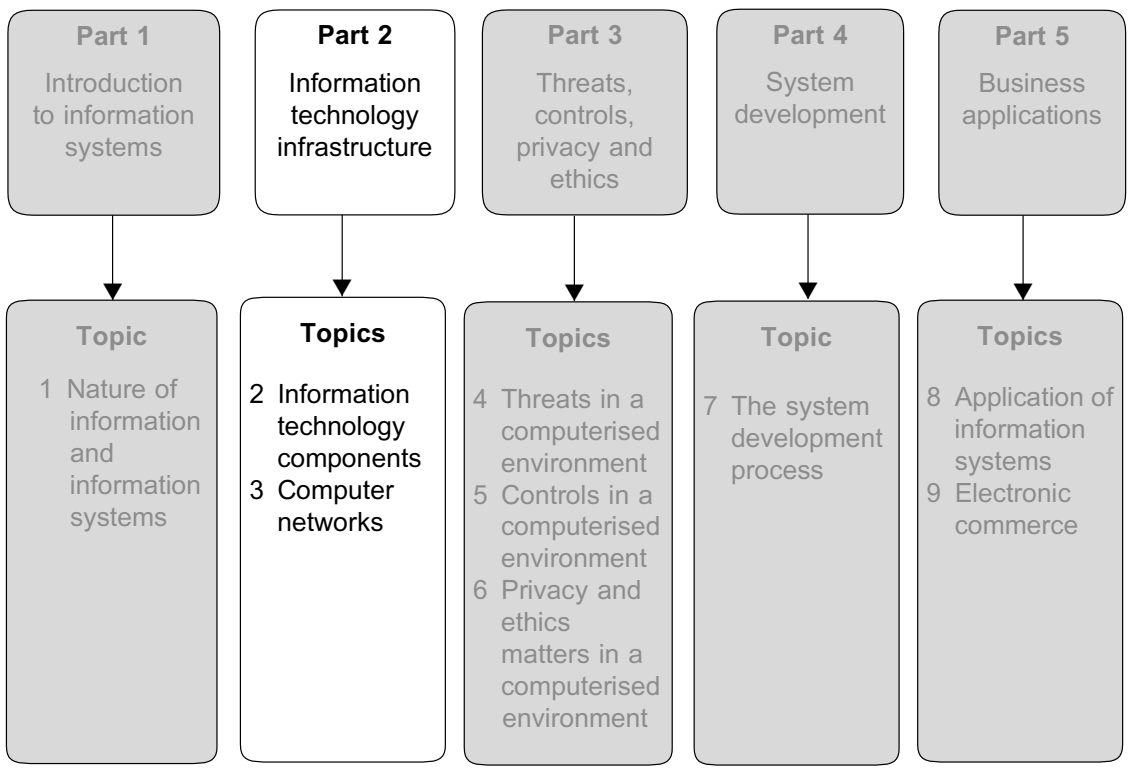
Your answer to application question (c). could include the following:

This question is open for interpretation. You must choose between the two options and motivate your answer. Your motivation can include amongst others, the advantages and disadvantages of centralisation.

Information technology infrastructure

PURPOSE

The purpose of part 2 is to assist you in identifying and describing various components of the information technology infrastructure, including hardware components, software, data communication and networks, and to show the relationships among these components and concepts. You will also be presented with distributed processing concepts.



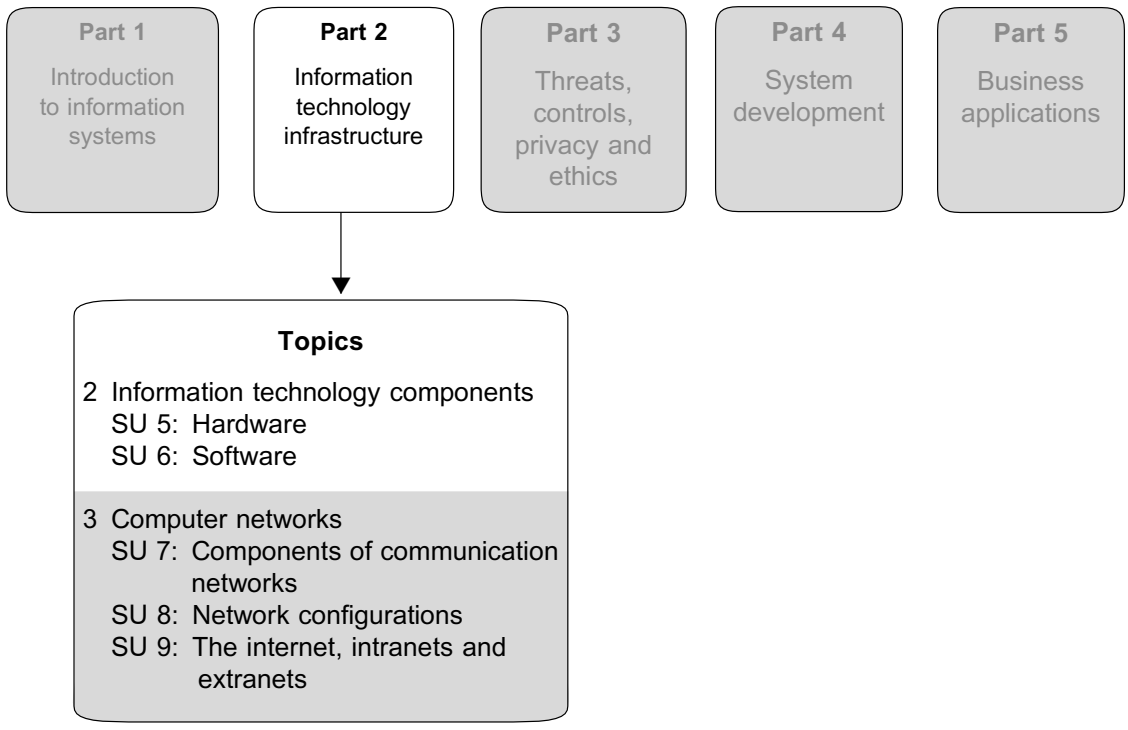
Information technology components

LEARNING OUTCOMES

After studying this topic, you should be able to

- identify and describe the different hardware components of a computer system
- describe the factors to take into account when a computer system is to be selected for an organisation
- evaluate the current and future needs of information systems by organisations when selecting computer hardware
- identify and describe the different types of software, that is, system software and application software; list the sub-types and describe the functions of these software programs
- identify and describe key software trends and issues

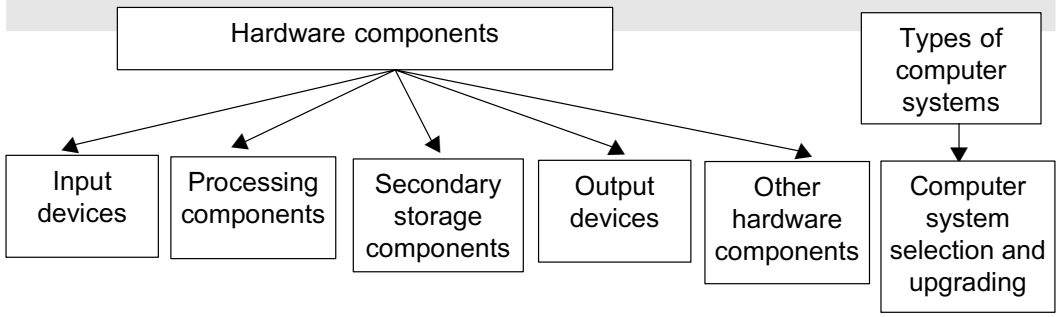
This topic consists of two study units:



STUDY UNIT 5

Hardware

In this study unit



1 INTRODUCTION

Computer hardware refers to the ***physical parts*** of a computer system. Computer hardware can be classified in many ways. One way of classifying computer hardware is to divide it into internal and external hardware devices.

Internal hardware devices, also referred to as ***components***, include the ***motherboard, central processing unit (CPU), Random Access Memory (RAM), hard disk drive***, and the BD/DVD/CD (optical disc) drive.

External hardware devices, also referred to as ***peripheral devices***, include the ***monitor, keyboard, mouse, speakers, printer*** and ***scanner***. Computer networks also consist of computer hardware and software, but this will be dealt with in detail in Topic 3.

In this study unit, we will be looking at various computer hardware components and peripheral devices, such as those that assist with the input (capturing of data), processing, data storage and output activities of an information system.

2 ROLE OF HARDWARE

The function and purpose of computer hardware is to assist users with the input (capturing of data), processing, data storage, and output activities of an information system.

For example, an accountant captures accounting data on the computer system using a keyboard (input device). The data input is processed by the computer system (processing), and transaction information is created and stored on the computer's hard

disk drive (data storage). The transaction output is also displayed on the computer monitor and is printed on paper that is later filed (output devices).

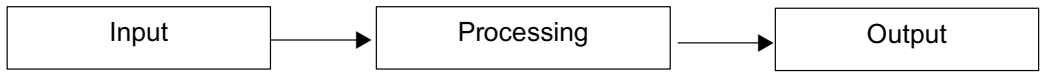


FIGURE 5.1: Activities of a computerised information system

3 HARDWARE COMPONENTS

Computer hardware includes ***input devices*** (keyboard, mouse, scanner), a ***central processing unit*** (also called the CPU) that processes data into information, a ***primary memory*** that provides working storage space for the CPU for program instructions and data to be processed, ***secondary storage*** for storing data and information, and ***output devices*** (monitor, printer, speakers).

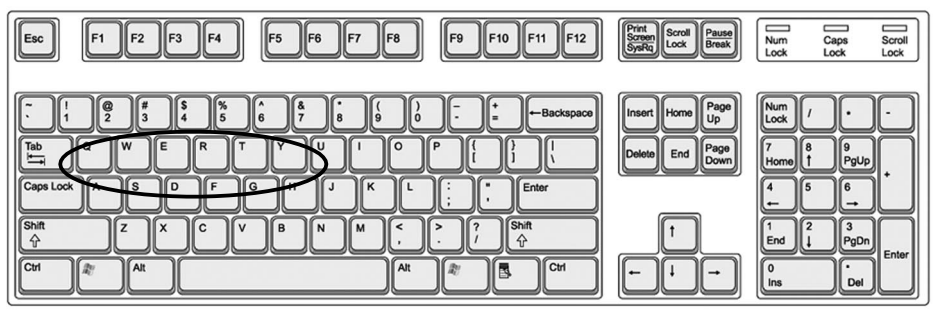
4 INPUT DEVICES

Input devices refer to the ***physical peripheral devices*** used for ***data entry and input*** and are used to ***provide control signals*** for the user interface. Input devices are used for data entry by entering human-readable data (words written by a writer on a piece of paper) into a computer (eg entering characters into a computer using a keyboard) where the data are converted into machine-readable data.

There are different kinds of input devices. Certain input devices are for general purposes (eg keyboard, mouse) and others are created for a specific or specialised purpose (eg head & face 3D colour scanner, digital X-ray system).

4.1 Keyboard

A keyboard, together with a computer mouse, is the most common and popular input device used with a computer system. This device is used to ***input text, numbers and special characters*** by pressing various buttons (also known as keys) on the keyboard. The most common keyboard layout is known as the QWERTY design, that is, the first six letters across the upper-left row of the keyboard.



Computer keyboards also include a row of function keys (usually F1 to F12) along the top of the keyboard, as well as arrow keys and a numeric keypad on the right-hand side. Modifier keys, such as Control, Alt and Shift, can be used in conjunction with other keys as ‘‘shortcuts’’ to perform certain operations. Computer keyboards are connected to a

computer system by either using a USB cable or connecting wirelessly using Bluetooth or Wi-Fi technology.

USB (Universal Serial Bus) is the most common type of ***computer port*** used in modern computers to ***connect*** peripheral and storage devices to computers.

A ***port*** is an interface between one computer and different (other) computers or peripheral devices.

Bluetooth refers to ***low-power, short-range radio technology*** and is used to link devices such as phones, computers and peripheral as well as other network devices wirelessly.

Wi-Fi is a ***wireless networking technology*** that uses radio waves to provide wireless high-speed network connections to connect computers and peripheral and other network devices. Wi-Fi is any wireless local area network (WLAN) product that works with no physical wired connection between the sender and receiver by using radio frequency (RF) technology.

4.2 Computer mouse

A computer mouse is ***a point and click device***, where two-dimensional motion is translated into the movement of a cursor on a computer's display. The current computer mouse uses optical technology to track its movements, have in general at least two buttons, that is, a left and right button for either left click or right click, and a scroll wheel to enable the user to scroll up and down easily through web pages and documents. A computer mouse is connected to a computer system either by using a USB cable or by connecting wirelessly using Bluetooth or Wi-Fi technology.

4.3 Imaging and video input devices

Imaging and video input devices capture images, be they scanned documents or recorded pictures and video, and then convert these captured images or video into digital format.

A ***scanner*** is an ***optical input device*** that ***scans*** images, printed text, handwriting and even objects and then ***converts them into a digital format***. Common forms of scanners are flatbed scanners. As with a copier, the image or document is placed on the glass plate or window of the scanner for scanning. The user then selects the action he/she would like the copier to perform, for example either scanning or copying the image or document placed on the glass plate. Scanned images can be edited using image editing software, and scanned text and handwriting can be recognised and converted into computer readable text and characters using optical character recognition (OCR) software, thus making it easier and faster to capture large amounts of text.

Digital cameras record and store still photographs or video digitally, either on the internal storage of the camera or on the memory card in the camera.

Today, ***webcams*** are some of the most common imaging input devices when it comes to new computers and laptops, enabling users to use voice over IP (VOIP) technology for programs such as Skype to have digital face-to-face conversations with friends, family or business associates.

Current trends include cameras that are able to record video in high definition (HD) as well as three dimensional (3D); portable electronic devices such as cell phones with built-in digital cameras; and webcams as a standard option for new laptops.

Other imaging and video input devices include fingerprint scanners, barcode readers, 3D scanners, laser rangefinders, and specialised medical imaging including digital X-ray system.

4.4 Touch-sensitive screens (monitor)

Touch-sensitive screens can double as both input and output devices. A ***touch screen*** is an ***electronic display monitor*** that is able to detect the place on the screen that was touched. The touch screen enables you to interact directly with what is displayed on the screen, rather than indirectly through a cursor controlled by a mouse or a keyboard. By touching an icon displayed on the screen, a program or application can be launched or closed. Some touch screens work by the user either touching the screen with a finger or hand, where others require the use of a stylus (pen used to touch a touch screen).

Currently touch screens are used in devices such as all-in-one computers, tablet computers, smart phones, personal digital assistants (PDAs), satellite navigation devices, cell phones and hand-held video game consoles. Touch-screen technology has greatly contributed to the increased popularity of the iPad, other tablet PCs and smart phones. Other examples include the self-help information kiosks available at various airports and shopping centres, where information on, for example, flight times, airport layout, shopping centre layout and so on can be obtained by selecting various options on the display by pressing the applicable icons, thus interacting with the touch-sensitive screen.

4.5 Audio input devices

Microphones capture sound that is ***converted*** into ***electrical signals*** that can be recorded digitally. Speech recognition technology converts spoken words into text or translates speech into instructions to be performed by the computer. Speech recognition is used in the following applications:

- Voice dialling on cell phones.
- Speech-to-text processing where spoken words are processed into text in word processors and e-mails.
- Automated answering system at call centres that require callers to provide certain information to assist call operators in resolving problems quickly or supplying information, for example the DSTV call centre.

Activity 5.1

What input devices do you think an accountant would use most while working on his/her computer?

Feedback

Probably a keyboard for inputting data, for example capturing a supplier invoice in Pastel Partner Accounting software, and a computer mouse for navigating Microsoft Windows & Pastel Partner Accounting.

---

5 PROCESSING – THE CENTRAL PROCESSING UNIT (CPU) AND PRIMARY MEMORY

Data and instructions are entered into a computer for processing. This processing is carried out by the CPU, which utilises the primary memory for storing and retrieving data.

5.1 Central processing unit (CPU)

The CPU is the ***component*** of a computer system that carries ***out the instructions*** of computer programs, and is the primary component of a computer. The CPU carries out the instructions of a program in sequence by performing the basic arithmetical, logical, and input/output operations of the system. The CPU is, effectively, the brain of the computer.

A CPU consists of three components:

- The arithmetic/logic unit (ALU), which performs mathematical calculations and logical operations
- The control unit, which fetches program instructions, decodes them and directs the instructions in and out of the ALU, the registers, the primary and secondary storage, and the output devices
- Registers (primary memory) are temporary high-speed storage areas used to hold program instructions before, during and after their execution by the CPU

5.2 Executing instructions

Executing instructions involves two phases:

The **first phase**, consisting of steps 1 and 2, is called the instruction phase.

Step 1: Fetch instruction.
Step 2: Decode instruction.

The **second phase**, consisting of steps 3 and 4, is called the execution phase.

Step 3: Execute instruction.
Step 4: Store results.

The CPU executes all four steps (both the instruction and execution phases) for every instruction processed. After completing one instruction, all four steps are performed again for the second instruction, and so the process continues.

The CPU process involved in executing and completing all four steps (being the instruction phase followed by the execution phase) is called a *machine cycle*.

5.3 Clock speed

Clock speed, also called clock rate, is the ***speed*** at which a ***CPU executes instructions***. The faster the clock speed of a computer, the more instructions a CPU will be able to execute per second. Clock speed is measured in megahertz (MHz) or gigahertz (GHz).

5.4 Primary memory

Primary memory or main memory is also just called ‘‘memory’’.

The CPU ***stores and retrieves information*** directly from and to the memory. This memory is accessed by the CPU, in a random manner, thus *any location of this memory can be accessed by the CPU* either to read information from it, or to store information on it.

Two types of memory technology implement primary memory. The first is called *random access memory (RAM)* and the other *is read only memory (ROM)*. The CPU can write and read information from any primary memory location implemented using RAM. The other part of primary memory is implemented using ROM.

The different types of primary memory are described in detail below:

- *RAM (random access memory):* RAM is the main memory. Data can be ***written into*** RAM and be ***read from*** RAM. In contrast, ROM only permits you to read data. Generally, RAM is ***volatile***, which means that it requires a steady flow of electricity to maintain its contents. As soon as the power is turned off, whatever data were in RAM, is lost.
- *ROM (read-only memory):* Most computers contain read-only memory that holds instructions for starting up the computer. One cannot write data to ROM and ROMs are ***non-volatile***. Non-volatile means that this type of memory does not require a steady flow of electricity to maintain its contents. The ROM will retain its contents even if the power is turned off.
- *PROM (programmable read-only memory):* A PROM is a memory chip on which a program can be stored. Once a PROM has been used, the program ***cannot be erased*** or be used to store something else. PROMs are ***non-volatile***.
- EPROM (erasable programmable read-only memory): An EPROM is a type of PROM that ***can be erased*** by exposing it to ***ultraviolet light***. EPROMs are ***non-volatile***.
- *EEPROM (electrically erasable programmable read-only memory):* An EEPROM is a type of PROM that ***can be erased*** by exposing it to an ***electrical charge***. EEPROMs are ***non-volatile***.

6 SECONDARY STORAGE

Secondary storage, also called permanent storage, refers to ***storage devices or media*** that are able to store large amounts of data, instructions and information ***permanently***, unless erased. Secondary storage is not directly accessible by the CPU and is non-volatile owing to the fact that it does not lose data when the device is powered down.

Secondary storage is classified as either removable (portable) or non-removable (semi-portable and inseparable).

Secondary storage media and devices include the following:

6.1 Magnetic hard disk drives

In modern computers, hard disk drives are generally used as secondary storage. These can be classified as either ***removable or non-removable*** media as external hard disk drives have recently become very popular because of their storage capacity and their ease of use. These hard disk drives connect to a computer by means of its integrated USB interface.

HARD DISK DRIVE

A hard disk drive (HDD) is a ***non-volatile, random-access*** device for ***digital data***, made up of a ***spindle of magnetic rotating disks*** called platters, which record and store data magnetically.

The disks are housed inside a protective enclosure called the hard drive. Data are read magnetically from and written to the platters by the read/write heads mounted on an electrically controlled arm that moves from the centre of the drive to the outer edge and back again. The head float on a film of air above the platters to reduce wear and tear, thus it does not actually touch the platters. An electronic circuit controls everything and acts as a link between the hard drive and the computer. Currently, storage capacity can be as much as 3 terabytes per individual hard drive. Recent innovations include the solid-state drive (SSD). This data-storage device uses solid-state memory to store permanent data. SSDs use non-volatile flash memory chips, which retain data and contain no moving parts.

6.2 Optical disks

Optical disk media include compact disks (CDs), digital versatile disks, or digital video disks (DVDs) and Blu-Ray disks (BD). They are classified as ***removable media***.

OPTICAL DISC DRIVE

An ***optical disc drive***, referred to as a CD-ROM or DVD-ROM drive, is a ***disk drive*** that uses ***laser light or electromagnetic waves*** to read or write data to and from optical disks.

Optical disks are composed of millions of small bumps and indentations. Laser lights or electromagnetic waves from the optical drive read these bumps and indentations as zeros and ones, thus binary code. Accordingly, the computer processes the code, which is translated into information output, that is, images, text and sound.

The amount of information that can be stored on optical disks ranges from 700 megabytes for CDs, 4.7 gigabytes for single-sided, single-layer DVDs and 25 gigabytes for single-layer Blu-ray disks.

Optical disks are very common and are popular for distributing music, video (including movies), software programs (including system and application software, computer and gaming console games) and the storage or backup of data on personal computers as well as in businesses. Optical disk drives are also incorporated in many modern appliances, computers and even motor vehicles.

6.3 Flash memory

Flash memory is a storage device, that is, a ***memory chip***. Flash memory is ***non-volatile***, meaning that no power is needed to maintain the information stored.

Flash memory is effectively EEPROM, which can be electrically erased and reprogrammed. It is classified as removable media and is primarily used in memory cards, USB flash drives, MP3 players and solid-state drives (SSDs) for general storage and transfer of data between computers. Other applications include cell phones, digital cameras, digital audio players, smart phones and laptop computers.

Flash memory does not have any moving parts, has fast read access times, good kinetic shock resistance when compared to conventional hard disk drives, and is extremely durable, being able to withstand intense pressure, extreme temperatures, and can even be submerged in water when packaged as a ‘‘memory card’’. Flash memory can range from 2 gigabytes to more than 2 terabytes per individual flash memory card and more than 2 terabytes for SSDs, with unthinkable capacities being predicted for the future.

USB flash drives and memory cards have replaced most previous portable data storage media, for example floppy disks and Zip disks. A USB flash drive connects to a computer via its integrated USB interface.

6.4 Other secondary storage devices and media

Various other secondary data storage media and devices are still in use, but because of technological changes, some of these are rarely used today and have been replaced by faster, larger capacity and more reliable storage media and devices.

Some of the older types of media include floppy disks, magnetic tape, Jaz disks and Zip disks. Each of these must be inserted into an appropriate drive in order to be read by a computer.

Owing to the fact that secondary storage devices are not always accessible by a computer, they are commonly used for ***backup and archive purposes***. A secondary storage device may be used to restore a recent backup to a new system if a computer stops functioning.

6.5 Tertiary storage

Tertiary storage typically involves ***robotic mechanisms*** that insert and remove removable mass storage media in a storage device. Examples include ***tape libraries*** and ***optical jukeboxes***.

When a computer system needs information that is stored in tertiary storage, it will first obtain the location of the tape or disk containing the information by querying a database catalogue. A robotic arm will then be instructed to fetch the tape or disk from the library and place it in the drive, where data are often copied to secondary storage before use. The robotic arm will then return the tape or disk to its original location in the library when the computer has finished reading the information, where it can be accessed without human interaction. Tertiary storage is primarily used for the ***archiving of rarely accessed information*** and ***extremely large data stores***. The access time of tertiary storage is very slow when compared to other types of permanent storage device.

Activity 5.2

What secondary storage devices do you use on a regular basis?

Feedback

AIN1501 lecturers use flash memory, more specifically USB flash drives, on a regular basis. This happens when large tutorial letters created by lecturers cannot be e-mailed and the files are then distributed using USB flash drives.

---

7 OUTPUT DEVICES

Output devices are the ***physical peripheral devices*** used to ***communicate*** the ***results of data processed*** by a computer ***to the users***.

These devices are used to provide ***human-readable data*** (words displayed on a monitor or printed on paper) ***processed from*** machine-readable ***data*** (information in digital format). Output can be visual, audio, or digital.

7.1 Monitor/display/screen

The terms *computer monitor, display* and *screen* are used synonymously.

The computer monitor is an ***electronic visual display*** that shows the computer's ***user interface and output***.

This allows the user to interact with the computer by, for example, using the keyboard or mouse to input data, thus making it probably the most used output device. As discussed under input devices, touch-sensitive screens can double as both input and output devices.

LCDs (thin-film transistor liquid crystal displays) are used as laptop computer screens and flat panel monitors. Smaller LCDs are used in cell phones, smart phones, handheld TVs, PDAs, and portable video game devices.

The **quality or resolution** of a monitor's output is measured by the number of **horizontal and vertical pixels** used to create an image.

New technology and innovations that are becoming more popular are high definition television (HDTV), LED TV monitors and 3D monitors.

7.2 Printer

A printer is an output device that is able to produce ***printed paper documents***. Printed paper output is also called hard copy.

This is the ***physical version*** of an electronic document, which comprises the output of information on paper. This is a very useful and popular form of output, especially in businesses. There are ***two main types*** of printers namely inkjet and laser printers.

- ***Inkjet printers*** print images by propelling tiny jets or droplets of ink onto paper.
- ***Laser printers*** print by scanning a laser beam back and forth across a drum inside the printer. This builds up a pattern of static electricity on the drum, which attracts a powdered ink called toner. The toner is transferred from the drum onto the sheet of paper, where finally a pair of heated rollers bonds the toner into the paper.

Inkjet printers are the most commonly used type of printer; however, laser printers are the typical choice for businesses being generally faster than inkjet printers are and able to handle greater volumes.

The **speed of a printer** is measured by the number of **pages per minute (ppm)** it is able to print, whereas the **quality or resolution** of a printer's output is measured by the number of **printed dots per inch (dpi)**. Printers with a higher dpi will produce clearer prints. While some printers can only print in black and white, most printers today can produce colour prints.

Current trends for modern printers are to include printing, scanning, faxing and photocopying features. Printers that include these additional features are sometimes called ***multifunctional printers (MFP)***. These printers are also able to interface directly with electronic media such as memory cards and digital cameras.

Other types of printers are:

- ***Dot matrix printers*** are still used for basic text printing but are becoming increasingly rare.
- A ***plotter*** is a printing device generally used to draw up technical plans, blueprints and schematics on paper using a pen. However, they have been replaced by wide-format conventional printers, which are now typically referred to as plotters.

Most new printers ***connect*** to a computer system using a ***USB cable***. However, some printers can be connected to one or more computers wirelessly over a Wi-Fi network. Such printers, known as network printers, have built-in network interfaces that are either wireless and/or Ethernet based. This enables all users connected to the network to use the network printer.

7.3 Speakers

Speakers ***convert electrical impulses into sound waves*** to produce ***audio output*** that can be ***heard by the listener*** or user.

Speakers and headphones are some of the most popular output devices used with computer system. Some speakers may be specifically designed to work with computers, while others can be connected to any audio system.

Activity 5.3

Think of any general output devices that you may already be using in your home.

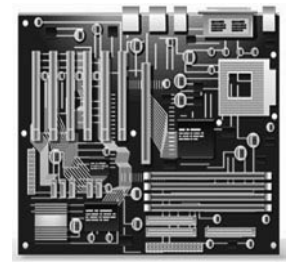
Feedback

What about a radio with speakers or a television screen for watching your favourite television series? Alternatively, your cell phone, equipped with a small LCD screen to read text messages and a speaker for playing your favourite song as a ringtone?

8 OTHER HARDWARE COMPONENTS TO NOTE

As discussed above, a computer system comprises of various hardware components. In addition to the components mentioned above, a computer system also includes the following basic components:

- ***Computer case*** – a case in which all of the computer's ***internal components*** are **stored**.
- ***Motherboard*** – the motherboard is the most important component inside the computer case, as it connects the components of the computer including the CPU and primary memory, secondary storage devices (the disk drives including CD-ROM drive, DVD-ROM drive or hard disk drive), as well as any peripheral devices connected to the computer via connection ports. The motherboard also contains ports or expansion slots where sound cards, graphics cards or network cards can be added to a computer system.



- ***Power supply*** – a power supply delivers direct current (DC) electrical power to the internal components of the computer.
- ***Video card*** – a video card or graphics accelerator card is an expansion card whose function it is to ***generate output images*** to a monitor. Most video cards offer added functions, such as accelerated rendering of 3D graphics or the ability to connect multiple monitors. High performance video cards are used for purposes more graphically demanding, such as 3D rendering and PC games.

- ***Sound card*** – a sound card is an expansion card that facilitates the ***input and output of audio signals*** to and from a computer.
- ***Network card*** – a network interface card (also known as a network adapter) is a computer hardware component that enables a computer to ***connect to a computer network***.

9 TYPES OF COMPUTER SYSTEMS

Computers differ in terms of

- size (eg desktop computers that can fit on an office desk and mainframe computers taking up an entire room) and
- functionality (eg desktop computers used for drawing up annual reports, workstations used for 3D rendering and supercomputers used for weather forecasting or nuclear simulations).

It is therefore important to classify computers correctly, so that you are able to choose the correct computer for a specific application or use.

Some of the different types of computer system are described below.

9.1 Mobile devices

Mobile device is a term used for a variety of small portable computer devices. These include:

- **Laptops**

  Laptops or notebooks are small lightweight portable computers that can be carried around by the user. Laptops can run on battery power and are portable all-in-one computer system, typically having a built-in LCD display, keyboard and pointing device such as a touch pad. Reputable, high quality laptops are, however, more expensive than their equivalent desktop counterparts.

- **Netbooks**

  Netbooks are portable computers that are smaller and cheaper than conventional laptops; however, the internal components are less powerful than those in standard laptops are.

- **Tablet PCs**

  A tablet PC is a portable computer with a touch screen as its primary input device. Most tablets are slightly smaller and weigh less than the average laptop. A popular example is the Apple iPad.

- **Smart phones and PDAs (personal digital assistants)**

  These are small handheld computers. They have limited hardware capabilities when compared to some other mobile devices listed above.

9.2 Desktop computers

Desktop computers are inexpensive computers that are powerful enough to perform most business computing tasks. These computers are not designed for portability, but are small enough to fit on a home or office desk.

9.3 Workstations

A workstation is simply a desktop computer that may contain special hardware enhancements such as a more powerful processor, additional memory and enhanced capabilities for performing specific or specialised tasks. Workstations are used for tasks such as 3D model rendering by engineers.

9.4 Servers

A server is a computer that is dedicated to providing a specific service or performing a specific task. Servers usually have powerful processors, and large memory and storage capacity.

Typical types of server include a

– database server; dedicated to a database
– file server; manages a large collection of computer files
– transaction server; processes business transactions
– web server; processes web pages and web applications

9.5 Mainframe computers

Mainframe computers are large powerful computers used in organisations to service multiple users using smaller, single user machines. These computers are capable of processing and handling large amounts of data quickly. Mainframes are used for tasks such as transaction processing.

9.6 Supercomputers

Supercomputers are the most powerful computer systems of all. These computers have the fastest processing speed and the best performance. Supercomputers are used for performing calculation-intensive tasks such as weather forecasting, fluid and aero dynamics, nuclear simulations, and complex scientific computations.

Activity 5.4

Would you recommend a desktop of mainframe computer for an accountant to do work if he/she is running an accounting practice from home?

_____

10 COMPUTER SYSTEM HARDWARE SELECTION AND UPGRADING

Selecting the correct computer hardware will require an understanding of the information needs of the organisation and the computer software needed to perform the specific tasks the organisation requires. The hardware selected should support the current and future needs of the organisation, thus the hardware components and devices should allow for later upgrading, as it is inevitable that the needs of the organisation will change.

The minimum or recommended hardware requirements should be considered first. The hardware should preferably meet the recommended requirements. Certain hardware considerations are discussed below.

10.1 Processor speed

Selecting the right microprocessor is extremely important. Processing speed, typically measured in megahertz (MHz), or gigahertz (GHz) these days, is probably the first consideration. The higher the number of MHz or GHz, the faster the processor will access programs and process data. If speed is important, consider choosing a microprocessor with a high speed.

10.2 Primary or main memory

Primary memory (RAM) is needed for the temporary storage of programs and data while the data are being processed. Some application software requires a considerable amount of RAM to function properly, and newer software versions usually require more RAM than older versions. Typical personal computers come with 2 GB of RAM, or more. Make certain the PC has sufficient RAM to run the software you will be using.

10.3 Secondary storage

The types and amounts of secondary storage required needs to be considered. Typical computers come with a hard disk drive and a DVD drive already installed. A hard disk drive contains one or more rigid storage platters and provides for the permanent storage of large amounts of data. Although the disk itself cannot be removed from the drive, a CD or DVD can be used to store data and the media disk can be removed from the drive. The storage capacity of a hard disk is an important consideration because it is used to store all system and application software. Typical hard disk capacities are 250 GB and can go up to a few terabytes. Make sure that the PC you are considering has sufficient secondary capacity for your needs.

Flash drives are also easy to use and are portable.

10.4 Output devices

Output devices produce output in either soft copy or hard copy form. Most computer systems come with a monitor (for soft copy output), but you may have to purchase a hard copy device, such as a printer, separately.

10.5 Network devices/internet connectivity

These days, all people conducting business are required to have access to either a network or the internet. Most computer systems have as standard a built-in network interface card or wireless network capabilities. Connectivity to the internet has also been made much easier with the introduction of 3G cards that can be connected to any computer with a USB port.

11 SUMMARY

Computer hardware refers to the physical parts of a computer system. Computer hardware includes input devices, a CPU for processing data into information, primary memory providing working storage space for the CPU, secondary storage for storing data and information, and output devices. Computers also differ from one another in terms of size and functionality. All of the above need to be considered when selecting a computer system, thus keeping the information system needs of the organisation in mind.

The next study unit (study unit 6) deals with computer software, distinguishing between the different kinds of software and the specific purposes and uses of the various types of software.

Self-assessment

a. Briefly describe input devices and list five different types of input device.
b. List the components of the central processing unit (CPU) of a computer and briefly explain the functions of each of these components.
c. In executing instructions, the computer performs four steps, which are divided into two phases. Name the two phases and list the steps performed in each of them.
d. Give the term used to describe the speed at which a CPU executes instructions.
e. Give the two ways in which clock speed is measured.
f. Describe primary memory and list the two types of memory technology.
g. Briefly describe secondary storage devices in a computer system.
h. List the two types of secondary storage media in a computer system, and give relevant examples.
i. Briefly explain a tertiary storage device in a computer system.
j. Briefly describe output devices and list three different types of output device.
k. Briefly describe a printer and list the two main types of printer.
l. Give the term used to describe the quality or resolution of the output of a monitor.
m. Computers differ from one another in terms of size and functionality. List the six types of computer system.
n. List and briefly describe four types of server.
o. List the different factors to consider when selecting a computer system.
p. Application question:

   (This is a practical example to evaluate your knowledge and skills.)

   Your friend is an accountant and he wants to start his own business. He will be using Pastel Partner accounting software to perform accounting work for his prospective clients. He has heard that you are busy studying the AIN1501 module at Unisa and wants your input on which computer system he should purchase to enable him to perform his work effectively and efficiently. He has roughly R10 000 to spend on a

computer system. He has provided you with the system requirements for Pastel Partner Version 11 as well as following three computer system advertisements (see next page for details).

Required:

Evaluate the three advertisements, and choose one of the three computer systems he should purchase for his business to run Pastel Partner on and give reasons for your choice.

Pastel Partner Version 11 system requirements:

Pastel Partner Version 11

Pastel Partner : System Requirements

HARDWARE Single User
Minimum: Pentium III
Recommended : Pentium IV 2GHz or Higher

OPERATING SYSTEM
Minimum: Windows XP
Recommended: Windows XP or higher

Requirements for all Users: DVD/CD-rom drive

RAM
Minimum: 512MB
Recommended: 1028 MB or Higher

SCREEN RESOLUTION
Minimum: 800 x 600
Recommended: 1024 x 768

Advertisements provided:

Advertisement 1

SMART COMPUTING

Computer specials for this week ONLY

The small business beater:
DELL INSPIRON N5010 I5-460M LAPTOP
- Intel® Core i5-460M processor 2.53 GHz
- 4096MB RAM
- 500GB HDD
- 1.3 Webcam & Bluetooth
- DVD writer
- Integrated Ethernet LAN 802.11g/n
- 15.6" LCD screen
- MS Windows 7 Home Premium
- 3 Year local on-site warranty

+ HP LASERJET M1132 colour multi-functional printer

For only: R 8,999 (incl. VAT)

Advertisement 2

CORE CORPORATION

CORE deals:

For CORE business & entertainment:

ACER AZ5763 AIOT – 3D Desktop PC
- Intel® Core i5-2400S processor 3.4 GHz
- 6144MB RAM
- 1TB HDD
- Blu-ray player
- Integrated Ethernet LAN and 802.11b/g/n WLAN, webcam, 1GB dedicated video RAM
- 23" Touchscreen
- MS Windows 7 Home Premium
- 1 Year collect, repair and return warranty

R 13,995 (incl. VAT)

Advertisement 3

Computer Hyper

Making computer sense

Hyper drive price specials:

HeePaa 12 TW999BS Laptop

- Intel® Celeron Dual Core T10 processor 1.2 GHz
- 512MB RAM
- 80GB HDD
- DVD writer
- Integrated Ethernet LAN and WLAN
- MS Windows 7 Basic
- 15.6" LCD screen
- 1 Year warranty

Please note that this laptop cannot be upgraded in any way! It is what it is ☺

For a HYPER price of R 3,499 (incl. VAT)

Assessment feedback

In question p, you should motivate that the computer system advertised in advertisement 1 is the most suitable choice for your friend. The reasons motivating this decision can include that this computer system meets all the recommended system requirements of Pastel Partner V11.

Advertisement 2 was automatically excluded because your friend only had R10 000 to spend, and this system came in well over the available R10 000 at R13 995. Although the computer system in advertisement 3 cost far less than the available R10 000, the computer system did not meet the minimum/recommended system requirements for Pastel Partner V11:

According to the system requirements given on the previous page, Pastel Partner Version 11 requires the following:

	Minimum requirements	***Recommended requirements (for optimal performance)***
Hardware (processor)	Pentium III processor	Pentium IV–2 GHz or higher
RAM	512 MB of RAM	1 028 MB or more of RAM
Operating system	Windows XP	Windows XP or a later version of Windows as an operating system
Screen resolution	Screen resolution of at least 800 x 600 pixels	Screen resolution of 1024 x 768 pixels
For all users	A DVD/CD-ROM drive	

As per advertisement 3:

- The processor is only a 1.2 GHz processor – recommended 2 GHz or higher
- A minimum requirement of 512 MB RAM
- MS Windows 7 Basic which is a later version than Windows XP
- The laptop includes a DVD writer, thus includes a DVD/CD-ROM drive.

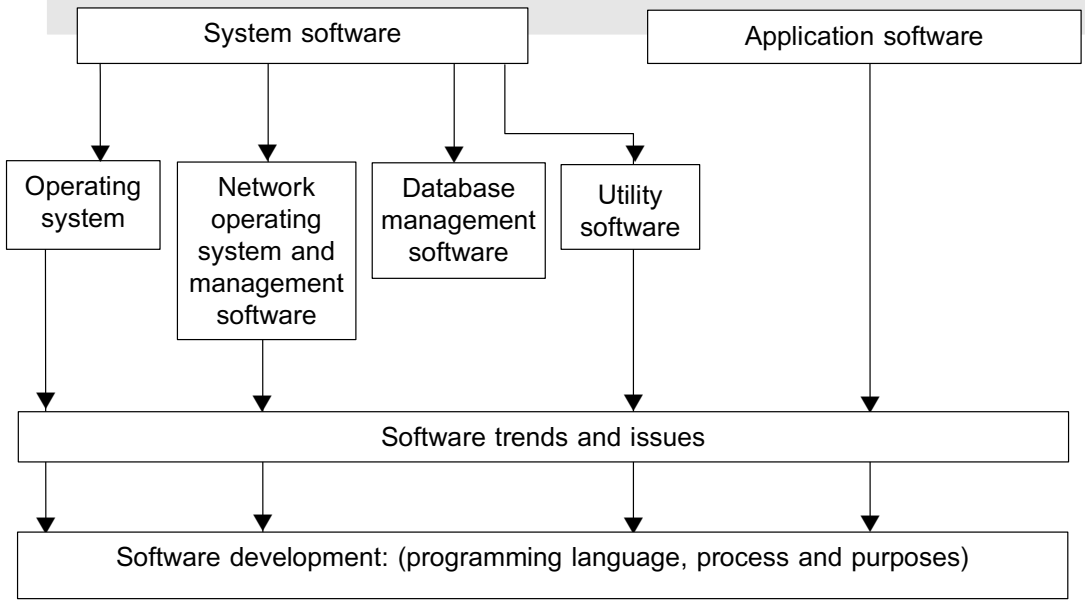
Thus, this system did not meet the minimum recommended system requirements for running Pastel Partner Version 11.

Consider all the factors and give reasons for your choice. Marks will also be awarded for stating that advertisement 1 included a multifunctional printer, which is necessary for your friend's business.

STUDY UNIT 6

Software

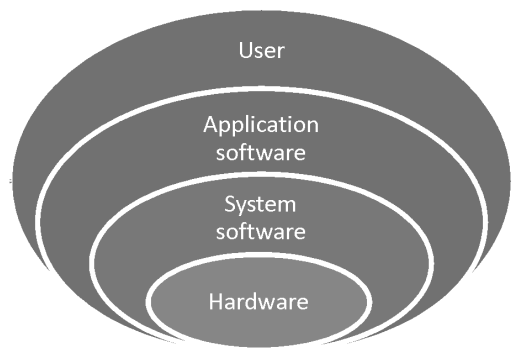
In this study unit



1 INTRODUCTION

In the previous study unit, we looked at computer hardware and various computer system components. In this study unit, we will look at system and application software. We will also briefly discuss software trends and issues, as well as software development.

Computer software consists of ***computer programs*** and ***related data*** that give ***instructions*** to the ***computer hardware***, thus ***controlling*** the ***computer hardware***. Computer software can be divided into two categories: system software and application software. System software provides the basic non-task-specific functions of the computer that manage the activities and functions of the hardware and provide a platform for application programs to run on the computer system. Application software comprises programs that are



The relationship between the levels of software

run on system software and are used by users to accomplish specific tasks. Software is ***intangible***, thus it is not physical and cannot be touched. Software consists of lines of code written by computer programmers using programming languages.

Software can be pre-installed on a computer system, for example, an operating system (eg Windows 7), together with anti-virus programs and a web browser. Commercially available software can also be purchased off the shelf. These programs can then be installed on a computer system. Examples include word processing programs on CD or DVD from a store.

Software can also be downloaded from a vendor's website after an online purchase and be installed on the computer system. Some software is also available free of charge for downloading and installation on a computer system (freeware and shareware).

2 SYSTEM SOFTWARE

System software is designed to ***manage and control the activities and functions*** of the ***hardware*** and provides a ***platform for application programs to run on*** the computer system. System software includes operating system, utility software and database management software.

2.1 Operating system

The operating system consists of ***software,*** which ***enables*** the various ***parts of a computer system*** to *work together* by performing tasks such as transferring data between memory and disks or rendering output to a display device. It also provides a platform on which to run a system and application software, as well as a user interface.

An operating system consists of many components. The ***kernel*** is the central component of an operating system and controls the most critical processes. It is the link between the applications and the actual data processing done by the hardware. The kernel provides the most basic services, such as the hardware-software interaction, device management and memory management. The operating system will run more efficiently if the kernel is more efficient.

An operating system perform the following important *tasks and functions*:

- *Processor task management* – the operating system assigns various tasks to the processor and allocates the required computer resources for processing.
- *Memory management* – the operating system controls the allocation of main memory and other storage areas to a system and application software programs. This is to ensure that the memory of the computer system is used to its optimum level to increase the performance and speed of the computer system.
- *Device management* – the operating system uses special programs called *drivers* that act as translators between the electrical signals of the hardware and the high-level programming languages of the operating system and application software, to communicate and manage hardware devices. For example when a computer system receives input from a keyboard, the electrical impulses are translated by the applicable divers into computer readable input that is used by the operating system and application software as input.
- *File management* – the operating system ensures that files in the secondary storage

are available when needed. It also helps to protect these files from unauthorised access.

- *Application program interface (API)* – an API is a set of commands, functions, and protocols which programmers can use when creating software for a specific operating system.
- *User interface* – the user interface (UI) facilitates interaction between a user and the computer system. New developments in user interfaces have been in the area of the graphical user interface (GUI), providing an easy-to-understand interface for computer users. The input and output peripheral devices (refer to study unit 5 – hardware) are part of the computer's user interface.
- *Network capabilities* – most operating systems include features that help users to connect to computer networks.

2.2 Types of operating system

Various types of operating system exist. An operating system can be categorised in many ways, for example commercial and open source or based on the type of computer it controls.

If it is categorised based on the type of computer it controls and the applications it supports, the ***categories*** are the following:

- *Single-user, single task* – This operating system was developed to manage one user doing one thing at a time.
- *Single-user, multi-tasking* – Currently, most people use this type of operating system on their personal computers. Examples include Microsoft Windows and Apple Mac OS platforms, which will let a single user have numerous programs running at the same time. For example, a Windows user is able to do calculations using a spreadsheet while copying image files from a flash disk to the local hard drive disk while simultaneously sending and receiving e-mail messages.
- *Multi-user* – This type of operating system allows different users to make use of the computer's resources at the same time. The operating system ensures that the needs of the various users are balanced, and that each of the programs they are using has adequate and separate resources so that a problem with one user does not affect the entire community of users. Examples include Microsoft Windows Server 2003, Microsoft Windows Server 2008, UNIX, Linux, Mac OS X, and Novell NetWare.
- *Embedded* – An embedded operating system is developed for use in small machines like smart phones, PDAs and even tablet PCs. It can operate with a limited number of resources, is very compact and very efficient. Examples include Microsoft's Windows Mobile and Google's Android.

Modern operating systems for personal computers include Microsoft Windows, Mac OS X and UNIX, which are sold commercially. Linux is an operating system created and distributed according to the principles of open source, thus being available free of charge. Open source requires the distribution of original source materials that can be studied, altered and built on, with the results once again being freely distributed.

2.3 Factors to consider when choosing a computer operating system

The ***speed*** and ***user interactive environment*** of an operating system determines the ***ease of use*** of the computer and the ***speed and reliability*** of computer programs. If an operating system cannot guarantee the security of the data stored, or is unable to block viral programs, then the operating system is not worth using no matter how user friendly it is. Thus, in order to purchase a reliable operating system, the following factors need to be considered:

- *Ease of use*: It must be easy to use. With Microsoft Windows, most of the tasks are available in dialog boxes and shortcuts. This makes it interesting and time saving even for computer-illiterate staff.
- *The intended use:* Many operating systems are quite flexible and can be used for different purposes, but it still pays to consider their relative strengths and weaknesses.
- *Level of security:* The system should provide an appropriate level of security. This includes both logical access to the specific computer system, as well as network security.
- *Hardware compatibility:* The system has to be capable of supporting the parts of the computer system and the different types of device in use.
- *Software compatibility:* This is an important issue if you plan to use commercial software. The operating system selected should support the applicable software programs used in performing the necessary tasks. Thus, the software needed for performing the tasks has to be compatible with the operating system selected.
- *Technical support:* This refers to the range of services providing assistance to the operating system products. In general, technical support services attempt to help the user solve specific problems experienced with a product. Technical support may be provided telephonically or online by e-mail or on a website.

2.4 Utility software

Utility software was developed to ***help analyse, configure, maintain and optimise*** a computer system. Utility software usually focuses on how the computer hardware, operating system, application software and data storage operate.

Most operating systems usually come with pre-installed utilities. Utility programs can also be purchased and installed separately.

Utility software includes:

Type	Tasks/uses	Examples
Anti-virus and anti-spam software	These software utilities are generally used to prevent, detect and remove malware, including computer viruses, computer worms, Trojan horses, spyware and adware.	**Kaspersky Anti-Virus, Norton Anti-Virus, BitDefender Anti-Virus, McAfee, AVG Anti-Virus and Symantec to name just a few**
Backup utilities	These utilities create an exact copy of all the information stored on a disk, and are capable of restoring either the whole disk (eg in the event of disk failure) or selected files (eg in the event of accidental deletion or corruption of a file).	Norton Ghost, Acronis True Image and Symantec NetBackup to name just a few

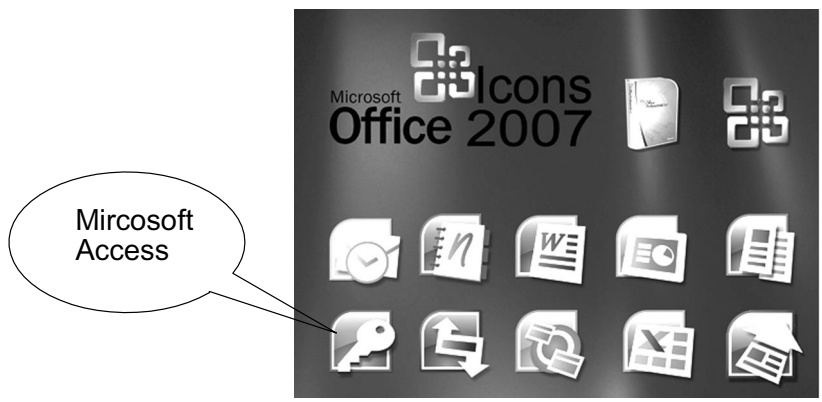
Type	Tasks/uses	Examples
Data compression software	These utilities are used to reduce the size of files. A compressed file takes up less disk space. It can be transferred to another system or over the internet quicker than an uncompressed version. This is achieved by the software using unique algorithms to compress data by encoding information using fewer bits than the original version would use. A typical utility program used for *data file compression* is *WinZip* or *7Zip,* which creates compressed zip or 7z files that can be easily unzipped to the original version. *Media compression* is used to save compressed audio, image and video files. Examples of compressed media file formats include MP3 audio, JPEG images and MPEG video files, which can be played and viewed by media playback programs with built-in encoders that read the compressed file formats. 7-Zip is open-source software. You can use 7-Zip on any computer, including a computer in a commercial organisation. You do not need to register or pay for 7-Zip. For more information visit *http://7-zip.org/*	Win-Zip, 7-Zip and Win-RAR
Disk compression utilities	These utilities can compress/uncompress the contents of a disk, increasing its storage capacity.	Microsoft's Windows disk compression utility
Disk utilities	Disk utilities including disk storage utilities, disk defragmenters, disk checkers, disk cleaners and disk space analysers. These utilities analyse the disk space, sort files, check for disk errors and areas that are corrupt and clean the disk by deleting redundant files, all of which improves the operating efficiency of the hard drive.	Microsoft's Windows error checking and defragmentation tools
File managers	These utilities provide the user with an interface to work with file system. They provide a convenient method of performing routine data and file management tasks. The most common operations performed on files or groups of files are create, open, edit, view, print, play, rename, move, copy, delete, search/find, and modify attributes, properties and permissions.	Microsoft's Windows Explorer
Network utilities	These are small software utilities, designed to monitor hardware and network performance, analyse the computer's network connectivity, configure network settings, check data transfer or log events.	

Activity 6.1

What utility software would you use if you wanted to decrease the size of large files? What reasons can you think of for decreasing the size of large files? *[Hint: refer to data compression software.]*

2.5 Database management system

A *database management system (DBMS)* is a program or ***collection of programs*** that ***enables a user to store, modify, and extract information from a database***. Different types of DBMS exist, from a small system that runs on a personal computer to a giant system that runs on a mainframe. Microsoft Access is an example of such a program.



Examples of mainframe database applications include a computerised library system, a booking reservation system and a computerised inventory system, for example the programs provided by SAP or Oracle.

Requests for information from a database are made in the form of a query, which is a question. The set of rules for making queries is known as a ***query language***. Each different DBMS uses a different query language. One semi-standardised query language is called SQL (structured query language). Complicated languages for managing database systems are called fourth-generation languages or 4GLs.

The information from a database can be presented in various formats. Most DBMSs include a report writer program, including a graphics component, which enables a user to obtain output data or information in the form of a report together with charts and graphs.

> You will learn more about database systems in Practical accounting data processing in AIN2601.

2.6 Network operating system and management software

A *network operating system (NOS)* ***allows a computer system and devices connected*** to the network to ***communicate*** with one another. The NOS performs the same tasks and functions for a network as an operating system (OS) does for a computer, for example processor task management, memory management and device management. Popular NOSs are Microsoft Windows Server 2003, Microsoft Windows Server 2008, UNIX, Linux, Mac OS X, and Novell NetWare.

Network management software includes software tools and utilities for managing networks. These tools and utilities enable the network manager to scan for viruses on the network, monitor the hardware that is shared and manage the validity of software.

3 APPLICATION SOFTWARE

Application software is used to ***accomplish specific tasks*** other than running the computer system and assists users in performing specific tasks. Application software may consist of a single program such as an image editor, or a collection (often called a *software suite*) of related but independent programs and packages that have a common user interface or shared data format, such as Microsoft Office, which consists of a closely integrated word processor, spreadsheet, database, and so on.

Advantages of using a software suite include the fact that all the packages have a similar look and feel making them very easy to use; information can be transferred easily between all the *packages*; and all the packages are installed in one single operation. An example of integration between the packages included in a software suite could be where a table including complex calculations is initially drawn up in a spreadsheet and then the table is transferred to a word processor to form part of a detailed annual financial report.

Application software can be either ***off-the-shelf software*** or ***in-house developments***. You will learn more about this in study unit 16.

3.1 Types of application software

Type	Tasks/uses	Examples
Word processing	This software enables users to create and edit documents.	Microsoft Word, WordPad, Notepad, Word Perfect and Open Office Writer
Spreadsheet	This allows users to create and edit documents and to perform simple or complex calculations using a grid of rows and columns.	Microsoft Excel, Lotus 1-2-3, and Open Office Calc
Database	A database is a collection of data. The purpose of this software is to organise and manage data. Database software allows the users to store and retrieve data from databases.	Oracle, Microsoft Access and Open Office Base
Presentation	Software used to display information in the form of a slide show is known as presentation software. This type of software includes three functions, namely editing which allows insertion and formatting of text, methods to include graphics in the text and a functionality to execute the slide shows.	Microsoft PowerPoint, Open Office Impress and Apple Keynote.

Type	Tasks/uses	Examples
Multimedia	This software allows users to create and play audio and video media. The different forms of multimedia software include audio converters, players, burners, video encoders and decoders.	Media Player, Real Player and iTunes
Web browser	This software allows users to access information on the World Wide Web (WWW).	Windows internet Explorer, Mozilla Firefox, Apple Safari, Google Chrome, and Opera

Activity 6.2

What types of application software have you previously used? Did you do some of your school assignments on a computer? What programs did you use?

_____

3.2 Factors to consider when choosing application software

The application software selected is influenced by the specific task to be undertaken. Thus, certain application software is more suited to perform certain tasks. For example, it is much easier to write a report on a word processer than on a spreadsheet. Likewise, it is almost impossible and highly inefficient to draw up a budget on a word processor instead of using a spreadsheet. This is because calculations and formulas used in a spreadsheet are updated as information change, whereas a word processor does not have this function.

Also, keep in mind that application software is developed to work on a specific operating system and have minimum hardware requirements. This is called *minimum system requirements*, which ensure that the selected software is able to run on the operating system loaded on the computer system, and that the minimum hardware requirements are also met on the system where it is going to be used.

Please refer back to self-assessment activity p. 46 in study unit 5 to see how the minimum system requirements affected the choice of hardware.

4 SOFTWARE TRENDS AND ISSUES

With the increased competition in the computer software industry, software developers need to make sure that they attend to the needs of the users of their software. Software is becoming more and more powerful, including more features and becoming easier to use.

Currently, increased attention is given to software updates and upgrades to ensure that software operates at its best. Licensing to restrict the unlawful copying of software and the development of software – at no cost – are also currently hot topics.

4.1 Software bugs, updates and upgrades

Software quality is very important, especially for commercial application and system software like Microsoft Office, Microsoft Windows and Linux. If software is *faulty*, it can cause the computer system to crash resulting in a user's work being deleted, lost, or corrupted. Errors and faults are called ***bugs***. Most software bugs are discovered and removed (debugged) through software testing. Bugs are also reported by users when they encounter problems while using the software.

A ***software update*** is made available by free download and provides bug fixes and minor software improvements. Software updates may include new drivers to support the latest hardware such as for printers. Sometimes, a software update is called a *software patch* because it is applied over software that users have already installed. A software update does not provide a full software package installation.

A ***software upgrade*** is a purchase of a newer version of the software you are currently using. The upgraded software is usually a more fully featured version (which might include new or improved features in the program for example additional chart types) of the user's current software version. Software upgrades are rarely free, although you can often upgrade at a reduced price.

> You will learn more about these concepts in study unit 17 point 5 under System maintenance types.

4.2 Copyright and licences

The majority of software products are protected by copyright and licensing laws. The software's licence gives the user the right to use the software in the licensed environment. Software may come with the licence when purchased off the shelf, or with an Original Equipment Manufacturer (OEM) license when supplied with hardware. Other software comes with a free software licence, granting the recipient the rights to modify and redistribute the software. (See open-source software below.)

Software piracy is the illegal distribution (copying, downloading, sharing, selling, or installing multiple copies onto personal or work computers) of software and programs for business or personal use. Software piracy is illegal and punishable by law.

Current trends in software require it to be registered or activated using a registration or activation code before full functionality is given to the user. The registration or activation might take place by either automatic activation via the internet or by the user phoning a call centre to activate the product.

- **Shareware, freeware, public domain software and open-source software**

- ***Shareware*** (also known as trial versions or demo versions) refers to proprietary software provided to users on a trial basis. It is often limited by any combination of functionality, availability, or convenience without payment. Limitations may include an evaluation period of, for example 60 days, after which the software will stop working. The motivation for shareware is to give users the opportunity to use the program and judge its usefulness before purchasing a licence for the full version without limitations. Norton Antivirus special free trial offer will enable you to try your downloaded Norton Antivirus for a full 30 days, after which you will not be fully protected by the product.
- ***Freeware*** is computer software that is available for use at no cost. However, an optional donation is usually applicable. The use of freeware usually has one or more restricted usage rights. Limitations may include that the software may not be used on

a computer in a commercial organisation. OpenOffice suite, 7-zip file compression, and AVG anti-virus are some examples of freeware.

- ***Public domain software*** is computer software placed in the public domain. Consequently, there is no intellectual property ownership or copyright of the software.
- ***Open-source software*** is computer software where the program's source code is freely available to the public. Programs can be modified and freely distributed by anyone. These programs are often developed as a community rather than by a single organisation. Linux is an example of an open-source operating system.

It is important to note that software support, bug fixes and software updates may not necessarily be supplied for shareware, freeware, public domain software and open-source software. These are important factors to consider when deciding to use these types of software.

5 SOFTWARE DEVELOPMENT

Software development (also known as software application development or software design) is the development of a software product. Software development is used to refer to the activity of computer programming (also known as coding), which is the process of writing and maintaining the *source code*. Source code is written in a programming language. A ***programming language*** is an artificial language designed to express computations that can be performed or executed by a computer. Thousands of programming languages have been written, but some of the most well known ones are C, C++, C#, Java, JavaScript, Perl, PHP, Python, Ruby, and SQL.

Software development includes all of the processes involved from the conception of the desired software through to the final development of the software program or product.

Software is developed for a variety of *purposes*. This includes

- meeting the specific needs of a client or business (in the case where software is specifically developed for that customer)
- meeting a perceived need of potential users (in the case of commercial and open source software)
- for personal use (eg an accountant who is able to program may write software to automatically retrieve exchange rates from the internet and save this information to a specific file on his computer on a daily basis for easy access and use)

> Software development is discussed again in study unit 15: system development and 16: System implementation.

6 SUMMARY

Computer software comprises computer programs that provide instructions to the computer hardware. There are two main types of computer software: system software (managing the activities and functions of the computer hardware) and application software (used to perform specific tasks). Software is intangible, thus it cannot be touched. Software trends and issues were also mentioned including software bugs, updates and upgrades, copyright and licences, as well as shareware, freeware, public domain software and open-source software.

The next topic (topic 3) deals with computer networks, including the various components

of communication networks, network configurations and the internet, intranets and extranets.

Self-assessment

a. List the two categories into which software can be divided and describe their functions.
b. Illustrate the relationship between the levels of software by using a diagram.
c. Describe the role of an operating system and list and briefly describe the important tasks and functions it performs.
d. List the four different types of operating system, and provide examples of each.
e. List the factors to consider when selecting an operating system.
f. Give an example of a commercial and an open-source operating system.
g. Briefly describe the functions of utility software.
h. List five common utility software program types.
i. Briefly describe the functions of database management system (DBMS) and provide an example of a database application.
j. List three popular types of application software and briefly explain their functions.
k. List two factors to consider when selecting application software.

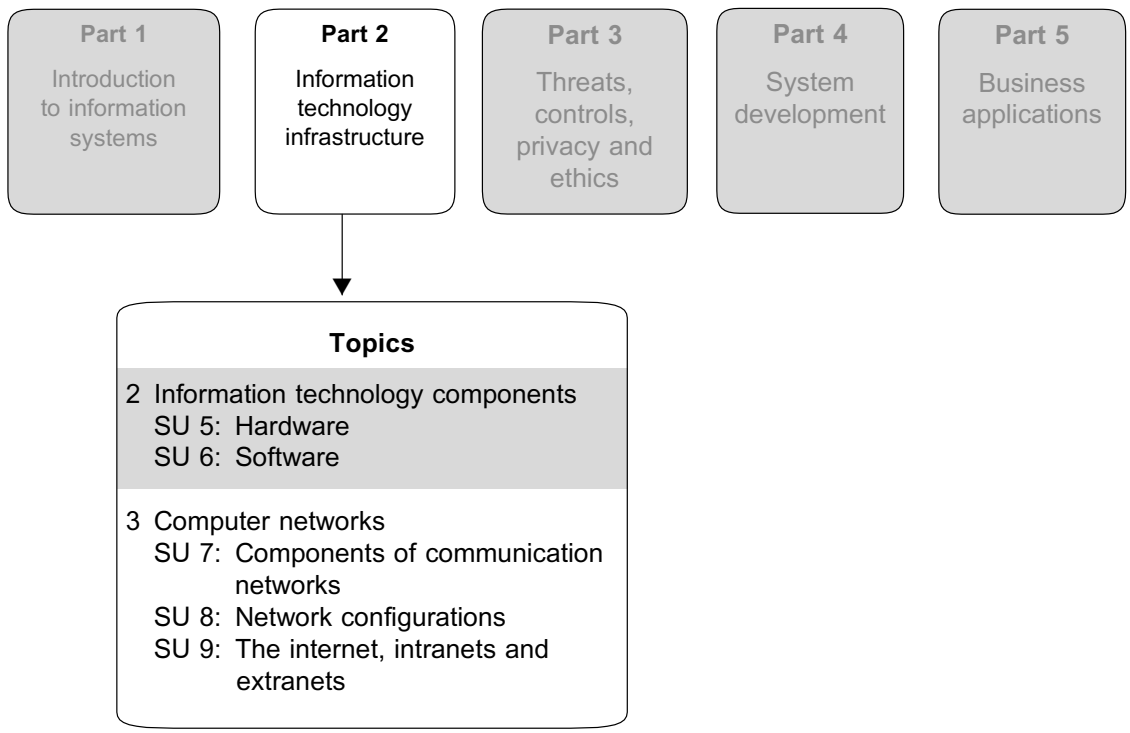
Computer networks

LEARNING OUTCOMES

After studying this topic, you should be able to

- identify and describe the different components of communication networks
- identify and describe data communication networks, including network topologies and geographic scope
- describe the factors to take into account when selecting a suitable network for an organisation
- describe the internet and its applications, and distinguish between intranets and extranets

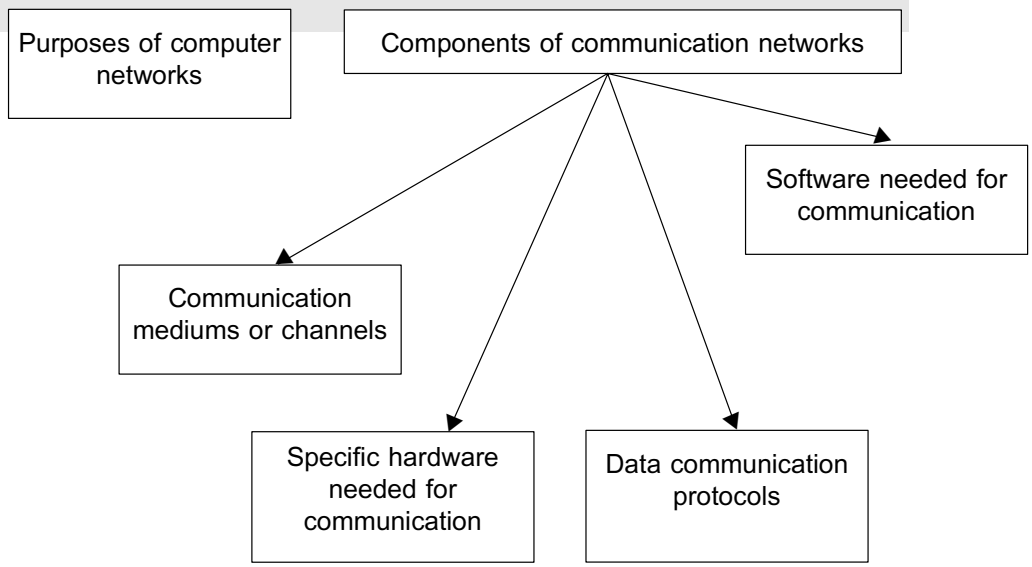
This topic consists of three study units



STUDY UNIT 7

Components of communication networks

In this study unit



1 INTRODUCTION

A *computer network*, also referred to as a network, consists of ***two or more computers or devices linked to one another*** by communication media, which facilitate communication among these connected computers or devices. The purpose of networks is to allow users to share resources, data and information, and to facilitate communication.

The previous topic dealt with the hardware and software making up a computer system.

In this study unit, we will be looking at why computer networks are used, as well as the various components of communication networks that enable communication between the devices connected to the network.

2 PURPOSE OF COMMUNICATION NETWORKS

Computer networks are used for various ***purposes***:

- *Facilitating communication:* Networks enable people to *communicate efficiently and easily* via e-mail, instant messaging, telephone, video telephone calls, and video conferencing.

- *Sharing hardware:* Networks enable computers connected to the network to access and use hardware resources on the network, such as printing a document on a shared network printer.
- *Sharing files, data, and information:* Networks enable authorised users to access data and information stored on other computers in the network. The ability to provide access to data and information on shared storage devices is an important feature of many networks.
- *Sharing software:* Networks enable users to run application programs on remote computers.
- *Information preservation: Backups of information* are shared and stored in multiple locations for easy recovery if information is lost or corrupted in the case of a system failure or as part of disaster recovery.

3 COMPONENTS OF COMMUNICATION NETWORKS

Components of communication networks include both the hardware and the software needed to enable computer systems to communicate with one another.

> In communication networks, a node is a ***connection point***. A ***physical network node*** is an active electronic device that is ***connected to a network,*** which is ***capable of sending, receiving or forwarding information*** over a communication medium.

These components include communication channels or media, communication hardware devices, communication protocols and communication software.

3.1 Communication media or channels

> *Communication media* enable ***signals*** to ***move from one point to another***. These communication media or *channels* are either *cables* or *antennae* that transmit signals from one location to another. Communication media can also be split between ***wired*** and ***wireless transmission***.

• Wired transmission

Wires and cables are ***media*** through which ***information*** can ***move from one network device to another***. The type of cable chosen for a network is related to the network's configuration (topology), protocol and size. Common wired mediums include

– twisted pair wire
– coaxial cable
– fibre optics

• Wireless transmission

With *wireless transmission*, ***signals are broadcast as electromagnetic waves*** through free air space. Wireless signals are ***transmitted*** by a ***transmitter***, and received by a ***receiver***. Wireless systems may be inexpensive because no wires need to be installed to transmit the signal. Wireless transmissions are, however, susceptible to both electromagnetic interference and physical interference. Common wireless media include the following:

– ***Microwave transmission***

Microwave transmissions are high-frequency signals sent through the air using earth-based transmitters and receivers.

– ***Satellite transmission***

Satellites use microwave radio to transmit information and are capable of transmitting voice, data and TV signals.

– ***Radio transmission***

Radio transmissions are signals of electromagnetic waves, which can travel through certain obstructions such as walls. Radio transmissions can be used to transmit voice and data, with both wireless LANs and cellular phones using radio technology.

– ***Infrared transmission***

Signals in the form of light waves are transmitted through the air between devices, requiring line of sight for transmitting within short distances of less than a few hundred metres.

Activity 7.1

Wireless transmissions are part of our daily lives. Examples include **using your cell phone to call a friend** to arrange **to watch a movie on DSTV**.

What part do wireless transmissions play in your daily life?

_____

3.2 Specific hardware needed for communication

Networking hardware includes network interface cards, network cables or communication mediums, switches and hubs, routers, modems, firewalls and other related hardware *needed for communication within a network*.

- A *network interface card* (or network adapter) provides a ***physical connection*** between the computer and the network cable or communication medium.
- The *communication medium or channel*, as described in the previous section, enables signals to move between locations.
- A *switch or hub* is a device that provides a ***central connection point*** for cables from workstations, servers and peripherals. Switches are usually active, which means that they electrically amplify the signal as it moves from one device to another.
- A *router* ***translates information*** and allows communication from one network to another. Routers choose the best path to transmit a signal, based on the destination address and origin.
- A *modem* is a telecommunication device that ***modulates and demodulates data***. The translation of data from a digital signal to an analogue signal is called *modulation* and the translation of data from an analogue signal to a digital signal is called *demodulation*. Modems allow data to be transmitted via various communication mediums owing to their being able to translate analogue electrical, light and radio signals into digital signals.

- *Firewalls* are the most important part of a network with respect to ***security***. Firewalls can be either ***hardware*** or ***software***. A network system implementing a firewall does not need human interaction for data transfer monitoring, as automated processes to reject access requests from unsafe sources and to allow actions from recognised sources, can be set up. With the increase in *cyber* attacks to steal data, plant viruses, and so on, firewalls play a very important role in network security.

Owing to improvements in wireless technology performance and technology becoming more cost effective, current trends are to move from a wired to a wireless networking environment. As discussed above, a *wireless router* is a router that includes the functions of a wireless access point and a network switch. Such devices allow access to the internet or a computer network without the need for a wired connection.

3.3 Data communication protocols

A *protocol* is ***a set of rules that governs the exchange of information and communication*** between computers and devices on a network. In order for two computers to communicate with each other, they must be able to understand each other, that is, they have to *speak the same language.* Various types of network protocols and standards exist because different computers and devices communicate in different ways with one another.

The *Open Systems Interconnection framework (OSI)* was developed in an effort to standardise international communication protocols, enabling communication across the globe. OSI defines seven layers of networking protocols, from the *lowest* layer in the hierarchy (the physical) to the *highest* layer (the application):

Layer 1: Physical	– Transmits the bit stream (electrical impulse, light, or radio signal) through the network at the electrical and mechanical level.
Layer 2: Data link	– Data packets are encoded and decoded into bits.
Layer 3: Network	– Logical paths are created for transmitting data from node to node by switching and routing technologies.
Layer 4: Transport	– Ensures complete data transfer by providing the transparent transfer of data between end system or hosts, and is responsible for end-to-end error recovery and flow control.
Layer 5: Session	– Connections are established, managed and terminated between applications.
Layer 6: Presentation	– Transforms data into a form that the application layer can accept and formats and encrypts data to be sent across a network, providing freedom from compatibility problems.
Layer 7: Application	– Supports application and end-user processes.

3.4 Software needed for communication

A *network operating system (NOS)* allows computer systems and devices connected to a network to communicate with one another. The NOS performs the same tasks and functions for a network as an operating system (OS) does for a computer, such as processor task management, memory management and device management. Popular NOSs are Microsoft Windows Server, UNIX, Linux, Mac OS X, and Novell NetWare.

Network management software includes software tools and utilities for managing networks. These tools and utilities enable the network manager to scan for viruses on the network, monitor the shared hardware and manage the validity of software.

4 SUMMARY

Computer networks allow communication, the sharing of resources (including hardware, files, data and information) and enable software sharing and information preservation. The components of communication networks include communication media, specific hardware, data communication protocols, as well as software.

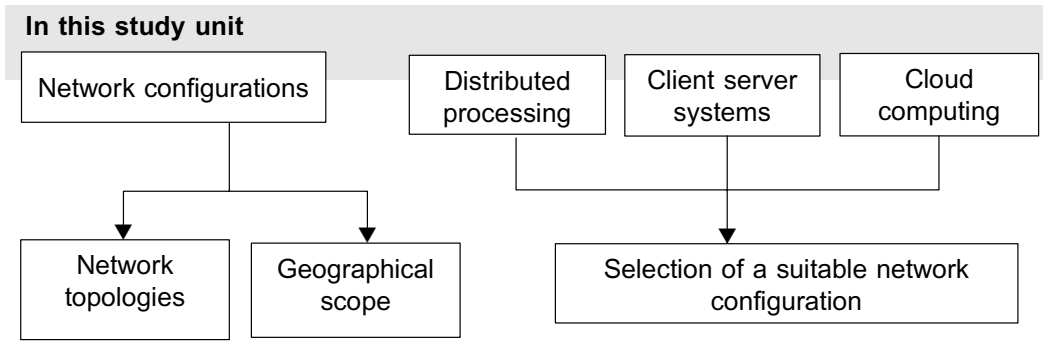
The next study unit deals with network configurations, including network topologies and geographical scope. Distributed processing, client server systems and cloud computing will also be touched on.

Self-assessment

a. Define computer networks.
b. List and briefly describe the purposes/uses of communication networks.
c. List and describe the components of a data communication network.
d. Name the two categories into which communication transmission media can be split.
e. Name three common types of wired media and four common types of wireless media.
f. What are the functions of a switch or hub?
g. Name the seven different layers of the Open System Interconnection framework (OSI).

STUDY UNIT 8

Network configurations



1 INTRODUCTION

Networks can be classified and configured in various ways depending on the *size* of the network, the *distance, or area* of network *coverage,* as well as the *media* to be used.

The previous topic dealt with the uses of networks as well as the components needed to enable computers and devices to communicate with one another.

In this study unit we will be looking at network topologies and geographical scope and touch on distributed processing, client server systems and cloud computing.

2 COMMUNICATION NETWORK CONFIGURATION

Networks may be *classified* according to a wide variety of *characteristics*.

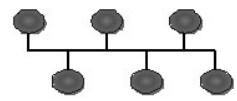
2.1 Network topologies

In computer networking, a *topology* refers to the ***shape or layout*** of ***connected devices.*** A topology is a network's ***physical layout*** or ***virtual shape*** or structure.

The five most common types of network topology are the following:

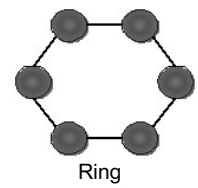
- ***Bus topology:***

  All devices are connected to a central communication cable, called the bus or backbone.



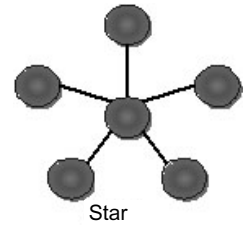
- ***Ring topology:***

  All devices are connected to one another in the shape of a circle or ring, thus each device is connected directly to two other devices, one on either side. Communication signals travel through the ring in the same direction, either clockwise or counter clockwise.



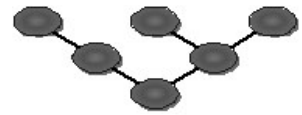
- ***Star topology:***

  All devices are connected to a central switch, hub, or router. Devices communicate across the network by sending data through the switch. This is the most common type of topology,especially for home networks.


Star

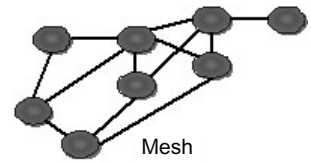
- ***Tree topology:***

  A tree topology is a hybrid, integrating multiple star topologies, connected together onto a linear bus back-bone. A star/bus hybrid approach supports the future growth of a network.


Tree

- ***Mesh topology:***

  Devices are connected with many redundant connections between network devices. A mesh network in which every device connects to all the others is called a full mesh.


Mesh

2.2 Geographical scope

Networks can also be categorised according to their *geographical scope*. Geographical scope refers to the *distance or coverage area* of the network, as well as the *communication media or channels* connecting the whole network together. Examples of different network methods include the following:

- ***Personal area network***

  A personal area network (PAN) is a network that connects different information technology devices around an individual person. PANs generally cover a range of less than ten metres. PANs may include wired and wireless devices. Wired devices usually connect using USB or FireWire connections, while wireless devices can connect via Bluetooth or Wi-Fi technologies.

- ***Local area network***

  A local area network (LAN) is a network that connects different computers and devices within a relatively small area. Examples include small office and home networks confined to one building or closely positioned buildings.

  Wireless LANs (WLAN) are LANs that use wireless technologies instead of wires and cables to connect computers and devices in the network.

- ***Metropolitan area network***

  A metropolitan area network (MAN) is a network that is larger than a LAN but smaller than a WAN, usually spanning a medium sized area such as a large campus or a city.

- ***Wide area network***

  A wide area network (WAN) is a network that covers a large area such as networks linking across metropolitan, regional, or international borders. The internet is the largest example of a WAN, which is made up of numerous smaller networks.

- ***Virtual private network***

  A virtual private network (VPN) is a computer network that uses public networks to connect nodes. Networks are created by using the internet as the medium for

communicating data. VPNs use encryption and other security systems to ensure that only authorised users can access the network and that the data is not intercepted.

2.3 Selecting a suitable network configuration

Selecting the correct network configuration will require an understanding of the networking and information system needs of the organisation.

In selecting a suitable network configuration, the following factors should be considered:

- *Area of coverage/distance between nodes*

  The geographic scope should be considered, as LANs will probably be used to connect office computers and devices to a network. The need to connect offices in different cities or countries also needs to be considered, as this will lead to long-distance communication.

- *Data communication volume and speed*

  The amount of data expected to be communicated within a network needs to be considered, as well as the speed at which the organisation requires the data to be communicated. This will influence the specific topology chosen, as well as the data communication media or channels.

- *Security*

  Access to the internet may lead to security risks, for example hackers may access an organisation's database; hence, applicable security measures should be implemented.

- *Hardware and software compatibility*

  The various hardware (including the communication mediums) and software used in the network should be compatible, enabling all nodes in the network to communicate with ease.

3 DISTRIBUTED PROCESSING

In a computer-networking environment, computers connected to the network may access and use the resources provided by the other computers and devices on the network.

> *Distributed processing* refers to multiple remote computer systems linked together, where processing is distributed to more than one of these computers. Distributed processing allows computers to work together in processing information or in performing tasks, or allows workstations to utilise powerful servers to enable more efficient and faster task processing.

4 CLIENT SERVER SYSTEMS

In a *client/server* network architecture, certain ***powerful computer systems*** are ***dedicated*** to ***providing*** a ***specific service*** or ***performing a specific task***. These computer systems are called ***servers***. Computers, called ***clients*** in this setting, which are connected to the network, have access to the resources provided by the servers. Clients then request the services provided by the servers connected to the network. These servers have operating system software installed that manages the network activities. As discussed in study unit 5 that dealt with computer hardware,

there are various types of server, including database servers, file servers, transaction servers and web servers.

5 CLOUD COMPUTING

Cloud computing refers to the provision of ***applications and services*** offered to a user, by another company (also known as a service provider) ***over the internet***. These computing resources and services are provided on demand by the applicable data centre. This means that users do not need the required hardware or applications to perform the specific tasks owing to the fact that the computing is done by the service provider who sends the required results to the user. Therefore, any user with an internet connection can access the cloud and the services it provides. The service provider carries out all the maintenance and development needed to provide the applications and services.

Examples include online backup services, social networking services and web-based e-mail such as Hotmail and Gmail.

Activity 8.1

Do you make use of cloud computing on a daily basis?

Feedback

If you have a Gmail account for e-mails or make use of Facebook you are using cloud computing.

After reading about cloud computing, you will have realised that by using your Gmail account for sending and receiving e-mails or by using Facebook to stay in touch with friends, you are actually making use of cloud computing.

6 SUMMARY

In this study unit, we looked at data communication networks, specifically how networks are classified. This includes networks classified according to their topologies as well as their geographical scope. Other concepts were also briefly explained, including distributed processing, client/server systems and cloud computing.The next study unit deals with the internet, intranets and extranets.

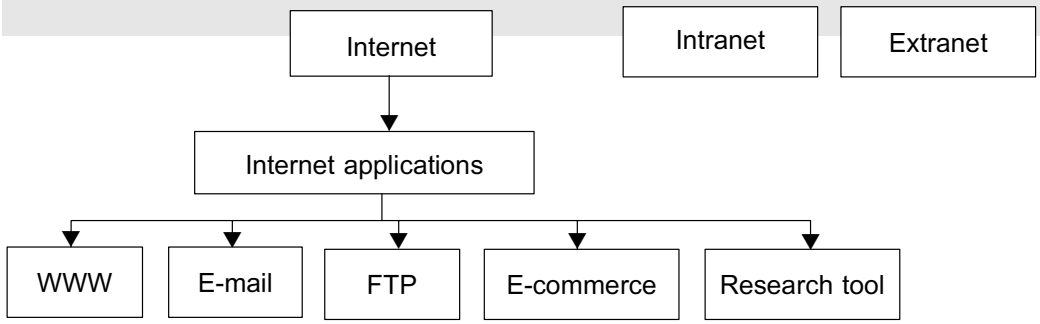
Self-assessment

a. List and describe five uses of computer networks.
b. List the two ways in which communication networks can be classified.
c. List the five most common types of network topology.
d. Networks can be classified according to their geographical scope. Name and describe any three.
e. Describe the factors to consider when selecting a suitable network configuration.
f. Briefly describe distributed processing and client server system.
g. Briefly describe cloud computing and give two examples.

STUDY UNIT 9

The internet, intranet and extranet

In this study unit



1 INTRODUCTION

The internet is a ***global network*** of computer networks, which supports communication and the sharing of data and offers vast amounts of information through a variety of applications (services and tools).

In the previous study unit, we looked at network configurations, as well as distributed processing, client server systems and cloud computing, where we mentioned the internet.

This study unit will deal with the internet, including internet applications (WWW, e-mail and File Transfer Protocol), e-commerce and using the internet as a research tool. We will also briefly discuss intranets and extranets.

2 THE INTERNET AND HOW IT WORKS

The internet is a network, connecting millions of networks, big and small, across the globe. The internet includes academic, corporate, government, public and private computer networks, and is the *world's largest network*.

2.1 How the internet works

An *internet service provider (ISP)* is a company that provides ***access to the internet*** to individual people and organisations. Examples include MWEB, @lantic, Telkom and Vodacom.

The internet uses the standard *Internet Protocol (IP)* technology to link different networks together.

> An *IP* is a ***communication standard or rules*** that define the way computers communicate and exchange data, and enables two networks to be connected and an *IP address* is a ***unique number*** used to ***identify computers*** on the internet.

The *Domain Name System (DNS)* was developed to allow the use of easier to remember domain names, instead of IP addresses, to locate computers on the internet. Domain names consist of words and letters.

Domain names consist of two parts. The first part names the host computer or organisation that registered the domain name (also known as the *second-level domain or SLD*), where the second part identifies the *Top Level Domain (TLD)*. TLDs identify the type or nature of the organisation using the address. The TLD includes

- .com commercial organisations
- .gov governments
- .org non-profit organisations
- .ac or .edu academic or educational institutions
- .net networking organisations
- .int international organisations

Country code TLDs also exist. They appear to the right of the TLD, and include for example:

- .za South Africa
- .au Australia
- .uk the United Kingdom
- .us the United States

> A *Uniform Resource Locator (URL)* is a ***unique address*** assigned to each computer connected to the internet, which ***identifies the computer*** to other ***hosts***.

A URL consists of the following parts: the scheme name, commonly called ‘‘protocol’’, followed by a colon. Depending on the scheme, a domain name or alternatively an IP address follows.

The internet is a *packet switching network* that uses *TCP/IP* (Transmission Control Protocol/Internet Protocol) as its *core protocol*.

> *Packet switching* involves systems that ***transmit data in small packets*** using the ***best path*** to their destination, thus enabling users to transfer large amounts of data over the internet.
>
> *TCP/IP* is a ***suite of protocols*** that governs network addresses and the organisation and packaging of information to be sent over the internet, and allows computers to communicate with one another.

2.2 Internet applications

Although many people think the internet and *the* World Wide Web (WWW) is the same

thing, they are not. The WWW is one of the many applications of the internet. The WWW, e-mail and FTP are some examples of internet applications that will be discussed.

- **The world wide web (WWW)**

The *WWW*, also simply known as the Web, is one of the *services* that run on the internet. It is a *collection of interconnected documents and other resources, linked by hyperlinks and URLs*. The Web is an *application* running on the internet.

The Web is a *menu-based system* using the *client/server model*. A web browser may be used to view *websites.* A home page is a cover page for the website that includes graphics, titles and text. *Hypertext* is usually used to write words and text, thus allowing certain words to be linked to other web pages. Users may click on these links to access the linked web pages' information. *Hypertext Markup Language (HTML)* is the standard page description language for web pages. Newer web standards include *Extendable Markup Language (XML)*, which is a mark-up language for web documents containing structured information, including words, pictures and other elements.

To view a web page on the WWW, one usually begins by typing the URL of the web page into a web browser. Another way of doing so is to follow a hyperlink to the web page. In this regard, the web browser sends a series of communication messages to retrieve and display the web page. *The web browser translates HTML so that the internet user is able to read the web page.*

- **E-mail and instant messaging**

E-mail or electronic mail is a method of exchanging messages digitally over computer networks between users. E-mail is also one of the services that operate across the internet or other computer networks.

E-mail can incorporate formatted text, colours and images in the message. In addition, documents can be attached to e-mail messages, allowing files to be transferred between users via the e-mail protocol.

An even faster, instant method of communicating by using text is instant messaging (IM). Using a computer or mobile device like a cell phone, a person can send text messages and get immediate answers if the other person is online. The advantages of instant messaging are that it is faster if the other person is available online, and you do not have to click through the same amount of steps, as you need to, with e-mail. Well-known instant messaging providers are Windows Live Messenger (previously MSN Messenger), Yahoo Messenger, Google Talk and Blackberry Messenger, preinstalled on the newer Blackberry phone models. (See the http://www.howstuffworks.com/ to read more about how IM works).

- **File Transfer Protocol**

File Transfer Protocol (FTP) is used to copy files from one computer to another over a network, such as the internet. FTP is built on the client/server model and it uses the model as well. It can be used to transfer huge amounts of data, for example by organisations transferring transaction data between regional offices. FTP can also be used to upload and download content from websites on the internet.

2.3 E-commerce

Electronic commerce, also known as *e-commerce*, is the ***online business process of selling, buying, delivering, servicing*** and ***paying for products and services*** over computer networks such as the WWW or the internet.

The objective of e-commerce is to add and expand revenue streams, enhance relationships with customers and business partners and improve efficiency using computer networks. It is important to remember that although the largest part of e-commerce is conducted entirely electronically, some part will entail manual interaction, as a service that has to be rendered or a product that is sold must be physically transported and delivered to a customer.

> In topic 9 of this module, we discuss E-commerce in detail.

2.4 Using the internet as a research tool

The WWW can be compared to a library to which users donate documents; however, in the absence of a classification system, it is difficult to find information. Search engines are web search tools that searches the web for keywords. Google is one of the most popular internet search engines freely available on the web. Examples of information available on the web for research include journals, encyclopaedias, dictionaries, government reports, calendars, indexes, statistical reports, research reports, books, manuals, manuscripts, video material, geographic maps, unpublished material, previously published textbooks and interactive communication.

Activity 9.1

Have you ever used the internet as a research tool?

Feedback

Have you ever purchased a textbook over the internet? Do you visit myUnisa or send e-mails to lecturers with queries about your study material?

3 INTRANETS AND EXTRANETS

In the current business environment, organisations have to be able to communicate more effectively, both ***internally*** with their employees and ***externally*** with their trading partners and customers.

An ***intranet*** is an ***internal or private network*** that is under the control of a single organisation. Intranets use IP standards and tools such as web browsers and file transfer applications, allowing employees to gain access to the organisation's information, making internal communication easier and less expensive. Only computers or users connected to the intranet can access the information available.

An ***extranet*** is a network that ***links an intranet to the internet***. It links selected information and resources on an organisation's intranet with trusted customers, suppliers, or business partners. Extranets also use IP standards.

Secure intranet and extranet access applications usually require the use of firewalls, user authentication, message encryption and the use of VPNs.

4 SUMMARY

In this study unit, we looked at the internet: how it works as well as various internet applications, including the WWW, e-mail and FTP. Other concepts were also briefly explained, including intranets and extranets.

In the next study unit, you will be introduced to the threats experienced by a computerised information system.

Self-assessment

a. Define the internet.
b. Name the standard technology used to link different networks to the internet.
c. Explain why the Domain Name System (DNS) was developed.
d. Explain how individual people and organisations are able to gain access to the internet.
e. Briefly describe the nature of the organisations that use the following top-level domains:

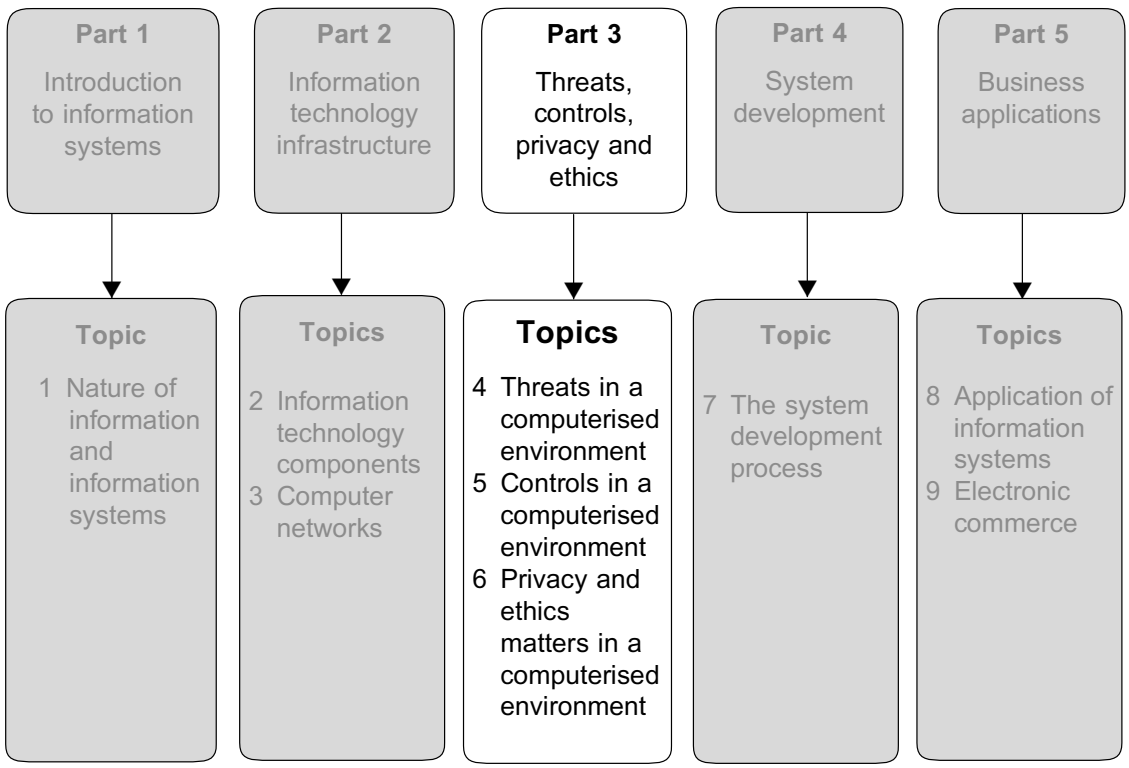
   .com
   .org
   .ac or .edu
   .gov
   .net

f. List and describe three internet applications.
g. Define a search engine and give one example.
h. Describe an intranet and an extranet.

Threats, controls, privacy and ethics

PURPOSE

The purpose of part 3 is firstly to create an understanding of the common threats faced by an information system. Thereafter, the importance of implementing appropriate and effective computer controls, including information technology governance, to address these threats, will be explained. Concerns regarding privacy and ethics in a computerised information system will be raised and possible measures to alleviate these concerns discussed.



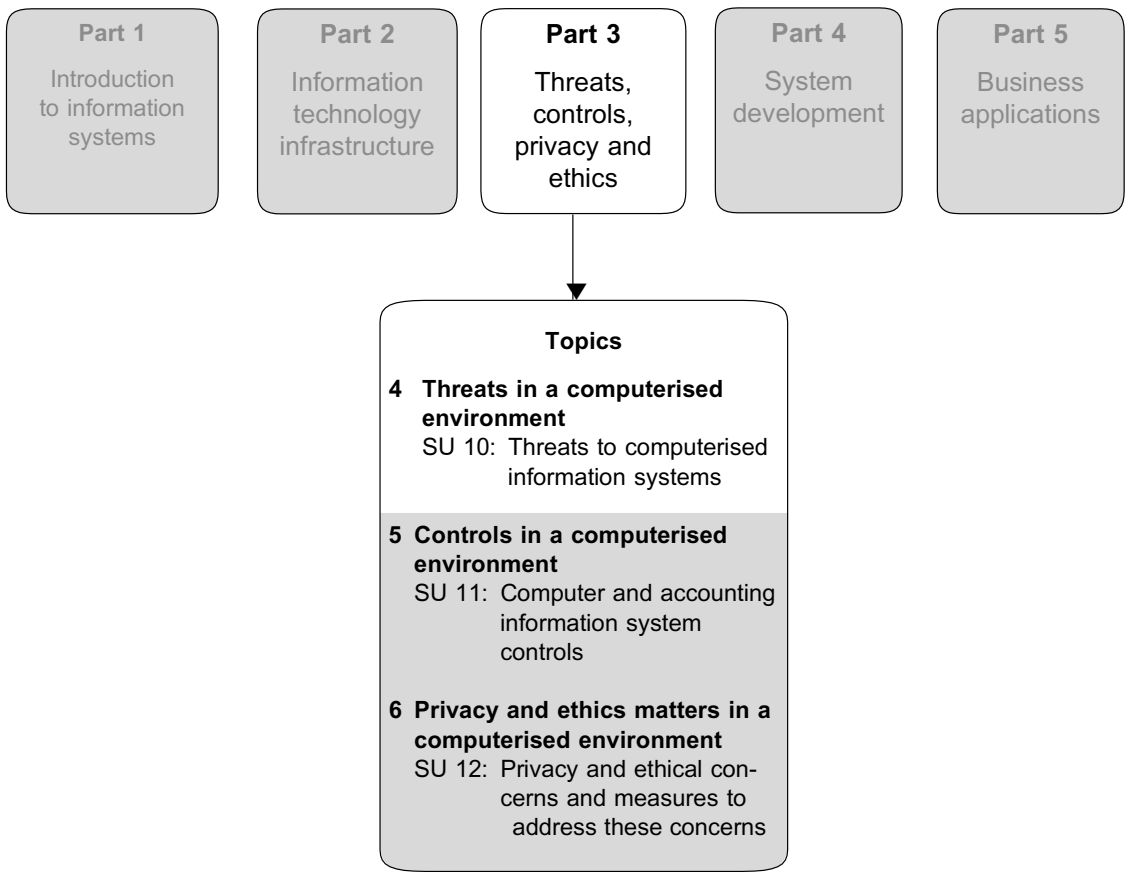
Threats in a computerised environment

LEARNING OUTCOMES

After studying this topic, you should be able to

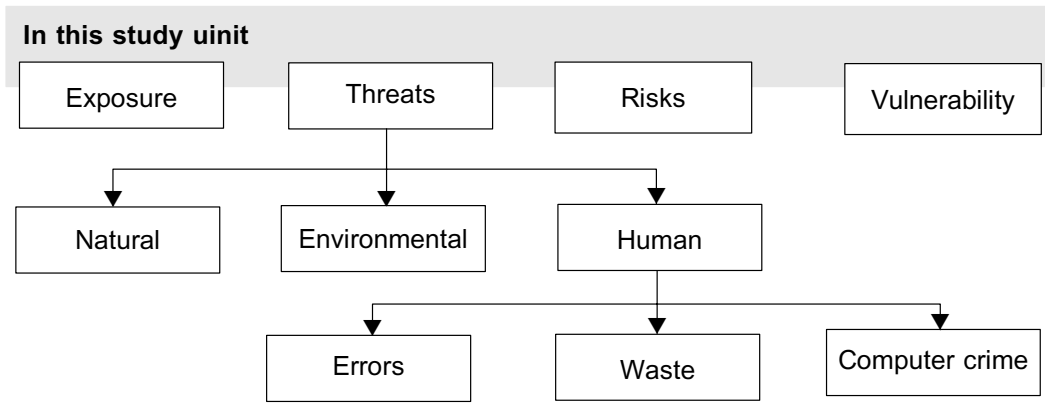
– explain the relationship between vulnerability, threats, exposures and risks
– list and describe the common threats to an information system

This topic consists of one study unit



STUDY UNIT 10

Threats to computerised information systems



1 INTRODUCTION

Today, most organisations have become strongly reliant on complex information systems. Even the most insignificant weakness in an information system might have a significant negative impact on the confidentiality, integrity and availability (also known as the CIA triad) of the information produced by the information system. This is true for both a manual information system and a computerised information system.

In this study unit, we will first explain the terms *vulnerability*, *threat*, *exposure* and *risk* and then explain the differences between them, after which our primary focus will be on the possible threats experienced in a computerised information system.

2 THE RELATIONSHIP BETWEEN VULNERABILITY, THREATS, EXPOSURE AND RISKS

It is important to understand that although the terms *vulnerability*, *threat*, *exposure* and *risk* are often used interchangeably, they all have different meanings. Once you understand what these four concepts are about, the relationship between them will also be clear.

- ***Vulnerability*** refer to a security weakness or flaw in the information system that creates an opportunity for an attack on confidentiality, integrity and availability of the information (CIA triad).
- The potential exists that vulnerabilities might be exploited, either intentionally or accidentally. This potential is known as a *threat*.

- The existence of vulnerabilities in the system ***exposes*** the organisation to financial losses and can be expressed as a function of the financial impact and the probability that these events will occur.
- A ***risk*** can be explained as the likelihood of the attack on information assurance occurring, that is, the probability of the vulnerability being exploited, and can therefore be quantified.

3 COMMON THREATS TO AN INFORMATION SYSTEM

Most organisations use an information system to process financial and operational data. Various threats may exist in such an environment because of system flaws, for example due to human error, revenue may be overstated in an instance where an invoice amount is captured as R40 000,00 instead of R4 000,00. However, the spotlight in this section will fall on potential threats in a computerised information system rather than a manual information system.

As explained earlier, threats exist because of certain vulnerabilities. These threats can be caused by nature, for example natural disasters, the environment such as power failures or human error.

3.1 Natural threats (resulting from natural, external vulnerabilities)

Natural threats are a result of natural disasters and include floods, fires, winds, thunderstorms, earthquakes and avalanches.

3.2 Environmental threats (resulting from environmental, internal vulnerabilities)

Environmental threats are because of internal vulnerabilities in the form of liquid leakages, chemical waste, power outages, various forms of pollution and environmental breakdowns.

3.3 Human threats (as a result of the acts of human beings)

The majority of threats to a computerised information system are known as *human threats.* These threats exist because of human beings and include errors, omissions, sabotage and, specifically, computer crime. We are now going to spend some time discussing these human threats.

3.3.1 Errors

Even though an information system might be computerised, human involvement will still be required to a certain extent. *Errors* include mistakes, failures, omissions and computer problems due to unintentional staff intervention, resulting in the output of an information system being inaccurate or useless. Errors can be a result of insufficient training, miscommunication of expectations or poor feedback.

Examples include IT staff updating hardware and making an installation error, or data capturers making errors while processing high volumes of transactions.

3.3.2 Waste

Computer waste can be broadly defined as the inappropriate use of computer equipment and resources, resulting in excessive costs and decreased profits. Computer waste is usually the result of poor computer resource and time management. Examples of waste

include employees printing documents they never read, surfing the net or visiting social networking sites during work hours or sending unnecessary e-mails from their work account. However, one of the best-known forms of waste is computer *spam*.

> ***Spamming*** is the use of e-mail for marketing purposes in the form of bulk messages sent to various e-mail addresses, instant messaging or social network profiles or cell phones. The user of the e-mail account, social network, instant messaging system, or cell phone has never indicated a desire to receive the advertising material and usually struggles to unsubscribe from the source.

3.3.3 Computer crime

Computer-related crime includes a wide range of illegal activities in which a computer and/or network are used as a **tool to commit a crime** or where a computer and/or network are **the target of a crime.** These two characteristics are also used to categorise computer crime.

> ***Cyber criminals*** are **persons committing computer crime** and include crackers, organised crime groups, terrorist and terrorist support groups, current and former disgruntled and unethical employees, and other insiders who have or have had authorised access to the information system, for example computer system consultants.

Cyber criminals are getting increasingly better at perpetrating cyber crime as they reinvest their profits in developing new capabilities for circumventing security technologies and buying the latest and best hardware. Computer-related crime will therefore in future become increasingly severe and complex and organisations will find it increasingly difficult to prevent and detect these crimes.

Owing to the wide variety of computer crime that occurs, only the more common types will be discussed for each of the main categories.

Computers and/or networks as tools to commit crime

- The ***motivations*** of hackers and crackers may differ, but their aim is similar, that is, to gain unauthorised access to a computer system by overcoming the security controls (*hacking*). Hackers hack into a system as a form of entertainment as well as to display their technical skill. In contrast, crackers are intent on causing damage to the system or stealing information from the system.
- ***IP spoofing*** means to forge the source IP address thereby concealing the actual IP address and making it appear to be the IP address of a trusted or authorised source. This enables the cyber criminal to remain anonymous while carrying out criminal activities. For example, by using IP spoofing, a criminal can send a fake sales order to an organisation, which seemingly comes from a legitimate client. This organisation might then manufacture and deliver goods that were never ordered thereby incurring unnecessary costs.
- ***Computer forgery*** takes place when advanced computer technology and programs are used to forge documents, for example official letterheads, matric certificates, degrees and identity documents. These forged documents are then used to commit fraud.
- ***Computer fraud*** can be defined as any fraudulent activity where a computer, computer system, or network is used to unlawfully take, alter, or use information or computer programs. Examples of computer fraud include altering accounting transaction data to conceal unauthorised, fraudulent transactions or deliberate

altering of a computer program's logic to calculate interest incorrectly for the benefit of the computer fraudster.

- ***Computer-related scams*** are a subsection of computer fraud and usually offer too-good-to-be-true deals, requiring sensitive personal information from the victim or money to be paid into the cyber criminal's bank account. For example, the victim is informed, via e-mail, that he has won a large amount of money in a foreign lottery and that the money will be paid out after the receipt of an amount of money for administration fees.
- ***Malware*** refers to malicious software designed to destroy and interrupt business operation and information through illegal access and use. It includes the following:
  - A ***computer virus*** is a program or programming code that replicates or copies itself repeatedly without the user's knowledge or consent. Viruses spread via attachments to e-mails and downloaded files or are copied to a USB flash drive or CD.
  - A ***worm*** is also a self-replicating program or program code, but differs from a virus in the sense that it does not need to be attached to an existing program. These copies are sent via the computer network to other computers in the network.
  - The distinguishing characteristic of a ***Trojan horse*** is that it looks like a valuable application, but is in fact only disguising a destructive program such as a virus, worm, logic bomb, and so on.
  - A ***logic bomb*** is an intentionally inserted program code that will set off a malicious function (eg delete or corrupt data or files) when triggered under certain conditions.

Activity 10.1

In January 2011, Douglas Duchak was sentenced to two years in jail for planting a logic bomb at the Transportation Security Administration's (TSA) Colorado Springs Operations Centre. Luckily, the logic bomb was discovered before it could execute. Read the full story at http://www.wired.com/threatlevel/2011/01/tsa-worker-malware.

Roger Duronio successfully planted and executed a logic bomb at UBS Paine Webber, which brought down 2000 servers at the investment bank, just because he was unhappy with his bonus. For his trouble, he was sentenced to eight years in jail. Read about him at:

http://www.theregister.co.uk/2006/06/08/ubs_hack_attack
http://www.theregister.co.uk/2006/12/13/ubs_logic_bomber_sentenced

---

- A ***Rootkit*** is a tool that grants an attacker continuous full access to a computer while hiding its presence. A well-written Rootkit can rewrite a computer's login script, which will then accept the cyber criminal's login even if the user or administrator tries to *change* it.
- ***Spyware*** is, as the name says, software that 'spies' on a user. The spyware programme will secretly transmit personal information or web browsing habits to a cyber criminal. The user is typically unaware of this invasion of privacy.
- ***Advertisements*** rooted in a software package, which typically display as a popup message are known as adware. The purpose of adware is to generate web traffic and obtain e-mail addresses.
- A ***blended threat*** refers to a combination of different malware used to exploit the vulnerabilities in a system.

- ***Identity theft*** occurs when personal information is acquired and used fraudulently without the owner's knowledge or consent, for example targeting tourists during a world sport event to steal their identity documents or passports. Identity theft is not limited to natural persons but also entails the theft of an organisation's identity. Identity theft is used to obtain goods and services fraudulently; withdrawing money from the victim's bank account, blackmail, terrorism, illegal migration, and so on. Criminals steal a person's identity by stealing e-mails, going through garbage, wallets and handbags, spyware, and so forth. Other methods used include social engineering, shoulder surfing and phishing.
- ***Social engineering*** means to study the user's social networking profile or chat rooms to get clues on what the user's password might be as people usually use something familiar as their password, for example, a loved one's or a pet's name, a favourite musician or writer.
- ***Shoulder surfing*** refers to hadowing the targeted user to 'accidentally' see or hear the password.
- ***Phishing*** literally means to 'fish' for sensitive personal information such as usernames, passwords, online-banking login details, credit card details. Phishing misleads the victim into thinking that electronic correspondence has been sent by a trustworthy source, for example a financial institution, thereby luring the victim to a spoofed (fraudulent) website. At this spoofed website, the victim is requested to divulge sensitive personal information. Both the e-mail and the spoofed website usually appear to be those of legitimate organisations. It is important to train users to be aware of the danger of phishing attacks.

  In South Africa, online banking users are the main targets of phishing campaigns. Below are two examples of phishing e-mails (the identities of the banks were changed):

From: Internet Banking Support [internetsupport@secureabcbank.com]

Sent: 25 November 2010 11:08

To: Viviers, Gerharda

Subject: Re: ABC-UpdateProcess-

Dear Valued Customer,

Additional security on our website brings unity and combined strength to our commitment to provide exceptional internet banking services.

It is strongly required that you upgrade your accounting to secure your funds, click below:

www.ibsecure-abcbank.com

ABC Bank

This e-mail was sent automatically please do not respond

Payment Made by Trustworthy Bank

Dear Customer;

A payment has been made to your account. To view the details of the payment, please **click here to login.**

If you have any questions or would like more information, please contact our support centre on 0860 123 000. If you are calling from outside South Africa, call **+27 11 299 4701**.

Our consultants are available between 8am and 9pm on weekdays, and 8am and 4pm on weekends and public holidays.

The Internet Banking Team

Activity 10.2

Log onto http://www.absa.co.za/Absacoza/Security-Centre/Banking-Security/Phishing-Scams to view more examples of phishing e-mails.

- *Acts of terrorism* committed using computers and computer networks are called cyber terrorism. Cyber terrorists believe that their political or social views will be advanced if they intimidate the government or organisation by destroying or threaten to destroy critical infrastructures (eg government defence system, emergency services, air traffic control, financial or banking system) or valuable information.
- *Cyber extortion* is similar to cyber terrorism, but the motivation is different. Where the cyber terrorist believes that the attack is for the greater good, cyber extortion is conducted for personal gain in the form of money being extorted from the victims to, for example, stop denial-of-service (DoS) attacks against a website. A *DoS attack* involves flooding the target website with phony data, messages, or requests, resulting in an extremely slow website response or crashing the e-commerce website completely.

You will learn more about DoS attacks in study unit 22.

Information systems as targets of crime

- *Software piracy* occurs when software is illegally copied. Software can be copied from a friend or employer, or even bought from somebody who has made a number of illegal copies from the original software. This is illegal as most software is copyright protected. Individuals and organisations are at risk of facing legal charges or criminal prosecution if properly licensed software is not used.
- The *theft of data* involves stealing data and can result in the loss of trade secrets, intellectual property and a competitive advantage over competitors. *Industrial espionage,* involving spying in a corporate environment to obtain data that is used to advance another organisation, is one of the best-known methods of committing

data theft. As data storage devices become smaller with larger storage capacity, the theft of data becomes easier. For example, many employees use their private unprotected USB flash drives to take work (data) home. This creates a security threat, as USB flash drives (and the data on these drives) are easily stolen or lost.

- The *theft or destruction of computer equipment,* for example monitors and desktops, often occurs in instances where organisations have not implemented sufficient policies and procedures to safeguard computer equipment. The motivation behind this crime is not always to gain possession of the physical asset itself, but may be to obtain access to the information stored on the computer.
- One of the most common computer crimes committed by an organisation's employees is the *theft of computer time*. This involves the unauthorised use of an organisation's computer resources for the employee's own personal financial benefit. An accountant may use the organisation's accounting software to prepare financial statements for private clients or a graphic designer might use the graphic design software to create an advertisement for her private clients.

Activity 10.3

a. Describe a situation where your family or friends were a victim of computer crime.
   - Explain what type of computer crime they fell victim to.
   - Explain whether the computer was the *tool* of the crime or the *object* of the crime.

b. During a visit to your friends, the subject of cyber crime is discussed. Most of your friends have heard of the term but do not know what it means.
   - Explain computer crime to them.
   - List some examples of computer crime.

c. If you are interested in computer crime and would like to read more about it, you can visit the online encyclopaedia – Wikipedia and search for computer crime or malware. You should find some interesting information.

---

4 SUMMARY

We started this study unit by explaining the terms *vulnerability*, *threats*, *risks* and *exposures* and discussed how these concepts are linked. Our focus in this study unit was the threats faced in a computerised information system environment. We established the three main causes of threats, that is, natural, environmental, or human behavioural causes. Threats resulting from human behaviour include errors, waste and computer crime. We also spent time to look at the various forms of computer crime.

These threats are present every day and do not only affect organisations, but also our private lives. You, as an accountant, must be aware of these threats as they might affect the organisation's reputation and profitability. This study unit has drawn our attention to the problem of computer crime; the next study unit will point us towards the solution. Study unit 11 will discuss controls to be implemented to prevent these threats being exploited, or in the case where attacks have already occurred, we will look at controls to minimise the impact.

Self-assessment

a. Briefly explain the terms *vulnerability*, *threats*, *exposure* and *risks*.
b. List and briefly discuss the three types of threat faced by an information system.
c. Briefly describe computer-related waste and computer-related errors.
d. List the two main categories into which computer crime can be categorised.
e. List and briefly describe four computer crimes committed where the computer is the target of the crime.
f. List and briefly describe eight computer crimes committed where the computer is the tool used to commit the crime.
g. Briefly explain the following examples of malware
    - Computer virus
    - Trojan horse
    - Worm
    - Logic bomb
    - Rootkit
    - Blended threat
    - Spyware
    - Adware

h. Name and briefly describe three ways to commit identity theft.
i. Discuss computer fraud and give a suitable example.

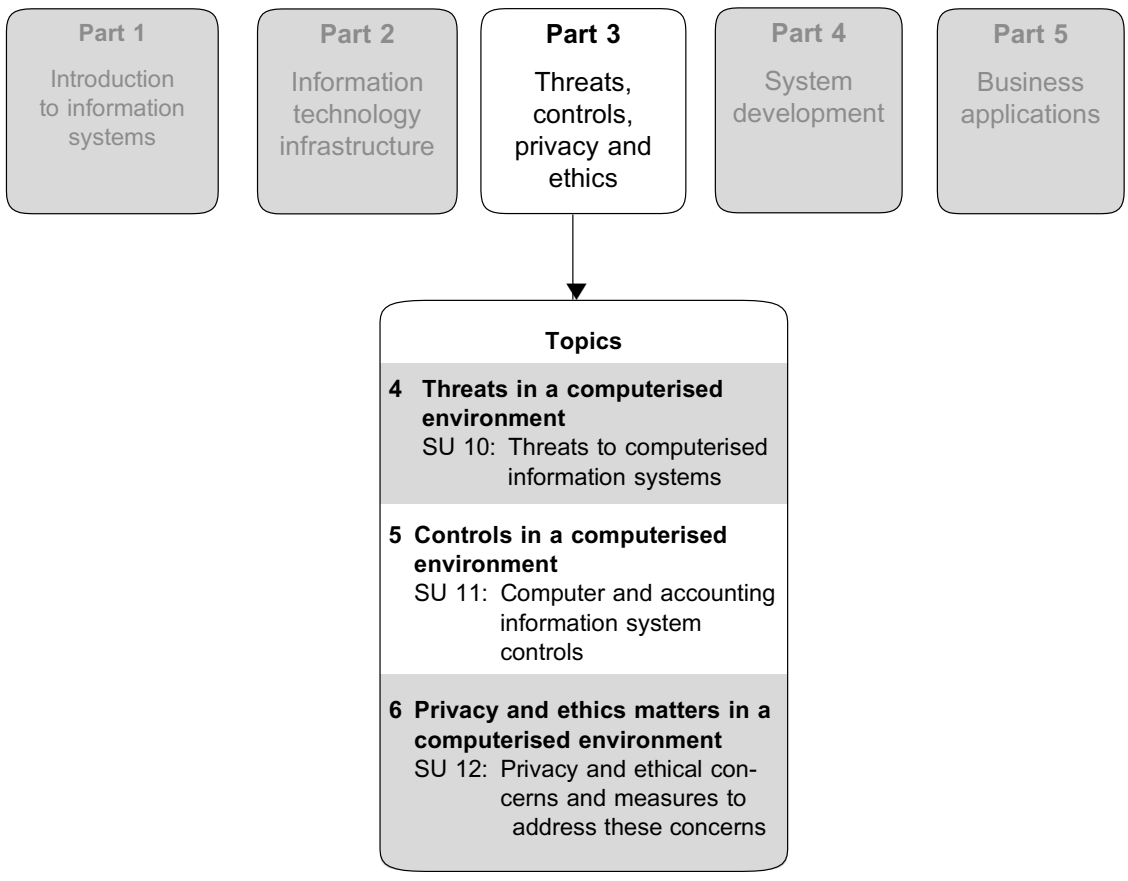
Controls in a computerised environment

LEARNING OUTCOMES

After studying this topic, you should be able to

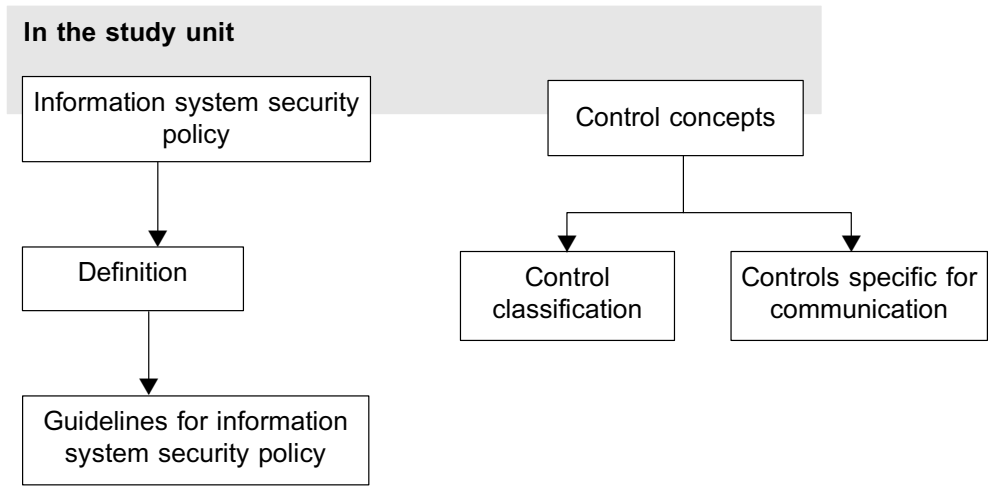
- explain the importance of and list general guidelines for an information system security policy
- identify organisation board responsibilities for IS governance in line with the King III report
- describe general and application controls, including disaster planning
- describe preventative, detective and corrective information system controls
- explain the components of disaster planning

This topic consists of one study unit



STUDY UNIT 11

Computer and accounting information system controls



1 INTRODUCTION

As you already know from previous study units, information is no longer only a nice-to-have, but rather a necessity in the business environment, enabling users to make sensible decisions.

In order for information to allow users to make informed decisions, information should meet the requirements of the CIA triad, that is, confidentiality, integrity and availability. In the previous study unit, you were introduced to various threats to the confidentiality, integrity and availability of information.

Before we carry on, let us review the difference between a threat and a risk. A ***threat*** is the potential that a vulnerability in a system will be exploited, while a ***risk*** refers to the probability that the vulnerability will be exploited and therefore risk can be quantified.

The only way to address the threats mentioned in study unit 10 is to develop an organisational ***information system security policy*** stipulating the control procedures to be followed. Before developing an information system security policy, an organisation will need to determine any threats to the existing information and then perform a ***risk assessment***. A ***risk assessment*** refers to the quantification of the likelihood of these threats resulting in the information system being attacked.

> You will learn more about risk assessment in Principles of strategy, risk & financial management techniques (MAC2602), as well as in the Auditing modules.

In this study unit, we will assume that a risk assessment has already been carried out. The purpose of this study unit is to introduce you to the controls that should be in place to mitigate any threats that have been quantified as risks. We will start this study unit by giving you some guidelines to follow when compiling an information security policy. These guidelines are based on the King III report, the Information Security Forum (ISF) and the Control Objectives for Information and Related Technologies (CobiT). The final section of this study unit will discuss controls classified by type and function and then focus on disaster planning.

2 INFORMATION SYSTEM SECURITY POLICIES

2.1 Defining an information system security policy

An *information system security policy* is a ***formal document*** describing the ***procedures*** to be followed by the organisation when ***addressing threats*** to the information system. The policy provides a ***framework*** for the **measures** to be taken to ensure ***sufficient protection*** of the information system.

2.2 Documents containing guidelines for an information system policy

The likelihood of threats or risks being exploited can be largely minimised, by implementing sound internal control processes in the form of a good control environment and an information system policy. The internal control process, comprising the control environment, risk assessment, the information system, control activities and monitoring of controls, will be discussed in detail in the Auditing modules.

Organisations should take a step back and carefully consider the components included in their information system policy, as these will differ from organisation to organisation.

There are, however, a number of documents containing guidelines for information system control. These are aimed at helping the organisation when compiling an information security system policy.

The documents we are going to discuss both refer to Information Technology (IT) governance. It is important to remember that there is an academic difference between the term Information System (IS) and Information Technology (IT). In the business environment, these two terms are used interchangeably and are therefore treated in a similar manner in this study unit.

These documents include the following:

2.2.1 The CobiTframework

The *Control Objectives for Information and Related Technologies* (CobiT) is a well-known framework with the main objective of assisting management to find a balance between risk and control investments in a fickle information system environment by implementing an information technology (IT) governance system.

IT governance refers to the structures and processes in place to ensure that IT benefits are delivered to help the organisation achieve and sustain success in the end.

Management should ensure that adequate investment is made in an information system, finding a balance between too little investment, which might expose the organisation to information system risk, and too much investment, which might lead to unnecessary cost.

CobiT follows a top-down approach to an information system:

- High-level control objectives are defined for every information system process.
- Information system processes are linked to specific detailed control objectives.
- Auditing guidelines support the control objectives in order to determine how these objectives can be monitored.

If you are interested in reading more about CobiT, you can visit the Information Systems Audit and Control Association's (ISACA) website at www.isaca.org/.

2.2.2 The King III report

The King III report was released in South Africa in September 2009 to address reduced institutional and individual investor confidence resulting from business failures and dubious accounting restatements. The report provides guidelines for restoring and maintaining investor confidence through good corporate governance. The concept of corporate governance will be discussed in study unit 12.

In the King report, *information technology (IT) governance* features as a new and expanded area. As a subset discipline of corporate governance, it will have an influence on risk management, assurance and reporting frameworks. Ultimately, IT governance is the responsibility of the board of directors and should, therefore, be taken into account when compiling an information system security policy.

According to King, the board's responsibilities include

– aligning IT objectives with the performance and sustainability objectives of the company
– delegating responsibility for the implementation of an IT governance framework to management. The CEO should appoint an appropriately qualified chief information officer and an IS steering committee should be established.
– monitoring and evaluating significant IT investment and expenditure with regard to the measurement and management of value received
– complying with relevant IT laws and standards as part of risk management
– appointing a risk committee to ensure that IT risks are addressed and the necessary controls implemented
– appointing an audit committee to consider IT in the financial reporting process and the consideration of whether an organisation can be classified as a going concern. (You will learn more about this in the next section.)
– managing information assets through the implementation of formal processes to manage and protect information, including personal information privacy

2.2.3 Information Security Framework (ISF)

The ISF was established in 1989 as an independent, not-for-profit organisation. The aim of this body is to supply authoritative opinion and guidance on all aspects of information security. The ISF offers valuable services to its members, including a library full of research and report material on information security, information risk management and related topics.

If you would like to find out more about the ISF, you can visit their official website by clicking on the following link: https://www.securityforum.org/

3 CONTROLS

Controls can be classified using various methods. Two of the most common ways is according to the type of control, which includes general and application controls, or by the function of the control, which includes prevention, detection and correction. Specific system controls should also be implemented to ensure reliable data communication and the safeguarding of assets. It is important to take into account that a control can fall into more than one category. For example, the control of duty segregation can be classified as both a general and preventive control.

3.1 Controls classified by type

This section of study unit 11 will introduce you to the controls that are applicable in a computerised information system environment. However, an in-depth study is included in the Auditing modules, where the focus will be on controls related to the information system as a whole.

Controls in an information system environment can be classified by type:

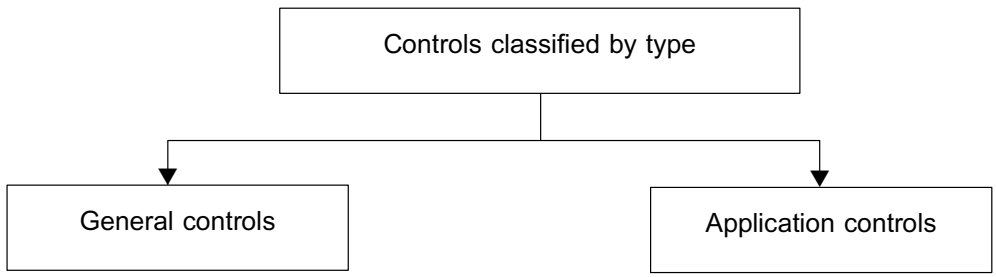


FIGURE 11.1: Controls classified by type

3.1.1 General controls

General controls are overall controls affecting all transaction processing. General controls are implemented to ensure the effective operation of the organisation's accounting information system.

General controls	
Organisational controls	***Segregation of duties*** within each task in the transaction cycles should be present. By ***segregation of duties,*** we mean that one single staff member should not be responsible for the initiation, authorisation, processing and review of a transaction. In a computerised transaction processing system, the segregation of duties regarding system development and data processing is extremely important.
Operational controls	Every task within the transaction processing system must be described in a ***procedure manual***. These manuals should be kept in a safe place, such as a fireproof safe. Only ***competent staff*** should be appointed to take responsibility for the transaction processing system. Training will also ensure staff competence. Rotation of tasks assigned to certain staff should be done on a random basis. A sound control environment starts with ***management*** in a top-down approach. Management could implement general controls – for example compiling a policy on changes, or development system procedures and human resource policies and practices that make a commitment to excellence.

Controls to protect the IT environment	The information centre is the place where all the information system activities take place. The controls listed below are all examples of restricting access to the computer or information. • ***Controls against human access*** to the information centre should be implemented. These controls include fences around the restricted area; locks and keys to restrict access to the information centre; key staff wearing badges to tell them apart from intruders, physically inspecting the restricted area and consulting a logging access report of the area over a specific period. It could also include installing biometric access controls, which involve using computer software to identify fingerprints, handprints, voice patterns, signatures and retinal scans of individuals authorised to enter the restricted area. • ***Access to computer and information***: Access control software ensures only authorised users obtain access to powerful programs and sensitive information by controlling and monitoring user access and the way information is shared between users. Access control software *firstly controls the identification* of users, that is, users need to identify themselves usually through user IDs (login IDs) or unique account numbers (your bank account number for example). The user is then taken through an *authentication process* (eg entering a password) to verify the user is the person he/she claims to be. After users have been identified and authenticated as authorised users, *access control lists* will define the specific programs and data they have access to and what permissions they have (read, write, copy, etc) (Dull, Gelinas, & Wheeler, 2010, p 281). Different permissions and access to programs and data can be assigned to different users. For example, only the human resources manager and the divisional manager will have access to individual staff members' salaries on the staff system. The financial clerk will only have access to totals for the entire division's salary bill to enable him/her to process the necessary transactions in the financial system. The human resource manager might only have view (read) access of the salary bill in the financial system while the financial clerk will have processing (write) rights. It is management's responsibility to ensure the implementation of an access control policy. Passwords, usernames and personal identification keys (PIN) are effective ways of preventing unwanted computer access. Individuals should take care when selecting passwords, PINs, or usernames that it will not be easily identifiable or obvious for intruders. Passwords should include numbers, capital letters and special characters and should not be a word related to your everyday life. Also never divulge your password, especially not to somebody you do not know very well. • ***Firewalls*** are technological barriers designed to prevent unauthorised or unwanted communication between computer networks or hosts. • ***Encryption***: This is a process of transforming information into a readable format and is a measure of control. Encryption is the conversion of data into a form called cipher text that cannot be easily understood by unauthorised people. *Decryption* is the process of converting encrypted data back into its original form, so that it can be understood.

	Controls against natural elements are very important for preventing or minimising the impact of disasters and include the following (disaster planning is discussed in the next section): • ***Back-up power***, in the form of an uninterrupted power supply (UPS), generators or solar power to prevent damages to equipment or loss of information in the case of power failures. • ***Smoke detectors***, which alert staff and emergency services to the possibility of a fire. Early detection can help to prevent or limit the damage to computer equipment and save lives. The information centre should have sufficient ***fire extinguishing equipment*** in order to prevent the spread of fires in emergencies. • If the ***floor*** in the information centre is ***raised*** it will prevent water damage from flooding. ***Temperature control*** in the information centre is necessary to prevent damage, as computer system should be kept at a constant temperature. • It is important to pay a monthly ***insurance*** fee to enable the organisation to replace computer equipment in the event of damage or loss. • ***Maintenance*** on computer equipment should be done on a regular basis to monitor the usability of hardware.
IT asset accountability controls	Controls ensuring the accuracy of information should be implemented and executed by staff who are not responsible for processing or capturing of transactions, for example: • The details of control accounts in the general ledger should be documented in subsidiary accounts. • Reconciliations should be prepared by a staff member who is not involved in capturing and reviewed by an independent senior staff member.

3.1.2 Application controls

Application controls are specific to the functioning of individual applications. Application controls relating to a computerised information system comprise the following:

Application controls	
Input controls	The purpose of input controls is to prevent and detect errors when entering information into the information system in order to ensure validity, timeliness and accuracy. ***Input edit*** checks of transaction data, for example check digits, incorrect dates or date formats, completeness checks to ensure no blank fields are recorded, visual verification to confirm the general reasonability of documentation. See discussion on programmed edit checks under *Detective controls* as well. ***Data transcription,*** for example using a batch control log, batch serial numbers. ***Data observation and recording*** using record counts, control totals or other ways to balance the input totals with the source documents. ***Transmission of transaction data*** by using for example transmittal documents (batch control tickets) or read backs where the sender immediately receives feedback on the input information for comparison and approval purposes.

Processing controls	Processing controls are designed to ensure that *all* transaction data have been processed accurately and in time. When the processed information is reviewed, the reviewer needs to confirm that no data were lost, altered, or added during processing. Processing controls are also important to ensure that the database and files stay maintained. Examples of processing controls include the following: ***Physical inspections and checks***: These may include reconciliations, checking the work of another employee and acknowledgements. ***Logic checks***: Programmed edit checks such as sequence and reasonableness checks may also be applied in processing. For example an input value should not be 0 when there will be a number that divides it somewhere in a program. See discussion under *Detective controls* to see how this works. ***Run-to-run totals***: To ensure batched data are completely and accurately transferred between processes, output control totals are calculated and used as input control totals for the next processing sequence, thereby linking the one process to the next (Bodnar & Hopwood 2004:127).
	Audit trails: An audit trail is a set of steps put in place to keep proof of each action taken to execute a business process, for example keeping complete original records like receipts, etc of petty cash transactions. It enables individual transactions to be traced, provides support for general ledger balances, data to prepare financial reports with and correct errors where applicable.
Output controls	Output controls ensure the reliability and integrity of output information after the input and processing phase. • The output information should be reconciled to the input data based on documented procedures. • Discrepancy reports should be generated and investigated. • Files should be verified and audited on a surprise basis.

3.2 Controls classified by function

Preventive, detective and corrective controls create a three-layer internal control shield. Figure 11.2 below illustrates this control shield.

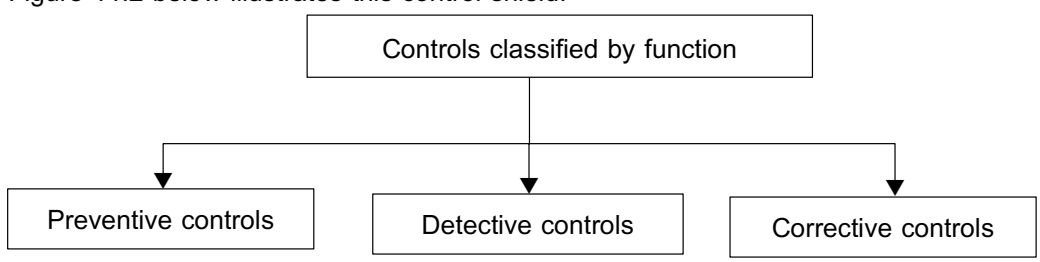


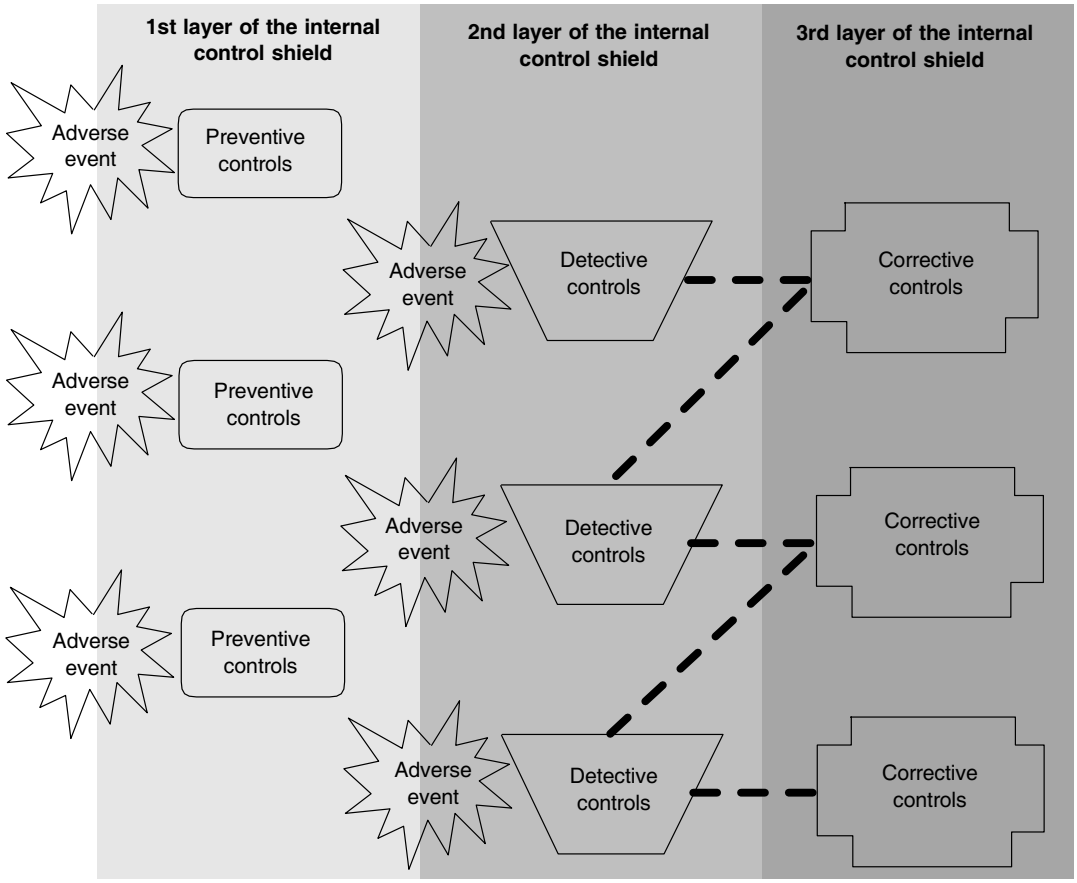
FIGURE 11.2: Controls classified by function

3.2.1 Preventive controls

Preventive controls are the first layer in the internal control shield. ***Preventive controls*** prevent and discourage adverse events such as fraud, errors, theft, loss, and so on from occurring. Implementing preventive controls and thereby preventing adverse events

from occurring is more cost effective and creates fewer interruptions in the normal operations than detecting and correcting adverse events after they occurred (Dull et al 2010:242). Examples of preventive controls include the following:

- ***Backup of data and documentation***: It is vital that backup copies of all important data and documentation are readily available in the event of original data being destroyed or damaged. Backups of important data should therefore be made regularly as per a pre-defined backup plan. For example, most financial system data is backed up daily, weekly, monthly and yearly. Files should be backed up on a different storage device, which is also physically removed from the original data storage device, to ensure that the backup data is not destroyed or damaged in the same adverse event that damaged the original data, for example a fire. Backup files must have the same level of protection as the original data and documents, as they contain the same



Source: Hall (2011:130). Adapted.

FIGURE 11.3: Shield approach to internal control

sensitive information and are open to cyber crime, corruption and destruction as well. Backups must be regularly tested to ensure backup files are uncorrupted and that the relevant data and documents are being backed up.

- ***Antivirus software:*** This software is used to prevent virus infections on computers and computer networks. Depending on the antivirus software program, the software will scan the computer, computer networks, e-mails, secondary storage devices, and so on regularly for viruses. As soon as a virus is found, the program will 'clean' the virus, that is, destroy it. It is very important not to ignore a virus warning from antivirus software. Antivirus software must also be updated regularly to ensure it protects against the latest viruses.
- ***Antispyware***: Antispyware is similar to antivirus software, the only difference being that antispyware protects the computer and computer system against the installation

of spyware. As with antivirus software, antispyware must be regularly updated to ensure it protects against the latest spyware.

- ***Spam management software***: Spam management software, filters e-mails to identify spam. If an e-mail is identified as spam, the e-m*ail is quarantined* and not delivered to the recipient's e-mail account. Recipients are informed of the e-mail and can usually request the mail administrator to release the e-mail, if it is not spam. If no instruction to release the e-mail is received, the e-mail is automatically deleted after a pre-determined time. It is important to allow recipients to identify spam e-mail senders and for the mail administrator to add these spam e-mail addresses to a list of e-mails that are automatically blocked as spam. A recipient must also be able to remove an e-mail address from the possible spam list so that e-mails from that specific e-mail address will go to the recipient's e-mail address directly and not be quarantined first.
- ***Training of staff***: Staff must understand why controls are imposed, what the benefits of these controls are and how to execute these controls. This will ensure staff will not try to circumvent controls and that they know how to execute controls properly. For example, they know how to make backups or why it is important not to share your password with colleagues.
- ***Software change and implementation controls***: These controls ensure that only authorised changes are made to existing software programs or that only authorised new programs are installed on the computer network.
- ***Adequate disposal of used/damaged/redundant equipment:*** When hardware reach the end of its useful life, (technological redundancy, damage, etc), a decision regarding the proper disposal needs to be taken in order to ensure that the confidentiality of data is maintained and the negative impact on the environment is minimised.

Other examples of preventative controls, which have already been discussed earlier in this study unit, are

– encryption
– firewalls
– biometric access controls
– raised flooring and temperature control in the computer room
– physical access controls such as locks, fences, alarms and security guards.

3.2.2 Detective controls

Detective controls are the second layer in the internal control shield. ***Detective controls*** search for, uncover and identify adverse events after they have occurred. Detective controls are very important, as it is impossible for preventative controls to ensure that all adverse events are anticipated and prevented before they occur. After each adverse event uncovered by the detective controls, organisations should determine the reason why the preventive controls did not prevent the adverse event and revise existing or implement new preventive controls where necessary. We can therefore say that detective controls help to assess the effectiveness of the preventive controls. Examples of detective controls include the following:

- ***Programmed edit tests***: These detective controls are automatically performed by the application software used in the data entry. Depending on the software program, errors identified can reflect immediately on the input screen to allow the input clerk to take corrective steps instantaneously to rectify the data, or the errors can reflect on an error report created periodically, and the errors must be corrected at a later stage. Some of the programmed edit tests which can be performed include the following:

- ***Check digit***: A check digit is used to verify the accuracy of an entered numeric code (eg bank account number, ID number, inventory bar code). The check digit is usually the last number of the numeric code and is calculated by applying a mathematical formula to the basic code (the other numbers in the numeric code). When the numeric code with the check digit is entered, the computer will automatically recalculate the check digit. If the check digit is not the same, the computer will indicate that the numeric code has been entered incorrectly and must be re-entered. A very simplistic example is the following: An inventory bar code, 756-543-6, is seven digits in length. The first six numbers is the basic code and the last number is the check digit. The check digit is calculated as the sum of the first three numbers less the sum of the last three numbers, that is, 6 [(7 + 5 + 6)-(5 + 4 + 3)]. If, for example, this specific inventory bar code is entered as 756-643-6 the computer will recalculate the check digit and get 5 instead of 6. The computer will then flag the inventory bar code as incorrectly entered. In practice, the mathematical formulas used to calculate the check digit are very complicated.
  - ***Mathematical accuracy checks***: The computer will re-perform calculations and compare the answers to calculations manually performed. For example, the total of the line items on an invoice must be equal to the original invoice total captured.
  - ***Alpha/numeric checks***: Data fields can be set to contain only numeric or only alphabetic characters. The alpha/numeric test will then test if the data entered in that specific data field were entered in the correct format. For example, if a data field can only contain numeric characters (1234567) and alphabetic characters (abcde) or alphanumeric (abcd4567) characters are entered into that specific field, that entry will be flagged as an error.
  - ***Limit checks***: When data are entered, these tests check whether the data fall within preset limits. For example, the quantity sold for a specific item can only be between 0 and 100, the working hours for casual staff can only be between 0 and 15 hours per week or payment terms must be 30, 60 or 90 days.

- ***Activity logs***: Activity logs indicate which users accessed a certain system and at what time. These logs should be reviewed regularly for atypical activities, that is, users logging in at unconventional hours, as these activities might indicate fraudulent activities.
- ***Intrusion detection system (IDS)***: IDS is software that monitors and logs attempts to access computer system and networks. An intrusion detection alarm is raised if the attempt to access the system falls outside predetermined activity parameters (unsuccessfully trying to access more than three times, etc) or falls within the parameters of possible malicious attacks (the predictable behaviour of a worm). An IDS is used to detect attacks from inside as well as outside the organisation.
- ***Hash totals***: A hash total is created by adding together all the data for a specified nonfinancial numeric field (eg inventory codes, invoice numbers, supplier and customer account numbers) in a batch. (A batch is a group of transactions processed together.) The total has no specific value other than as control to ensure the batch is captured completely and accurately. This is done by calculating the hash total for the batch at the start and ensuring that it agrees with the calculated hash total for the batch at the end.
- ***Other examples***: Detective controls, discussed earlier in this study unit, are
  - run-to-run totals
  - audit trails
  - smoke detectors.

3.2.3 Corrective controls

Corrective controls are the last layer in the internal control shield. Corrective controls, also sometimes called corrective measures, commence as soon as the detective

controls have uncovered and identified an adverse event. The purpose of ***corrective controls*** is to limit and repair the damage caused by the adverse event and should bring the organisation back to its normal working operations as effectively as possible. It is important to remember that for each adverse event identified there can be more than one corrective control and that the optimum corrective control must be chosen to rectify each adverse event. As with detective controls, corrective controls can have the effect of modifying existing controls or implementing new controls.

Even with the availability of more advanced technology, the recovery of data is not certain. It is therefore of the utmost importance to ensure that backups of important documents are made regularly.

Backup data restoration: The applicable data backup is restored. This restores the data and information back to the form it was in at the point the backup was made. All transactions between the backup date and the date the backup is restored will therefore be 'lost' and must be redone. It is, therefore, very important to inform all users before a backup is restored, to ensure they have a list of transactions that needs to be redone. The restoration of a backup is the last option, as redoing work is time consuming.

Please remember that it is very important that backups must be tested regularly to ensure they can be restored. An organisation does not want to find out that backups are corrupt and cannot be restored when it needs to restore the data.

- ***Data recovery***: In the event of a damaged or corrupted secondary storage device, multiple tools can be used to recover data, including specialised data recovery software or the replacement of a broken hardware component, among other things. An operating system failure is the most common reason for the need to recover data and a CD, called a live CD, containing a complete, functioning and operational operating system, can be used to boot up the computer so that the file system error can be fixed. Data and system backups can also be made regularly for data recovery purposes.
- ***Other examples*** of corrective controls are:
  - disaster recovery of complete system (in order to minimise financial loss and prevent a material impact on the financial reporting process, controls should be in place that enable a business to resume normal operations as soon as possible after a disaster has struck the organisation)
  - fire extinguishers (to minimise the damage caused by a fire)
  - backup power (to minimise the impact of a power outage)
  - insurance (to recover damage to be able to be in operation as soon as possible).

4 DISASTER PLANNING

Disaster planning forms part of mitigating the risk of substantial financial loss resulting from an unexpected disruption of normal business operations. Disasters include so-called 'acts of God', for example fires, floods and earthquakes, or deliberate human acts, for example terrorism, human error, or even sabotage.

Disaster planning comprises two elements:

- ***Controls*** to anticipate or prevent possible disasters (covered in the previous section).
- ***Disaster recovery or contingency planning after the event***: In order to minimise financial loss and prevent a material impact on the financial reporting process, controls should be in place that enable a business to resume normal operations as soon as possible after a disaster has struck the organisation.

The focus of this section will be on the second of these – disaster recovery or

contingency planning. The purpose of this is to ensure that in the event of a disruption of normal business activity, this ensures the integrity of information and the continuity of operations with the main goal of enabling the organisation to resume normal activity in the shortest possible time.

A disaster recovery plan is implemented according to the following three steps:

- Step 1: When designing the plan, planning should commence with an analysis of the organisation's needs (needs analysis), that is, the critical resources needed, should be identified.
- Step 2: A list of priorities for recovery should be compiled based on the needs analysis.
- Step 3: Once this has been done, a planning committee can be formed to design a disaster recovery strategy for approval by the board of directors.

Contingency controls include:

- training of staff on procedures to follow in case of a disaster
  - a designated individual to be in charge in an emergency situation
  - all tasks clearly defined and assigned
  - staff should know the priority of tasks to be performed to optimise limited resources
- fire safety plan
- waterproof ceilings and floors
- sufficient drainage
- adequate maintenance plans, for example to prevent leaking pipes
- uninterrupted power supplies
- separate generators
- physical access controls
- efficient office layout
- sensible attitudes to office behaviour
- ***Standby procedures:*** although normal operations are disrupted, some services can still be rendered.
- ***Recovery procedures:*** These procedures are performed when the cause of the disruption has been discovered and rectified.
- ***Backup arrangements***: It is extremely important to make backups of hardware, software and data immediately to ensure a smooth and swift recovery. A *hot site* or *cold site* can be used to backup hardware and software and an *incremental backup* protects databases.
- ***Hot site***: A room, located some distance away from the main business operations, containing spare computers with the appropriate software installed and peripherals and telecommunication links set up and ready. Once staff have been transported to this location, the backup of the database can be restored and operations can be resumed.
- ***Cold site*** (also known as a shell): A cold site is similar to a hot site, the only difference being that the computer environment does not contain hardware. Backup hardware needs to be brought on site before the system can be operational.
- ***Incremental backup***: A weekly backup is made of all files and stored off site. Backups need to be made more often if files change on a regular basis.

5 SYSTEM CONTROLS

Controls need to be put into place to ensure data communication between users is reliable and assets are safeguarded. These controls may already be implemented as general, application, preventative, corrective or detective controls.

> In Topic 9, you will also learn about controls specific to e-commerce.

Organisations can use the following ***data communication*** controls to ensure the reliability of data communication and the protection of assets:

- *Staff controls:* passwords and identification numbers are used to allow only certain staff access to particular information. (general control, preventative control)
- *Sign-on procedure:* A sign-on procedure to gain access to computer resources requires identification numbers, passwords, and other safeguards. (general control, preventive control)
- *Database controls:* These controls include passwords and identification numbers and access control to secure the data and database. (general control, preventative control)
- *Input controls:* Standardised input forms to reduce data entry errors and identification controls and passwords. (application control)
- *Processing controls:* Passwords, identification numbers and backup copies of data are examples of processing controls. (application control)
- *Output controls:* Record output generated from the computer in files or documents, the time they were generated and their final destination. (Application control)
- *Telecommunication controls:* Secure the data and information transfer. They include firewalls and encryption to eliminate corruption and fraud. (application control)
- *Interactive processing*: With interactive processing, people interact directly with the processing component of the system through terminals or networked PCs. (application control)
- *Help facilities:* Many designers incorporate a help facility into the system or application programs that allow users to find out more about a program or feature or the type of response expected. (general control)
- *Look-up tables:* Computer programs can develop and use look-up tables to simplify and shorten data entry. (application control)
- *Restart procedure:* In cases where the application crashed or had problems, a restart procedure can be used to restart an application where it stopped. (application control)

Activity 11.1

a. List some of the controls you have learnt about and that have you seen in your workplace or in another place where you have access to a computer.
b. Explain whether the abovementioned controls are effective. Give brief reasons for your answer.

c. Speak to a family member or a friend who is employed.
   - Ask them about the controls they have encountered in their workplace and then categorise these controls according to type and function.
   - Provide a list of examples of controls they might not even be aware of.

6 SUMMARY

In this study unit, we examined ways of alleviating the threats faced in a computerised information system environment and we referred to these as controls. Controls can be classified by type or by function. Finally, we examined the controls that should be designed and implemented in order to minimise the impact of a disaster. You will learn more about controls in your auditing modules.

In the next study unit, we are going to discuss privacy and ethical matters in a computerised environment.

Self-assessment

a. List two ways in which controls can be classified.
b. List six examples of general controls in a transaction-processing environment. In one sentence, briefly explain each control.
c. Briefly explain what is meant by application controls in an information system environment and briefly describe the four main controls thereof.
d. List the three categories into which controls can be divided if they are classified in terms of function.
e. Briefly explain the difference between preventative, detective and corrective controls in an information system environment.
f. List seven examples of preventative controls in an information system environment that can be used in an organisation.
g. List examples of detective controls in an information system environment and explain briefly, why they are regarded as detective.
h. Briefly explain what is meant by corrective controls in an information system environment and give examples of such controls.
i. List five disaster recovery or contingency controls.
j. Briefly describe a hot site and a cold site.

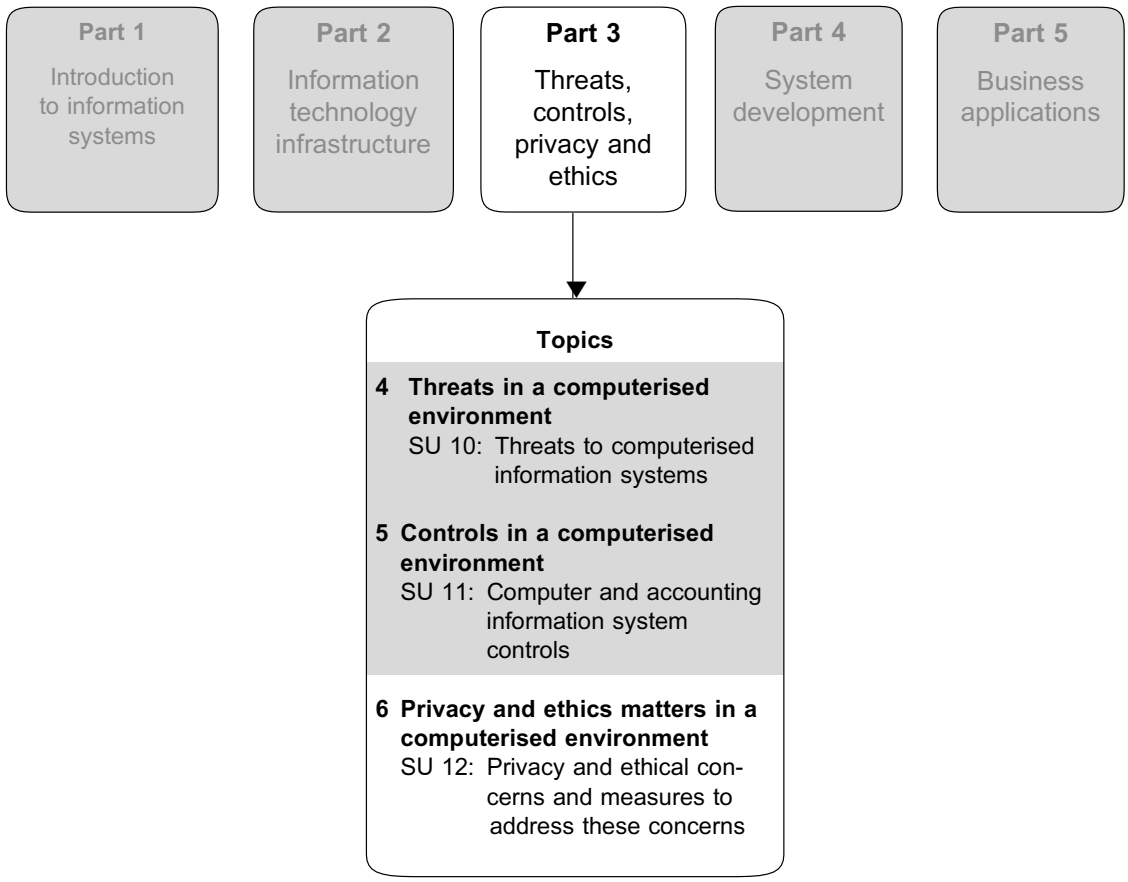
Privacy and ethical matters in a computerised environment

LEARNING OUTCOMES

After studying this topic, you should be able to

- identify privacy and ethical concerns in a computerised information system environment
- describe measures to address privacy and ethical concerns

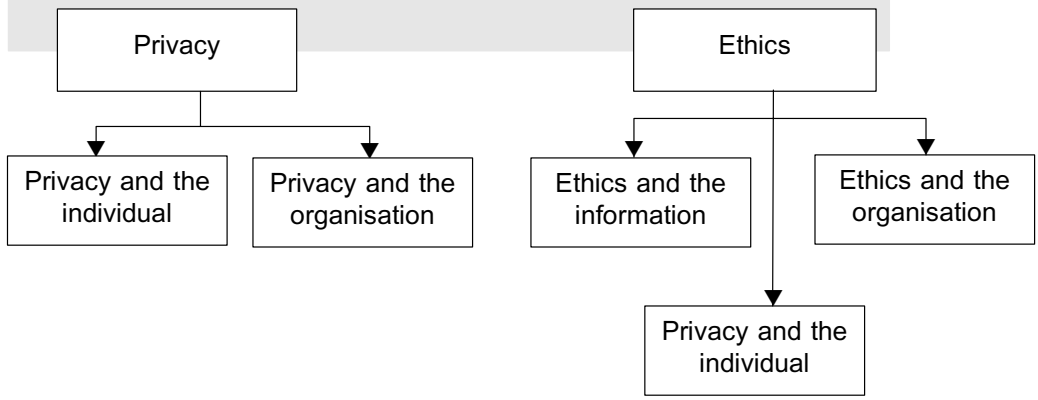
This topic consist of one study unit



STUDY UNIT 12

Privacy and ethical concerns and measures to address these concerns

In this study unit



1 INTRODUCTION

One of the greatest advantages of the internet and a computerised information system is that it makes information more available and accessible than ever before. However, there is another side to the coin. The organisation, and indeed the individual, is suddenly exposed because of a loss of privacy. This is not the only concern that needs to be addressed. The question of what can be regarded as ethical behaviour, that is, how people treat information, or what they do with it also needs to be addressed.

Study units 11 and 12 dealt with threats and controls in a computerised information system. This study unit takes this one step further by explaining what privacy and ethics are, in respect of the individual as well as the organisation, the concerns regarding privacy and ethics and possible measures to address them.

2 PRIVACY AND THE INDIVIDUAL

Respecting someone's privacy involves valuing the confidentiality of their personal information by using it appropriately and protecting the information. We as individuals use the internet on a daily basis as an incredible resource, whether it is for internet banking, social networking, research, or merely surfing the net for fun. However, it is frightening how vulnerable we are in terms of exposing ourselves to hackers who are waiting to gain access to our personal information. It is possible to retrieve deleted e-mail months later from the remote servers on which your mail was saved on its way to the intended recipient. Your browser announces your computer's unique identifier to every site you visit.

Government has a great deal of information about individuals and organisations, which raise a number of concerns about privacy. The Promotion of Access to Information Act emphasises that information should be easily accessible to those requesting it. However, this being said, always remember that you have the right to keep your personal information private. You have the right to decide with whom you will share your personal information. Moreover, it is your responsibility to be proactive in protecting your personal information.

Activity 12.1

Think of instances in your life where you are requested to provide your personal information, for example at the doctor, the bank and even when you enter a security estate.

The awareness of protection of personal information has increased even more since the Rupert Murdoch and News Corporation scandal where individuals' cell phones were hacked, violating their privacy. Click on the following link if you want to read more about the scandal:

http://www.dailymail.co.uk/news/article-2024787/Rupert-Murdoch-prevent-phone-hacking-scandal-fails-hit-News-Corp-profits.html

---

You can do the following to protect the integrity of your personal information:

- Be alert, do not share personal information unless it is absolutely necessary.
- Be proactive about the protection of your personal information, be informed about the latest scams so you do not become a victim.
- Do not provide your personal information when registering for a service without thinking twice.
- Be careful when you shop online and make sure your credit card detail, personal information and passwords are kept safe.
- Familiarise yourself with South Africa's legislation on the protection of personal information. When we wrote this study guide (2011), the Personal Information Protection Bill was still in draft form. When accepted, it will have a significant impact on the way organisations treat the information at their disposal.

You can read more about the draft legislation by clicking on the following link: http://www.dcs.gov.za/homepage_paia/Documents/Legislation/Bill-draft-privacy.pdf or search for Personal Information Protection Bill in http://www.dcs.gov.za.

3 PRIVACY AND THE ORGANISATION

In the context of the organisation, *privacy* refers to all information that is ***considered confidential*** and in need of ***protection from public disclosure***. Privacy has become an important issue owing to the vast amounts of data being made available to stakeholders of organisations. In most organisations, information is computerised making it easily accessible. It is important that proper control measures be put in place to ensure that information is managed as well as that it reaches its intended recipients only. Individuals have to respect the value and ownership of the information they receive and should not disclose any of its contents without the appropriate authority unless there is a legal or professional obligation to do so (Coetzee & Plant 2010:23).

All organisations, including their stakeholders, have the right to privacy. It is possible that information about an organisation and its employees will be abused should it be easily accessible by other organisations and/or former stakeholders with criminal intentions against the organisation in question. Controls should be in place to ensure privacy in an organisation operating in a computerised environment.

Many organisations have strict privacy policies governing the use of information. Privacy at work, for example, has shown that organisations use a computer-monitoring system that might tie directly to work stations, thus determining at any point what employees are busy with on their computers.

The following are examples of how the organisation can protect use of its assets and company time:

3.1 Computer monitoring

Computer monitoring software enables an employer to monitor the time an employee spends on specific tasks, to identify websites he/she visits, to record the employee's keystrokes and to grant the employer access to the employee's instant messaging chats. However, this method of privacy protection raises ethical concerns. Therefore, it is recommended that the employer uses this method as a last resort.

3.2 Electronic mail and voice mail

E-mail and voice mail raise a number of privacy issues in the workplace. Organisations have the right to view data sent to their servers and this is a normal routine check. However, this kind of control raises a conflict of interest, as employees also want to have privacy at work and are uncomfortable with too close supervision. It is recommended that employers should avoid going this route unless they suspect fraudulent activity or conspiracy with competitors.

3.3 Video monitoring

One form of control that many organisations use is video monitoring. Video monitoring is a method for deterring theft, maintaining security and monitoring employees. Employers also sometimes use cameras to monitor employee productivity and prevent internal theft.

3.4 Firewalls

Internet privacy can be described as the mandate of personal privacy concerning transactions or transmission of information over the internet. The potential for invasion of privacy over the internet is high, as internet users face the risk of having their privacy invaded by, for an example, advertisers using e-mail adverting. There is also the risk that outside users will gain access to the organisation's resources. In order to avoid this, organisations can install a 'firewall' to protect their private networks from external invasion.

4 ETHICAL ISSUES

When privacy is discussed, a strong emphasis is placed on its importance in terms of the control of information. Information privacy deals mainly with access to information; however, the manner in which people treat information or what they do with it may call their ethical behaviour into question. Ethical reasoning, contrary to professional practice, is something that cannot be learnt, as it involves doing what is right, based on a set of

moral principles. In every situation the question of what is the right thing to do should always be asked.

Individuals are not the only ones facing ethical issues. Organisations are also affected, especially in terms of their information.

4.1 Ethics and the individual

In an information environment, the individual may act unethically for various reasons. These may include self-interest or familiarity with organisation information, or because of intimidation by a dominant senior staff member trying to influence the decision-making process.

As mentioned earlier, ethical behaviour cannot be taught, as it is not based on rules and regulations. Although an action might be legal, it might not necessarily be ethical. The test for ethical behaviour is to ask oneself the question: 'What is the right thing to do in this situation?'

By using work e-mail for personal communication or by accessing social network sites during work hours, you are using the resources of the organisation. Ensure that you use it in accordance with organisation policy and in an ethical manner.

4.2 Ethics and information

Information ethics examines the ethical issues arising from the development and application of information technologies. It is clear from this kind of study how individuals and organisations feel about moral issues concerning, for example, privacy, access, ownership, protection and copyright of information.

The following principles relate to the ethical treatment of information. (Coetzee & Plant 2010:23–25):

- Integrity

  Information should be communicated with honesty and integrity, this means that it should neither be falsified nor presented in a misleading matter.

- Objectivity

  The highest possible level of objectivity should be exhibited when information is collected, analysed and communicated to the intended parties. Information should be handled fairly, without prejudice or undue influence of self-interest or bias.

- Confidentiality

  As discussed under privacy, information should be respected and not disclosed unless there is a professional or legal reason to do so.

- Professionalism

  Information should be handled in a professional manner.

4.3 Ethics and the organisation

The organisation should always strive to behave ethically. As ethics is not governed by rules, it is rather hard to enforce ethical behaviour in an organisation. A good starting point would be to set an ethical tone in the organisation. This can be achieved by management and staff together drawing up a code of conduct. A code of conduct includes an organisation's values and its responsibilities towards all stakeholders. Various descriptions of codes of conduct can be found in literature, but let us have a look

at how the International Federation of Accountants (IFAC) defines a code of conduct. The IFAC (2007) defines a code of conduct as follows (IFAC. 2007:5): ''Principles, values, standards, or rules of behaviour that guide the decisions, procedures and system of an organisation in a way that contributes to the welfare of its key stakeholders, and respects the rights of all constituents affected by its operations.''

Another way of fostering an ethical corporate culture within the organisation is by means of corporate governance. You have already been introduced to the King III report in study unit 11. The focus of this document is to provide organisations with guidelines on how to ensure sound corporate governance. Corporate governance can be broadly defined as the system that controls and directs organisations in formulating a strategy for preventing the misuse of assets against an ethical backdrop. Directors, managers and other employees need to keep in mind that they are merely the custodians of organisational resources and are accountable to the shareholders.

You will learn more about corporate governance in your Auditing modules

5 SUMMARY

This study unit examined two important issues; privacy and ethical matters in a computerised information system environment with reference to the individual and the organisation. Ways to ensure privacy and ethical behaviour were also suggested.

The next topic (Topic 7) explains the process of information system development.

Self-assessment

a. Explain the concept of *ethical behaviour*.

b. Match the concepts in column A with the definitions/explanations relating to ethical principles in column B:

Column A	Column B
Objectivity	Information should be handled in a professional manner.
Professionalism	The highest possible level of objectivity should be exhibited when collecting, analysing and communicating information to the intended parties. Information should be handled fairly without prejudice, or the undue influence of self-interest or bias.
Integrity	Information should be respected and not disclosed unless there is a professional or legal reason to do so.
Confidentiality	Information should be communicated with honesty and integrity; this means that it should not be falsified nor presented in a misleading matter.

c. Define a code of conduct.

d. Explain the term *computer monitoring*.

e. The following scenarios relate to a small accounting firm XYZ. State whether the following should be categorised as ethical or unethical behaviour, as well as the ethical principle(s) that applies/apply. If disclosed as unethical behaviour, state the reason for doing so and the applicable principle(s).

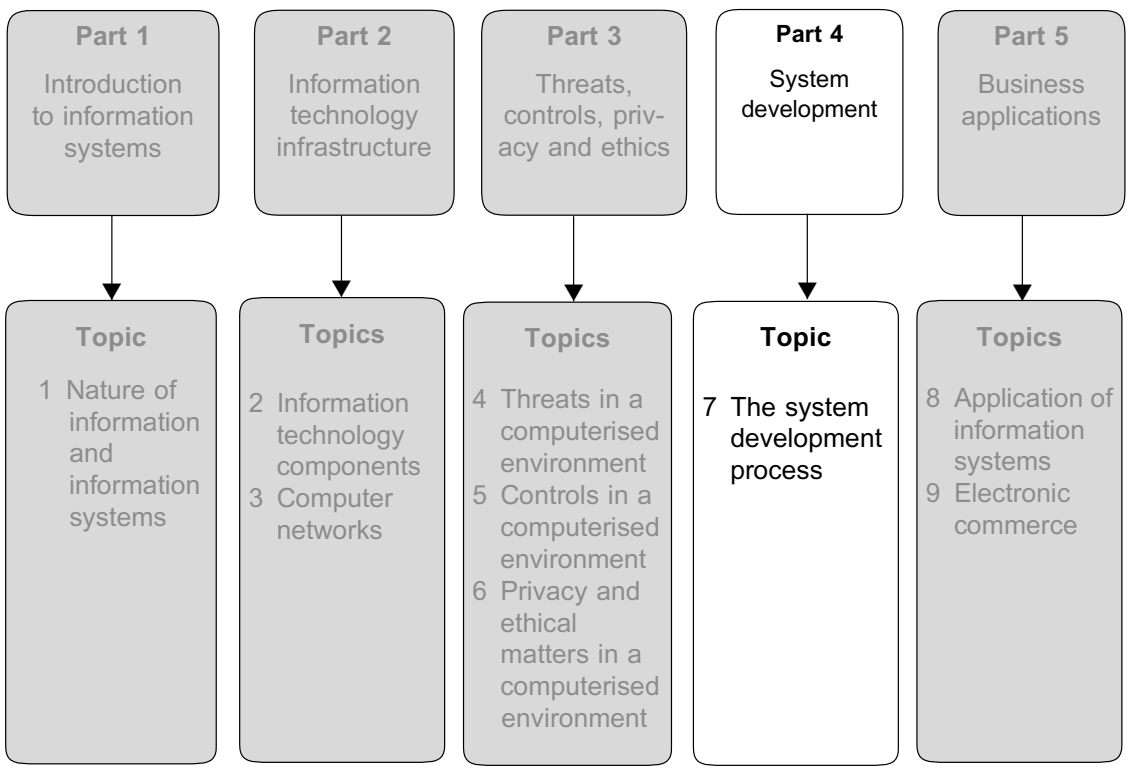
- Mr Mawethu, one of the firm's accountants, has claimed more hours for overtime than he is entitled to.
- Mrs Clarkson, the firm's payroll clerk, signs all claims that have the correct signatures and supporting documents.
- The firm's debtor clerk, Ms Abram, often discloses the firm's financial information to friends and family.
- The firm's chief accountant, Mr Cole, received a cheque of R10 000 as a gift when doing the books of one of the firm's clients.

SYSTEM DEVELOPMENT

PURPOSE

The purpose of part 4 is to equip you with knowledge of system design, system development and the implementation of information systems. You will also be exposed to the maintenance, review and performance measurement of an information system.

Part 4, Topic 7 The system development process



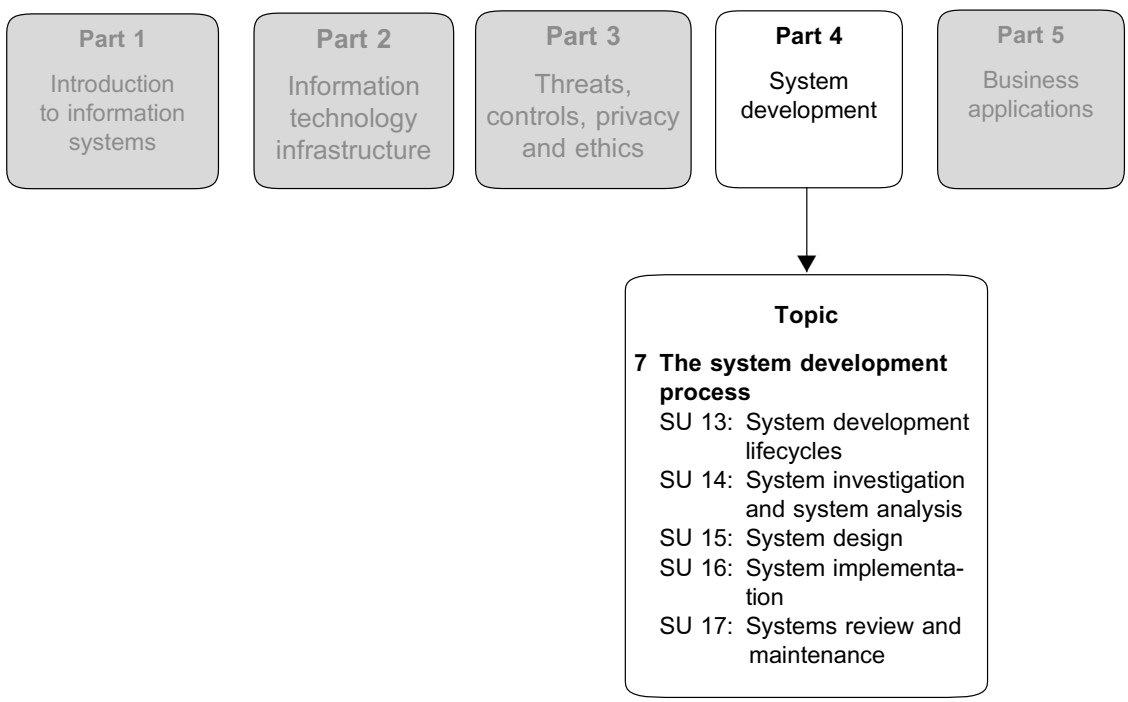
The system development process

LEARNING OUTCOMES

After studying this topic, you should be able to

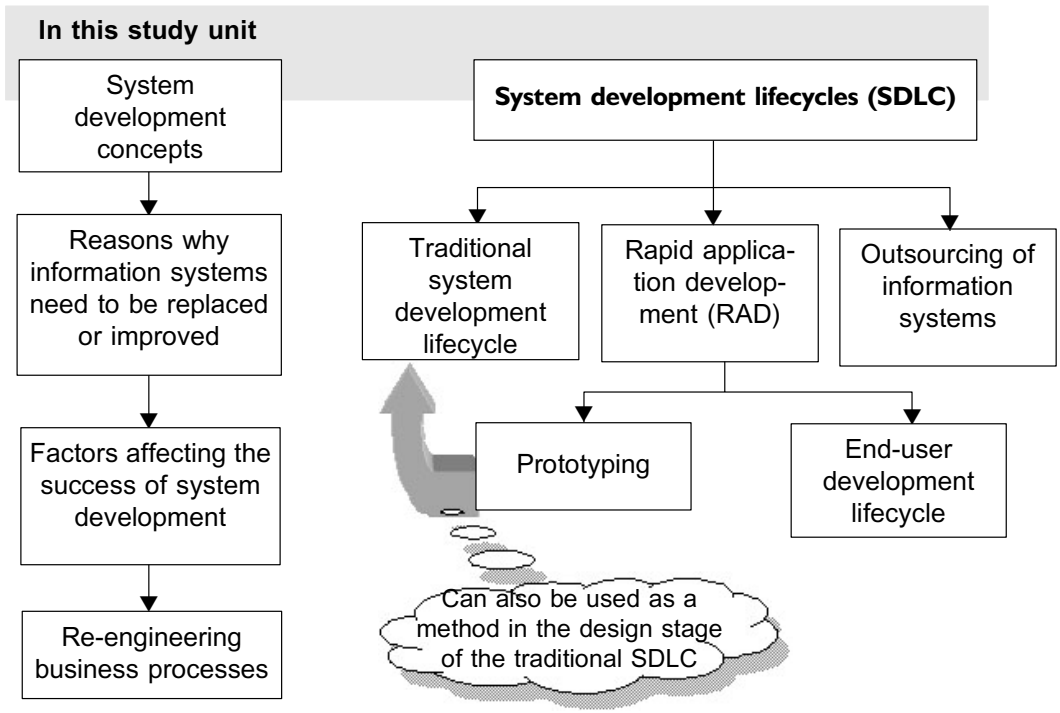
- define system development and describe the system development lifecycle
- describe factors affecting the success of system development
- describe the system investigation process
- describe the system analysis process
- identify and describe various techniques for evaluating existing system
- describe the system design process and the factors that have to be considered
- define the system implementation process and describe the steps to follow when implementing a system
- define the system review process and describe the different phases of the review process and the factors to consider during system review
- define the system maintenance process and describe the reasons for system maintenance
- differentiate between various types of maintenance and define system maintenance documentation and the maintenance team

This topic consists of five study units.



STUDY UNIT 13

System development lifecycles



1 INTRODUCTION

An information system that used state-of-the-art technology ten years ago would now most likely be regarded as outdated. Many reasons can be given for this, but the most important is probably the rapidly changing technological environment and the changing output needs of information systems. The business environment has become far more interconnected and globalised and information technology that satisfies this need has to be adopted.

System development initiatives arise from all levels of an organisation and are both planned and unplanned. Managers and employees are all users of information systems and are therefore part of the development process. Solid planning and managerial involvement help to ensure that system development initiatives support the broader organisational goals.

This study unit (study unit 13) deals with the development of an information system and different development lifecycles. The advantages and disadvantages of the different development approaches are discussed in detail.

2 WHAT IS INFORMATION SYSTEM DEVELOPMENT?

Information system development is the process of ***creating*** a ***new information system*** or ***modifying*** a ***current*** information ***system***. By employing ***information technology*** to ***develop a system***, problems or opportunities are transformed into solutions.

3 REASONS WHY AN INFORMATION SYSTEM NEED TO BE REPLACED OR IMPROVED

We have already said that all business systems should be open systems and these are constantly influenced by changes in the environment.

Typical changes include the following:

- *Changes in technology:* New technology can lead to new production processes or communication methods by using new and better equipment, which will affect the information system.
- *Changes in decision-making policies:* For example, decisions to centralise decision-making and information systems, or to decentralise decision-making and information systems, will lead to a need to replace, change, or improve the existing information systems.
- *Changes in the needs and demands of users and stakeholders*: To improve decision-making, the needs of the different users of information change continually.
- *Changes in the business environment:* Organisations need to stay competitive in an environment where the impact of an increasingly global market is enormous.
- *Changes in the nature of the organisation:* Changes in the activities of the organisation; for example more production lines or changes in production lines. This may also occur when two organisations merge.
- *Changes to maintain a competitive advantage:* A constant flow of new ideas and changes are necessary to stay ahead of the competition.
- *Changes to improve performance and productivity:* Re-design of business processes and the information system in order to improve the performance and productivity of the organisation.
- Depending on the impact of the change on the current system, a total redesign might be required (this will be covered in study unit 14–16), or modifications may be made as part of system maintenance (covered in study unit 17).

4 FACTORS AFFECTING THE SUCCESS OF SYSTEM DEVELOPMENT

System development can be considered successful if the system meets the needs of the users and the organisation on time and within budget. System development leaders have identified the following factors that can contribute to successful system development efforts at a reasonable cost:

- *The extent of changes in the system*: System development can mean slight adjustments to the existing system or it can result in the development of a completely new system.
- *The involvement of users and stakeholders:* It is essential to involve all users and stakeholders in the system development process, as this will ensure that the developers look at all issues and problems and that the users are more likely to accept the new software and the changes it involves. It is also essential for top management to buy into the development process in order for it to succeed. It is based on a

partnership between the end-user and the information system specialist. End-users are involved in designing applications. Organisations should be aware of the possible inexperience of their end-users and the impact of this on the success of system development.

- *The planning of the project:* It is essential to plan a development project properly. Poor planning will lead to problems like falling behind schedule or going over budget.
- *The selection of the developers used to develop the new system:* The previous experience of the organisation and the developers will play a major role in the success of system development.
- *The use of project management tools*: All tasks need to be determined in detail, including the use of personal and other resources and due dates for each task. A schedule should be drawn up including the details of the tasks, the due dates and the person responsible for helping management keep track of the process and keeping people accountable.
- *Change management achieved by the new system*: Some people do not find it easy to change the way they do things. As a new system will result in changes to such people's routines, management's ability to manage the change is critical to the success of a new system.

5 RE-ENGINEERING BUSINESS PROCESSES

Re-engineering involves drastically ***rethinking*** and ***redesigning business processes***, ***business structures*** and ***information systems*** to achieve a ***break-through*** in ***business results*** and to improve performance. Hall (2011:177) explains re-engineering as the identification and elimination of non-value-added tasks by replacing traditional procedures with those that are innovative and different.

Re-engineering usually takes place before a new system is developed, or it takes place in the initial phases of system development.

6 SYSTEM DEVELOPMENT LIFECYCLES

There are various approaches to the development of a new information system. This will be discussed in paragraphs 6.1 to 6.4.

6.1 Traditional system development lifecycle (SDLC)

The development of an information system and meeting the needs of the business are complex, difficult and expensive endeavours.

The *system development lifecycle* is a ***practical*** framework, which provides a ***broad*** context for the ***development*** stages of an information system (Boczko 2007:830).

To *overcome* the *complexity* of a *system development project* and to *improve* the *results*, the process can be *divided into several steps*. Setting a *goal and the tasks* for *each step* will ensure the development of an effective and productive system.

An overview of a traditional SDLC:

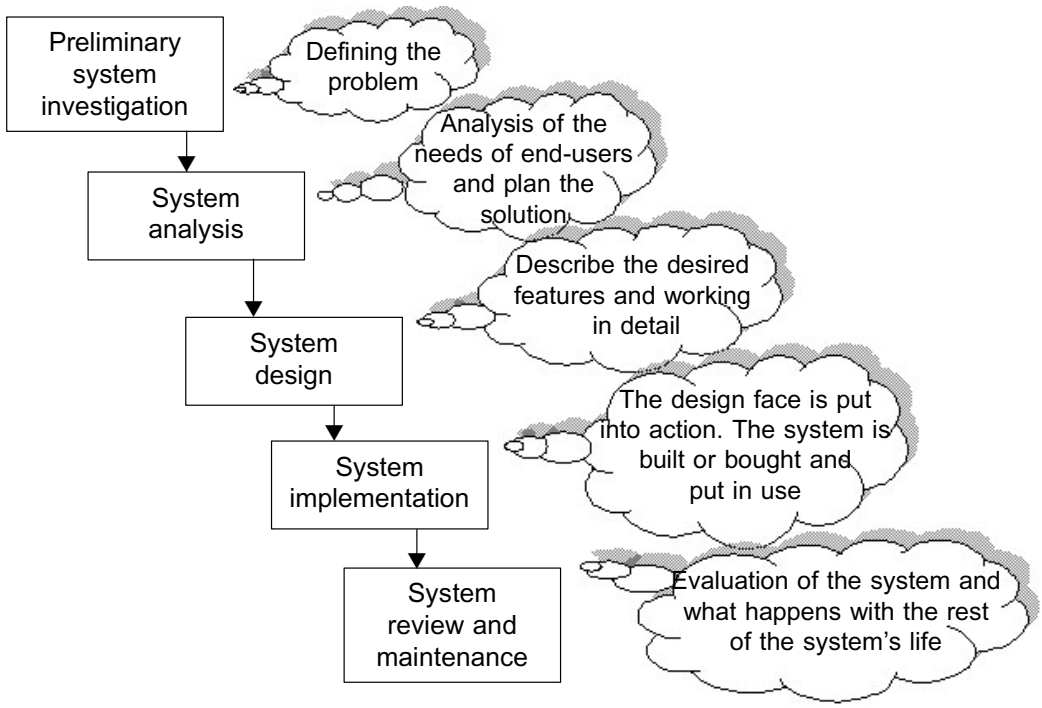


FIGURE 13.1: Overview of a traditional SDLC

These steps are discussed in detail in study units 14 to 17.

Using the SDLC approach has some advantages and disadvantages for an organisation that need to be considered and kept in mind.

Advantages and disadvantages of the SDLC

Advantages	Disadvantages
Less experienced staff can be used owing to the detailed guidelines and clearly defined stages.	Users cannot easily evaluate products to see if their needs are being met and their needs are often misunderstood because they are usually only involved in the planning stage.
Easy to manage. Control over the project is effective owing to revision at the end of each phase.	A stage cannot start before finishing the previous stage.
It ensures good documentation during all phases, simplifies maintenance and makes it possible to track system requirements back to the organisation's needs.	Creation of documentation is expensive and time consuming and it is difficult to keep documentation current.
Consistency among all projects, which can reduce cost. Personnel can be transferred from one project to another.	Going back two or more phases is very expensive.
Progress can be measured and controlled.	It is difficult to measure the progress within the stages.

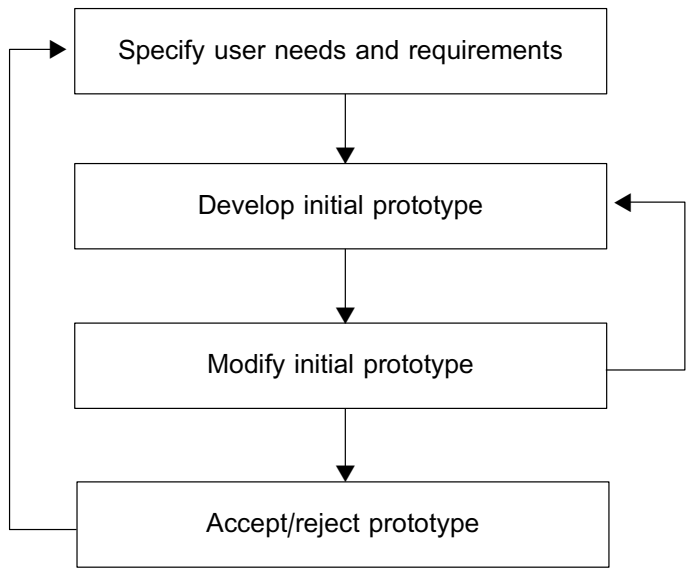
6.2 Prototyping

The development of new software is very expensive.

> One way ***to cut this cost*** is to ***build a scaled-down experimental*** version of the new information system ***(Prototyping).*** Prototyping, also known as evolutionary lifecycle, means the end-users can identify what they do not want as opposed to what they do want (Boczko 2007:875). The feedback of end-users can be used to improve the initial system throughout the process until the system is finally complete.

Note: Prototyping can also be used as an implementation method in the design stage of the traditional SDLC.

An overview of prototyping:



Source: Boczko (2007:875)

FIGURE 13.2: Overview of a traditional SDLC

Like the SDLC, prototyping has some *advantages* and *disadvantages* that need to be considered and kept in mind.

Advantages and disadvantages of prototyping:

Advantages	Disadvantages
Prototyping leads to a better understanding of the user requirements.	It is difficult to contain the extent of the prototype and the project never seems to end.
Users can use the prototype system during the development process and they can provide useful feedback.	
It is more flexible than the final system and users' thoughts are stimulated and new ideas can be tested.	Each iteration builds on the previous one and the final system might only be incrementally better than the initial system.

Advantages	Disadvantages
Development is faster and a prototype system can be produced in a short time.	System backup and recovery, security issues and performance can easily be disregarded.
Users might be able to use the new system without formal training as they have already used the prototype system to test it.	
Users are involved in the evaluation process and, as solutions emerge, they become more positive about the process and the results.	The focus is on development of the prototype and therefore system documentation is often partial or absent.
Prototyping allows for early testing, hence errors are detected early in the process.	

6.3 Rapid application development (RAD)

Rapid application development is a system development approach where ***workshops and focus groups*** *gather the requirements* of the new system from the ***end-users***. This method speeds up development. RAD makes the adapting of changes to system requirements easier and reduces paper-based documentation. User participation is facilitated and source code is automatically generated.

There are various advantages and disadvantages of RAD that need to be considered during the development process.

Advantages and disadvantages of RAD:

Advantages	Disadvantages
Time to deliver is less	Management complexity is increased
Changing requirements can be accommodated	Resource requirements may be increased
Progress can be measured	Suitable for a system that are component based and scalable
Cycle time can be short with use of powerful RAD tools	Suitable only when requirements are well known
Productivity with fewer people in a shorter period	Requires user involvement throughout the life cycle
Use of tools and frameworks	Suitable for projects requiring shorter development times

Source: Software Methodologies 2009

6.4 End-user development lifecycle

End-user development is a process where end-users ***develop their own*** applications, using ***existing application software***, to ***solve*** their information needs.

Advantages and disadvantages of end-user development:

Advantages	Disadvantages
Encourages innovation and creative solutions	Loss of control over data
Faster design/implementation cycle	The new system is not adequately tested for errors
Makes users more involved in the reviewing and maintenance of the system	Duplication of effort and waste of resources
Leads to better productivity of users' work	Poor documentation created
Reduces communication problems between users and the information system and they will understand the system better.	Users are not trained as programmers
It will be more acceptable to users and they will take ownership of the system.	Loss of control of quality in both programs and data

7 OUTSOURCING THE INFORMATION SYSTEM

Outsourcing the information system means ***obtaining some or all activities of the information system from an external service provider*** to ***handle*** all or parts of the ***data capturing and processing*** at a *predetermined annual rate*, rather than developing the organisation's information system internally.

Boczko (2007:888) identifies three outsourcing models:

On-site outsourcing: This is when the service provider provides the resources or facilities at the organisation itself.

Off-site outsourcing: This is when the service provider provides the service at a location other than at the organisation itself.

Blended outsourcing: This refers to a combination of on-site and off-site outsourcing.

The following *advantages and disadvantages* are attached to outsourcing:

Advantages	Disadvantages
Outsourcing allows organisations to concentrate on their core business and leaves the management of the information system to the service provider.	Organisations may be unwilling to outsource the entire process owing to confidentiality issues.
Outsourcing offers the client the advantage of using the latest technology.	Service providers may fail to satisfy the needs of the organisation or may deliver poor service.
Outsourcing reduces cost. It might mean substantial savings using economies of scale (savings, making use of mass production).	Long contracts can result in organisations being locked in to a contract, making it almost impossible to break the contract.
Outsourcing insulates organisations from uncertainty about the levels of service they can expect.	

Advantages	Disadvantages
Bidding on an annual basis will reduce cost even more.	Organisations may also feel that they lose control over an information system.
Outsourcing increases effectiveness because the supplier deploys higher-level expertise that improves productivity.	
Outsourcing can deliver benefits and change more quickly than in-house processes.	Organisations may have a problem finding service providers that can manage difficult processes.
Outsourcing unforeseen fluctuations of transaction processing is easier than planning and regulating them in-house.	

Activity 13.1

ICC Ltd's information technology manager has realised that the organisation's current information system no longer meets the organisation's needs. He therefore informs the executive management committee accordingly at one of their meetings.

Management asks him to compile a report on the various options they could consider to solve this problem. He subsequently asks you to help him to compile this report.

Required:

Write a report on this issue to be presented to the executive management committee.

Feedback

There are various approaches to the development of a new information system as discussed in paragraph 6.1 to 6.4.

In your report explain each of them briefly and consider their advantages and disadvantages.

It would also be a good idea to discuss the reasons for replacing the information system and the factors that might affect the success of the development of the new system.

---

8 SUMMARY

Organisations that use an information system that do not meet all users' requirements have a definite competitive disadvantage in the market. Therefore, organisations need to adapt their information system constantly, using the latest technology, upgrading the existing system, or acquiring a new system. The SDLC will lead them through this process. One of the advantages of using an SDLC model is that a project can be managed properly. It is therefore possible to ensure that the organisation makes the necessary progress. However, SDLC models do not guarantee that each step is

completed successfully before the next one is started. If one of the steps were neglected, it will have a negative effect on the next step and the final result.

The next four study units (study units 14–17) deal with the different stages of the SDLC in detail.

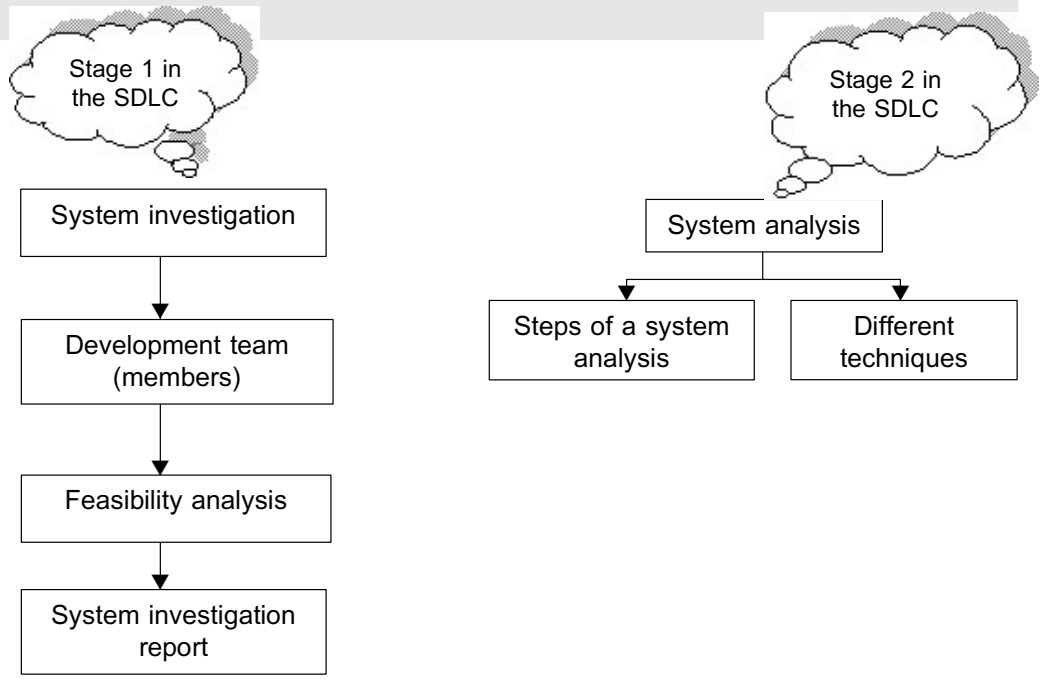
Self-assessment

a. Explain the term ‘‘system development’’.
b. Name and give seven reasons why a system need to be replaced.
c. Name and describe six factors that affect the success of system development.
d. Define the concept of re-engineering of business processes.
e. Using a diagram, explain the different stages in the traditional lifecycle of an information system development project.
f. Give four advantages and four disadvantages of the traditional SDLC.
g. Explain the term *prototyping*.
h. Give four advantages and four disadvantages of prototyping.
i. Explain the term ‘‘rapid application development’’ (RAD).
j. Give four advantages and four disadvantages of RAD.
k. Explain the term ‘‘end-user development’’.
l. Give six disadvantages of end-user development.
m. Describe outsourcing?
n. Give five ideal circumstances for the use of outsourcing.
o. Name and describe three outsourcing models.
p. Give five advantages and five disadvantages of outsourcing.

STUDY UNIT 14

System investigation and system analysis

In this study unit



1 INTRODUCTION

In the previous study unit, we explained system development and the system development lifecycle. During this study unit, we investigate the first two steps of the system development lifecycle. System investigation will identify the problem and system analysis will determine how to solve the identified problem. The steps to follow during the investigation and the analysis processes are described below.

2 SYSTEM INVESTIGATION

System investigation is the first phase in the system development lifecycle of a new or modified business information system.

During the *system investigation* phase, the ***needs*** of the organisation should be ***investigated*** and the ***potential problems*** and ***opportunities*** need to be ***recognised*** and considered in the light of the ***objectives*** of the company and its information strategy.

For the development of a new information system to be successful, the problem and the requirements of the end-user have to be thoroughly understood.

According to Stair et al (2008:408), system investigation attempts to uncover answers to the following questions:

- What main problems might a new or improved system solve?
- What opportunities might a new or improved system provide?
- What new hardware, software, databases, or procedures will improve an existing system?
- What are the potential costs?
- What are the related risks?

2.1 Development team

Once a decision has been made to initiate a system investigation, the first step is to determine which *members of the development team* should participate in the investigation phase of the project. Ideally, the following members should be included:

- a project manager
- upper-level managers
- middle level managers
- information system staff
- end-users
- other stakeholders

The *responsibilities* of a *development team,* who participate in the investigation, are the following:

- Gathering and analysing data
- Identifying shortcomings by evaluating the system against the goals of the organisation
- Writing a report justifying the system development and presenting it to management

2.2 Feasibility analysis

According to Baldauf and Stair (2011:529), a key part of the system investigation is a feasibility analysis. These authors refer to the following types of feasibility:

Type	Description
Technical feasibility	Determines whether the hardware, software and other system components can be acquired or developed.
Economic feasibility	Decides whether the project is a financially sensible investment.
Legal feasibility	Determines whether there are laws that prevent or limit the project.
Operational feasibility	Measures whether a project has the ability to be put into action.
Schedule feasibility	Determines whether a project can be completed within a reasonable time.

2.3 System investigation report

The primary outcome of system investigation is a *system investigation report*, which summarises the results of the investigation and the outcome of the feasibility analysis.

The report also includes recommendations; these can be to

- continue with the development of a new system, or
- modify the existing system in some way, or
- not change the existing system.

After the system investigation report is complete, it is reviewed by senior management, often in the form of a committee, consisting of senior management, users from the information system department and users from other useful areas. Subsequently a final decision is made.

3 SYSTEM ANALYSIS

A *system analysis* determines ***what*** to do to ***solve*** the identified ***problem***. It starts by ***clarifying*** the overall goals of the organisation and ***determining*** how the existing or proposed information system helps meet these goals.

The analysis of a small organisation's information system can be straightforward. On the other hand, evaluating an existing information system for a large organisation can be a long, tedious process.

3.1 The steps involved in a system analysis

When analysing a major information system, large organisations usually follow a formalised analysis process involving the following steps:

- *Set up a committee or team to do the system analysis:* The first step in the system analysis is to set up a team or committee to revise the existing system. This committee should consist of members of the development team, users, stakeholders, information system staff and management.

  Tools: Formal planning includes drawing up a list of objectives and activities needed to meet the objectives with due dates and a list of the resources required for each activity. Dates scheduled for committee meetings should be included.

- *Collect data and understand the requirements*: Collect more information about the needs and problems identified during the system investigation. During this process, the investigation team identifies the strengths and weaknesses of the existing system.

  Tools: A variety of methods can be used to gather more information, including interviews, observations, questionnaires and sampling.

- *Investigate the collected data:* The next step is to process the data into useful information. The overall purpose of the analysis is to determine user, stakeholder and organisational needs. The techniques used to do this include *asking directly*, *using critical success factors*, *specifying screen* and *report layout* and *using requirement analysis tools*.

  Tools: To illustrate the relationships between the different objects, associations and activities the following tools can be used: application flowcharts, grid charts, and computer-aided software engineering (CASE) tools.

- *Preparing a report on the existing system, new system requirements and project*

priorities, after the system analysis is concluded: A system analysis report is a formal report in which the conclusions of the system analysis phase are stated (Hall 2011:788).

According to Hall (2011:586), the report should cover the

- reasons for the system analysis
- scope of the study
- problems identified in the current system
- organisational requirements of the new system
- resource implications and economic effects
- explanation of what the newly developed information system should do to solve the problem
- performance criteria in terms of which success can be measured
- boundaries or constraints of the new information system

3.2 Different techniques to gather information on the existing information system

Typically, the analysis will start by looking at the existing system to determine the degree of change needed to solve the problem. According to Eccles, Julyan, Boot and Van Belle (2000:264–267) the following techniques can be used to gather information on the current system:

- *Interviews*. A one-on-one meeting with stakeholders, which is planned in detail to get their perception of the problems, shortcomings and requirements. The interview needs to be documented in detail.
- *Joint application development workshop (JAD).* Communication, understanding and consensus are a major problem when analysing the current system. Highly structured workshops with all stakeholders, focusing on the current system and discussing features of it, will overcome this problem.
- *Questionnaire.* This is not considered as effective as interviews for analysing the system, but can be used to gain an overall impression of users.
- *Observation*. This is often the best way to obtain information or to verify the details gained from the interview or JAD.
- *Document review*. To analyse the system all the latest documents relating to the system have to be gathered, including source documents, input forms, reports and system documents.

Activity 14.1

Black Beauty Tyres (BBT) is one of the largest tyre companies in South Africa with franchises countrywide. Like many other companies, BBT maintains specific performance criteria for its franchises. These include quality of products, levels of customer satisfaction and speed of customer service. Communication between the BBT franchises is essential for maintaining standards across all franchises. To this end, the company provides software to each franchise for accessing the most current information. Franchise managers or owners have access to daily performance records, new products and prices.

However, the top management of BBT has become concerned about some of the managers' complaints about difficulties in keeping up with constantly changing products, services and prices. They also feel they spend too much time monitoring performance using the current software.

These complaints have resulted in top management launching a system investigation. Management found that the current system is very complex and

managers are overwhelmed with too much information. They subsequently decide to introduce a new system to provide the following information faster:

- The latest products and services
- New or changed policies
- Alerts whenever the franchise underperforms in specific areas
- Suggestions to solve the problems identified

System analysts have been pushed for results and have therefore decided to consult head office only in order to meet the deadlines. Top management, on the other hand, is concerned that it will be an expensive project and do not want to spend too much money. It decided to involve only those managers who complained about the current system in the process.

Required:

a. Evaluate the procedure BBT decided to follow in developing a new system. Refer specifically to the factors affecting the success of system development.
b. The system analysts should prepare a report on the existing system, new system requirements and project priorities. Elaborate on the elements they should include in their report.

Feedback

a. Factors affecting the success of system development (see study unit 13)

   If BBT wants the system development process to be successful and to meet the needs of the users and the organisation on time and within budget, system development leaders have to consider the following factors:

   The extent of changes to the current system used by BBT depends on the complaints and outcomes of users and management.

   Some people do not easily change the way they do things. A new system will result in changes to the routine of these people and more specifically those who did not complain about the current system. Ignoring the view of these users might create significant problems.

   It is essential to involve all users and stakeholders in the system development process. This will ensure that the developers look at all issues and problems and that the users are more likely to accept the new software and the changes it involves. In order to succeed it is also essential for top management to buy into the development process. The idea to involve only head office might mean that the managers of the BBT franchises do not buy into the new system.

   BBT should also be aware of the possible inexperience of the end-users in using the new system and the impact this will have on the success of system development.

   It is essential to plan the development project properly. Pressure by BBT's management to provide the results in time might lead to ineffective research and planning. In turn, this poor planning might lead to problems like falling behind schedule or going over the budget.

   System development is an expensive process and BBT's management should keep this in mind. Trying to save money by doing an ineffective analysis of the old system and ineffective development will only result in more cost and failure of the development process.

b. Elements that should be included in the system analysis report are:

- reasons for the system analysis
- scope of the study
- problems identified with the current system
- organisational requirements for the new system
- resource implications and economic effects
- explanation of what the new information system should do to solve the problem
- performance criteria on which the success can be measured
- boundaries of, or constraints on the new information system

---

4 SUMMARY

During the system investigation stage, problems are identified and the system analysis determines the possible methods to solve these problems. After each stage, a report containing all relevant information should be produced. Appropriate and effective planning during the investigation and analysis stages will result in a well-organised and smooth design process.

The next study unit (study unit 15) will cover the third stage of the system development lifecycle, namely system design.

Self-assessment

a. Name and describe the key steps of the system investigation phase.

b. Briefly explain the system investigation report and its contents.

c. Name and describe the steps of a system analysis with specific reference to the tools used in each step.

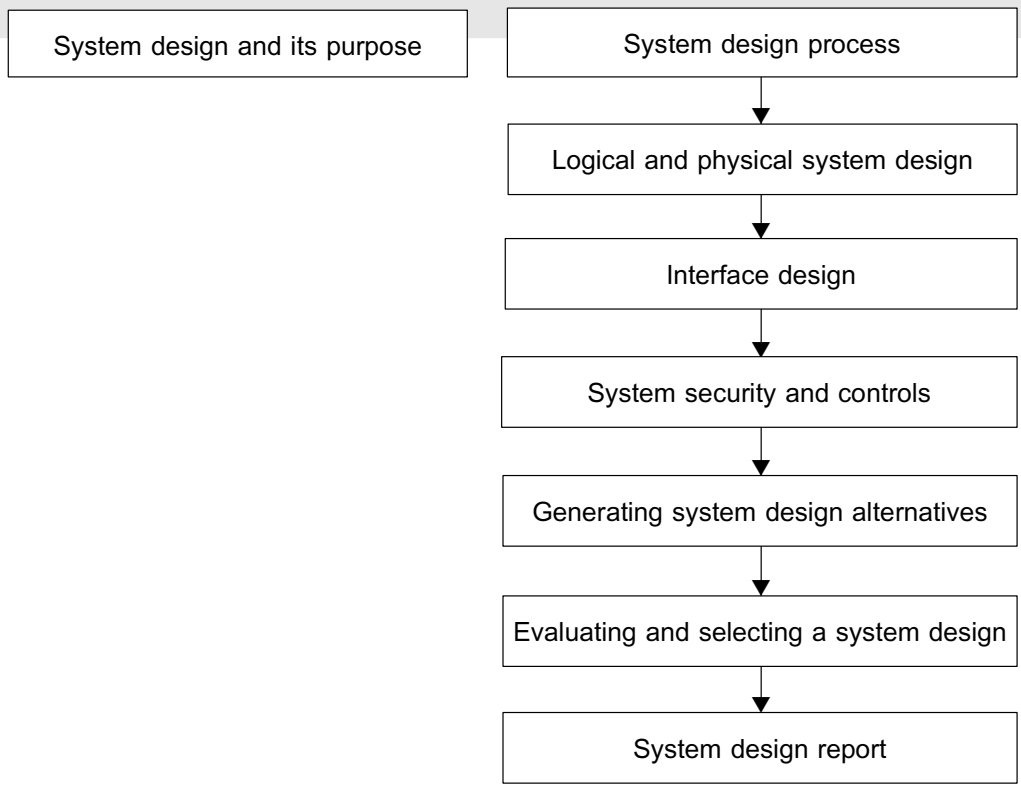
d. Name six elements that should be covered in a formal system analysis report.

e. Name and describe three different techniques for evaluating an existing information system of an organisation in order to develop a new system.

STUDY UNIT 15

System design

In this study unit



1 INTRODUCTION

In the previous study unit, we dealt with the system investigation process and its analysis in order to identify problems. In this study unit, we will describe how the resultant analysis can be used to design a solution. This design stage concerns the technical design. According to Hall (2011:788), system design concentrates on the analysts' viewpoint of information needs rather than the view of accountants and other users. The new system should overcome the shortcomings of the existing one and help the organisation achieve its goals.

2 SYSTEM DESIGN AND ITS PURPOSE

System design is the stage of system development in which a ***solution*** to a *problem* is ***planned*** and ***documented***. The system design stage *uses* the ***information*** from the ***investigation*** and analysis of the ***current*** methods and ***identifies methods*** that might ***achieve better results***. The question "How will the

new information system solve the problem?" needs to be answered during this stage. System design generally comprises two major components: logical design and physical design.

3 THE SYSTEM DESIGN PROCESS

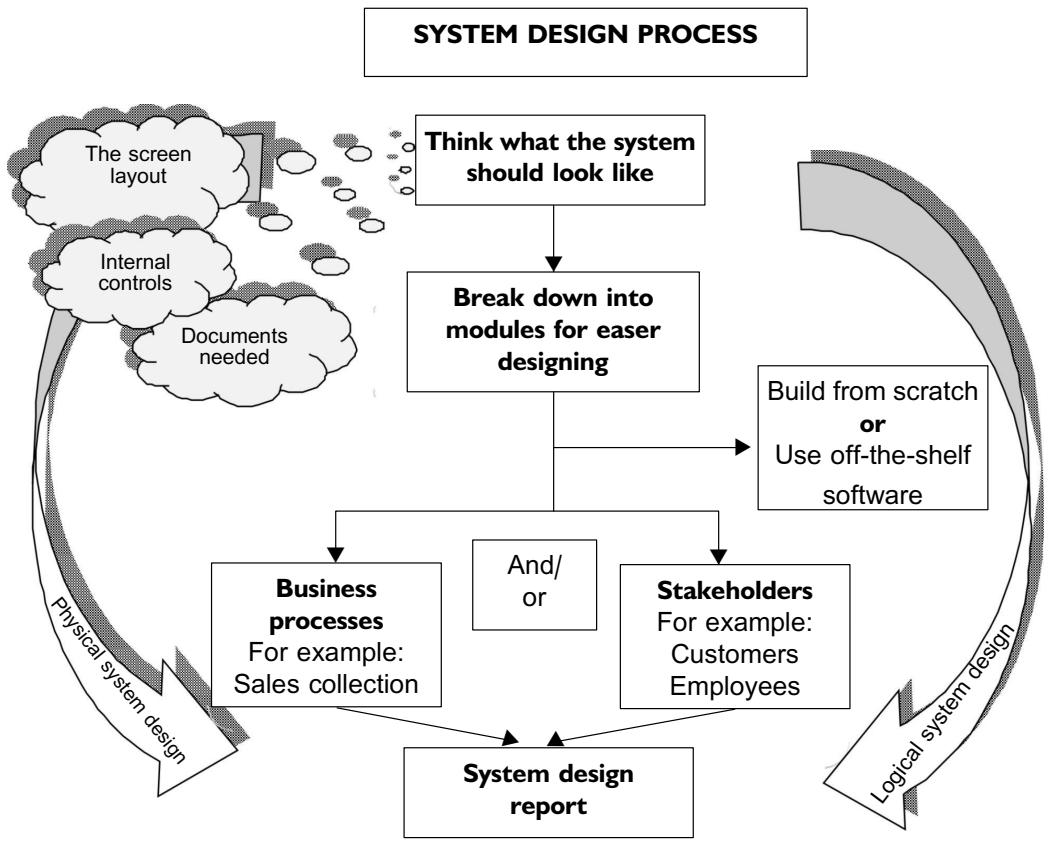


FIGURE 15.1: System design process

During this process, the two key aspects of system design are the logical and physical system design. Using the information gleaned from the previous two stages, the designers can start to think about what the new system should look like. For example, the interface design or screen layout, as well as the security, controls and the documents involved all need to be considered.

Designers will often break down the design process into smaller units to make the process easier. These units could be based on the business processes or stakeholders.

This is where designers also need to decide whether to build a new system from scratch or to consider some off-the-shelf software. Accordingly, the alternatives need to be generated and then evaluated and the advantages and disadvantages need to be considered. This will be discussed in detail in the next study unit (study unit 16).

Lastly, the final decisions should be written up in a report called the design report.

3.1 Logical and physical system design

There are two key aspects of system design:

Logical design: Logical design entails a ***theoretical design*** of the ***structure of the new system***. It describes the ***practical requirements*** of a system and ***conceptualises*** what the system will do *to* ***solve the problems*** that have been identified by earlier analysis. System design makes a huge contribution to the understanding of technical details and ensures that the technical details of the system do not obscure the best solution.

According to Stair and Reynolds (2008:527), the logical design specifications that are determined and documented include the

- output design
- input design
- process design
- file and database design
- procedure design
- telecommunication design
- controls and security design
- staff and job requirements

Physical design: During physical design, ***the broad, user-oriented requirements*** of the logical design are translated into ***detailed specifications*** which are ***used to code and test the computer programs*** (Romney & Steinbart 2009:684). In other words, *physical design specifies the characteristics* of the *system components necessary* to put the logical design into action.

According to Stair and Reynolds (2008:427), in this phase the characteristics of each of the following components must be specified:

- Hardware
- Software
- Database
- Staff
- Telecommunication
- Procedure and control specifications

3.2 Interface design

During interface design, some matters to take into consideration include deciding whether it should be a menu-driven or command-line interface. *Menu-driven system* means that users can simply click or select what they want to do from a list of commands. In a *command-line system* users have to type the command (what they want to do) into the computer.

3.3 System security and controls

The best time to deal with possible errors in a new system is early in the design phase. Dealing with problems at that time will be the most cost-effective for the organisation.

This step in the design process entails the review, modifying and evaluating of the system controls. Security and controls attempt to prevent problems and illegal activities before they occur. Policies and procedures need to be in place to reduce risks, which may undermine the information system.

Most information system departments establish tight system controls to maintain data security.

System controls can help stop computer abuse and computer crime by employees and others. It is vital to deal with these issues during the design phase to ensure that effective security for the new system is in place.

3.4 Generating system design alternatives

Different designs need to be put on the table to ensure an informed decision. When people or organisations require whole systems or a system to perform additional functions that an existing system cannot support, they often turn to outside vendors to design and supply their new system.

Request for proposal (RFP). If new hardware and software are required, a formal request for proposal can be sent to service providers. An RFP is a document that defines the details of the required resources such as hardware and software.

3.5 Evaluating and selecting a system design

The last step in the system design process is evaluating the various alternatives and selecting the one that offers the best solution in terms of the organisational goals. This step usually involves both an initial and a final evaluation of alternatives before the final design can be selected.

An *initial evaluation* eliminates the unwanted proposals and it is done after all the proposals have been submitted.

The *final evaluation* entails a detailed investigation of the proposals remaining after the preliminary evaluation. The final review process is usually done using preset criteria and a scoring point system.

The purchase of a system requires knowledge of both hardware and software. Organisations can obtain a system from one or more vendors (sellers or traders).

The following factors should be considered when selecting a service provider:
(Apply selection criteria as discussed in Topic 3)

- The availability of training for the clients' staff by the service provider
- Possible evaluation of the service provider done by an independent organisation
- Service provider's ability to repair hardware
- Products (goods and services) offered to clients
- Quality of the after-sales service offered by the vendor
- Reliability and financial stability of the service provider
- Timeframe to implement the system
- Service provider's ability to modify its software if required
- Financing for each option (This is discussed in the next paragraph)

3.6 Financial options

There are several financial options available for acquiring a computer system, including purchase, lease, or rent. Cost objectives and constraints set for the system play a significant role in the choice, as do the advantages and disadvantages of each option, demonstrated in the table on page 135:

Rental (short-term)	
Advantages	**Disadvantages**
No initial capital outlay	Most expensive form of finance
Payments are predictable	High monthly costs
No long-term commitment liability	No ownership
Rent payments are tax deductible	Link with vendors limits freedom and independence
Maintenance for the account of the vendor	May have to rely on maintenance
Leasing (longer-term)	
Advantages	**Disadvantages**
No initial capital outlay	Poor flexibility of upgrading
More flexible than purchasing	Longer commitment than renting
No long-term financial investment	May have to rely on maintenance
Less expensive than renting	Ownership remains with lessor
Tax benefits usually passed on by lessor	High cost of cancelling lease agreement
Purchasing	
Advantages	**Disadvantages**
Cheap form of financing	Highest initial capital outlay
Depreciation is tax deductible	Maintenance for own account or separate agreement
Total control over equipment	Other expenses including insurance
Can sell equipment at any time	May prevent investment in more profitable projects
Asset reflects on statements	

Source: Eccles et al (2000:326)

You will learn more about evaluating and selecting a suitable financing option in later modules teaching the application of financial management techniques.

Activity 15.1

Activity: (Black Beauty Tyres (BBT) continued)

Read the case study of Black Beauty Tyres in the previous study unit again and complete the following activity.

Required:

a. Name the finance options that BBT should consider for the new computer system and discuss the advantages and disadvantages of these finance options.

b. Discuss the factors BBT should consider when selecting a service provider.

Feedback

It is important to refer to the advantages and disadvantages as well as the other factors discussed in the text, but use the scenario to make your answer more applicable to BBT.

3.7 System design report

The results and conclusions of the system design process are included in a report, known as the system design report.

The system design report can be drafted in two stages:

a. Logical system design report:

This report is needed to guide the activities of the physical design and explain how the information needs will be met. It contains:

- an executive summary of the system design, including:
  - a review of the requirement analysis
  - a summary of all information needs, activities and decisions taken in this regard
  - criteria identified during the analysis phase that can be used to evaluate system performance
  - a detailed diagram of the planned system and the flow of information to meet the requirements

b. Physical system design report:

This reports on what has been accomplished and is vital to allow management to decide whether to continue with implementation. It should include at least

- hardware requirements
- software requirements
- database design
- communication design
- personnel requirements
- training requirements
- controls and security
- maintenance procedures
- building proposals

4 SUMMARY

The information system design process will affect the daily functioning of the organisation. Like all the other stages, the design stage strives to achieve organisational goals. The main goal of this phase, however, is to design a new or modified system to deliver the required information at the right time to the right person at the right price.

In the next study unit (study unit 16), the development of the new information system is taken one step further; the newly developed system needs to be put into use. The implementation of a new system is discussed in the following section.

Self-assessment

a. Explain the term *system design* and the purpose of this stage in the system development process.

b. Distinguish between logical design and physical design.

c. Give eight logical design specifications and six physical design specifications.

d. Explain what is meant by a *request for proposal (RFP).*

e. There are several *financial options* available for acquiring a computer system, including purchase, lease, or rent. Cost objectives and constraints set for the system play a significant role in the choice, as do the advantages and disadvantages of each option.

f. Give the advantages and disadvantages of rental.

g. Give the advantages and disadvantages of leasing.

h. Give the advantages and disadvantages of purchasing.

i. The evaluation and selection of a system design usually involves both a preliminary and a final evaluation before a design can be selected. Distinguish between the two.

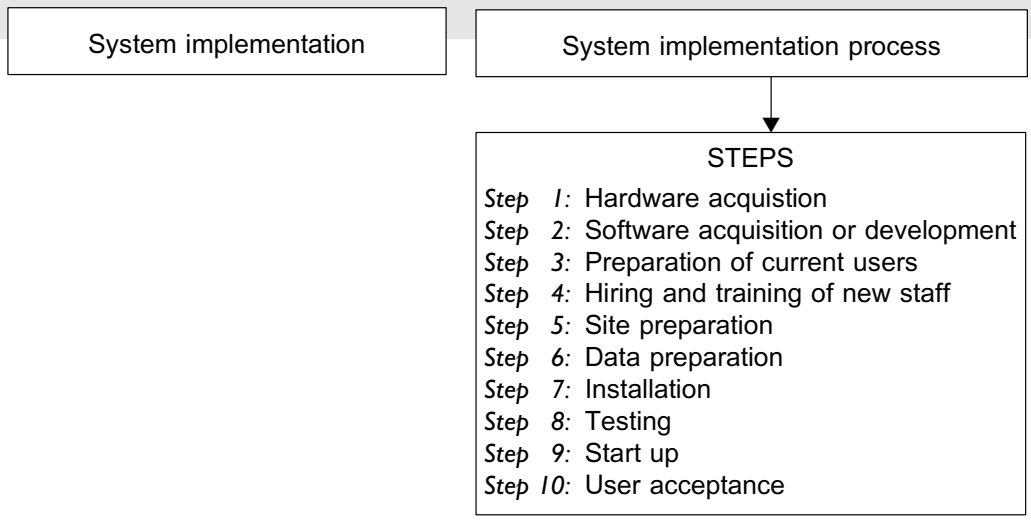
j. Organisations can acquire an information system from one or more service providers. Give seven factors to consider when selecting a service provider.

k. The writing of a system design report forms the final part of this stage. This report contains the results of this phase. Give seven items that should be included in this report.

STUDY UNIT 16

System implementation

In this study unit



1 INTRODUCTION

There are still a number of tasks to do, after the information system was designed successfully and before the system is ready to be used.

In this study unit, we discuss the tasks involved in the system implementation step of the system development process. Most of the planning has now been done and, during this stage, the development team goes into action.

2 SYSTEM IMPLEMENTATION

The purpose of *system implementation* is to ***finalise*** and install the system and to make everything, including users, ***ready for*** its ***operation***. The implementation stage ***puts the planned changes*** or ***new system*** into ***action***.

3 STEPS IN THE SYSTEM IMPLEMENTATION PROCESS

Stair et al (2008:445) emphasise the following steps in the system implementation process:

Step 1: Hardware acquisition

Step 2: Software acquisition or development

Step 3: Preparation of current users

Step 4: Hiring and training of new staff

Step 5: Site preparation

Step 6: Data preparation

Step 7: Installation

Step 8: Testing

Step 9: Start-up

Step 10: User acceptance

3.1 Step 1: Acquiring hardware

When implementing a new information system, hardware and other resources are needed. These can be obtained by purchasing, leasing or renting them (a*dvantages and disadvantages have already been discussed in study unit 15)* from an information system vendor or specialised hardware suppliers. It is vital to gain information on available hardware, hardware requirements *(to ensure that the hardware will meet the requirements to run the software)*, terms of the suppliers, and to consider these different options before making an informed decision.

Information technology suppliers refer to companies that offer hardware, software, telecommunication systems, databases, information, staff and other computer-related resources.

3.2 Step 2: Acquisition or development of software

This refers to the acquisition or development of software already identified according to the specifications set in the design stage.

Application software can be acquired by purchasing it from external developers or by developing it in-house; this is usually referred to as the make-or-buy decision. However, when it comes to software that serves more specialised needs it might be better to create new software that fits those specific needs, such as financial system.

Off-the-shelf software is software that can be purchased commercially. It typically requires some configuration so that the software package is tailored for the specific user. Thus, off-the-shelf software packages, such as word processors and anti-virus packages can be sold to many users. Off-the-shelf software may offer significant savings in that the initial cost may be lower because the software development has been spread over many customers. Moreover, the quality of the product is likely to be high because the developers have been able to test and fix program bugs and glitches as they are reported by users. However, it may happen that the software lacks certain important features.

In-house developed software cannot be purchased commercially. As the name indicates, the software needs to be developed in-house which will result in a one-of-a-kind program for a specific application. One advantage of having software developed in-house is that the users are able to get exactly what they want. However, it takes time to develop and test the new software and is usually more expensive than off-the-shelf options.

There are few circumstances when it makes sense to create software, as it can be very expensive and the benefits do not always justify the risks or costs.

Comparison of off-the-shelf software and in-house developed software

Factor	Off-the-shelf (buy)	In-house (developed)
Needs	Might not match needs exactly	Software should match your needs exactly
Cost	Cost of buying prewritten packages is lower	Higher cost
Time	Time spent on development will be drastically reduced, as the software can be acquired straightaway	Can take years to develop a system to suits your needs
Quality	Usually high quality	Quality can vary depending on the programming team
Competitive advantage	Other organisations can have the same software and the same advantage	Good software can create a competitive advantage

Database and telecommunication system acquisition or development:

Database and telecommunication systems require a mix of hardware and software. As such, many of the approaches discussed earlier for acquiring hardware and software also apply to a database system and telecommunication hardware and software.

3.3 Step 3: Preparation of current users

User preparation is the process where managers, decision makers, employees, other users and stakeholders are prepared, to enable them to use the new system when implemented.

3.4 Step 4: Hiring and training of new staff (if needed)

The size of the new system plays a vital role in the decision on personnel hiring and training. Organisations may have to hire and/or train new information system personnel. It may be necessary to appoint information system personnel for the new system.

3.5 Step 5: Site preparation

Site preparation refers to the physical preparation of the site where the new system is going to be located. This can be as simple as rearranging the furniture to accommodate the new computers or it can be as complicated as installing special wiring and air-conditioning. The extent of the preparation depends on the size of the new information system and the extent of the changes from the old system to the new system.

3.6 Step 6: Data preparation

In order to computerise the work processes, an organisation must convert all manual files to computer files. This process is called *data preparation or data conversion*. If already running an existing computer information system, backups of data should be made in compatible format to be uploaded on the new system.

All permanent data must be placed on permanent storage devices, such as hard drives or CD/DVD disks. The computerised data system and software will then be used to maintain and update the files.

3.7 Step 7: Installation of new hardware

Installation is the process of physically placing the computer equipment on the site and making it operational.

Someone from the organisation should supervise the installation process, making sure that all equipment specified in the contract is installed. The manufacturer is usually responsible for installing computer equipment.

After the system has been installed, the manufacturer is supposed to carry out several tests to make sure that the equipment is working as it is supposed to.

3.8 Step 8: Testing

Good *testing* procedures are crucial to ensure that the new or modified information system operates as intended. Insufficient testing can result in mistakes and problems.

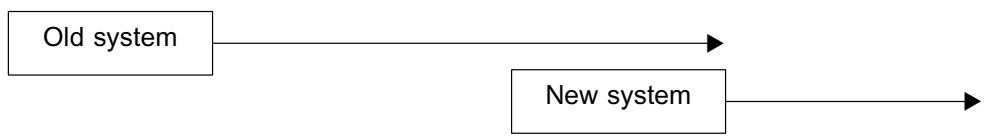
3.9 Step 9: Start-up

Start-up is the process of making the final tested information system operational. This process begins with the final tested information system. When start-up is complete, the system is operational.

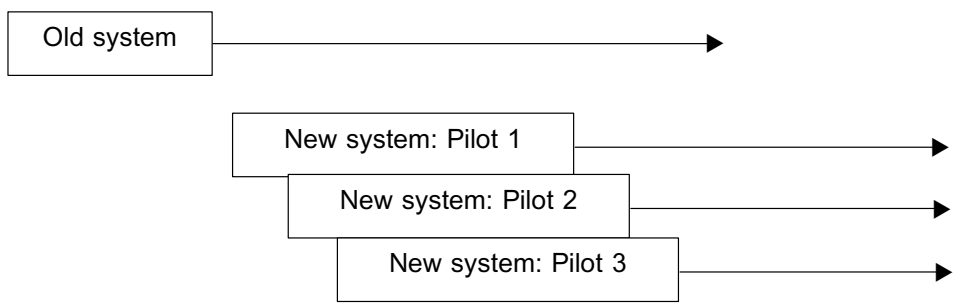
Stair et al (2008:452) refer to various start-up approaches that can be used, such as:

Direct conversion: The old system stops and the new system starts on a given date.

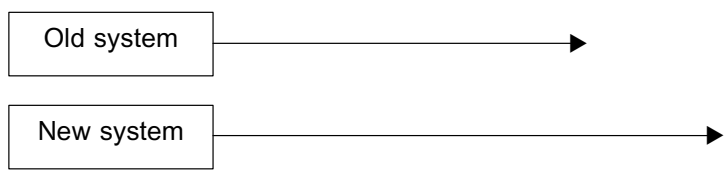
Phased-in approach: Components of the old system are phased out while components of the new system are slowly phased in.



Pilot running: The new system is used by a small group of users first, rather than all the users.



Parallel running: Both the old and the new system are run for a specific period.



The implementation of information system can be very disruptive and, if poorly managed, can lead to the ineffective operation of the organisation; therefore management must ensure that disruptions are kept to a minimum (Perry 2009:60).

3.10 Step 10: User acceptance

The user acceptance document is a formal agreement signed by the user that states that the installation of the system has been approved.

This legal document usually releases the information systems' vendor from legal responsibility for problems that take place after the user acceptance document has been signed. Such a document is only necessary if an outside supplier is used.

Activity 16.1

Africa Furniture is a large manufacturing company producing exclusive patio furniture. This furniture is distributed from one central warehouse to the nine provinces of South Africa.

Management has decided to decentralise the warehouse function by shutting down the central warehouse and opening nine new warehouses (one in each province). They have also decided to computerise the accounting process, inventory control and ordering process. These warehouses will be linked to a central mainframe server and will be able to submit orders and stock requests to the server from their premises. You have been contracted by Africa Furniture to plan and manage the implementation process.

Required:

a. List the steps that need to be followed during the implementation process.

b. Describe all the possible start-up approaches that could be considered for implementing the new system and recommend one for this scenario.

Feedback

a. Step 1: Hardware acquisition
Step 2: Software acquisition or development
Step 3: User preparation
Step 4: Hiring and training of staff
Step 5: Site preparation
Step 6: Data preparation
Step 7: Installation
Step 8: Testing
Step 9: Start up
Step 10: User acceptance

b. Possible start-up approaches:

Direct conversion: The old system stops and the new system starts at a given date. This is the cheapest approach and eliminates confusion that can be caused by running two systems in parallel. One vital problem should be kept in mind, however. Unexpected problems might appear after implementation and can cause huge problems for the organisation.

Phased-in approach: Components of the old system is phased out while components of the new system is slowly phased in. This approach is easier to manage and short-term disruptions are minimised.

Pilot running: The new system is first used by a small group of users, rather than all the users.

Parallel running: Running both the old and new system for a specific period. This makes it possible to compare the results of the two systems and eliminate any problems before the old system is turned off. One huge disadvantage is the pressure on staff to submit data to both systems.

Recommendation:

In this situation, it should be kept in mind that Africa Furniture is changing its distribution network as well as its information system at the same time. This means that parallel running is not an option as the old system will not be suitable for the new distribution network. This is also the case with pilot running and the phased-in approach. Therefore, the only possible approach is direct conversion.

4 SUMMARY

During the system implementation process, the new system is installed and put into action.

There are several steps to follow in implementing the new information system. These include preparation of physical sites, training of users, appointing staff, acquiring of and installing computer equipment.

The next study unit continues with the development process by explaining the review and maintenance of the information system after the changes or new system has been implemented.

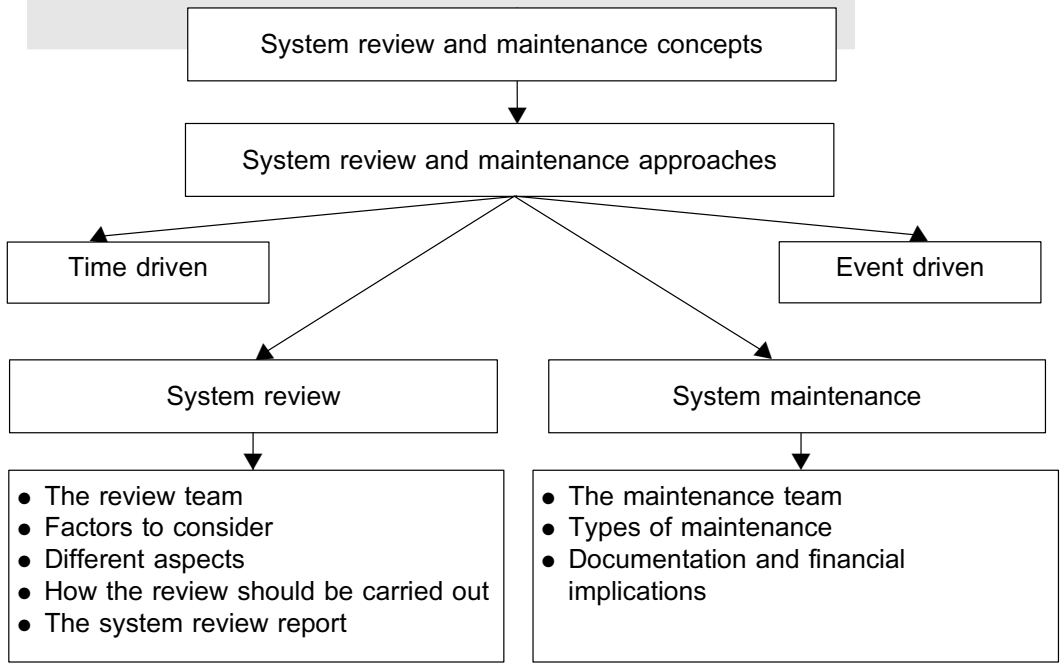
Self-assessment

a. Describe *system implementation* as a stage in the system development process.
b. Name and briefly describe the ten steps in the system implementation process.
c. Compare off-the-shelf and developed software by referring to cost, needs, quality, speed and competitive advantage.
d. Name and describe four different start-up approaches that can be used.

STUDY UNIT 17

System review and maintenance

In this study unit



1 INTRODUCTION

The new system is now operational; however, the development team still has to ensure that everything is running smoothly. During the lifecycle of a new or current system, the system should be reviewed and modified periodically to address the changing needs of its users. Moreover, the use of shortcuts might result in problems and unnecessarily high costs.

In this study unit, some important activities associated with system review and maintenance is dealt with. The development of a new system is an expensive process, therefore system maintenance is critical for the continued smooth operation of the system as well as to ensure that the system stays relevant for as long as possible.

2 SYSTEM REVIEW AND MAINTENANCE

System review is the ***monitoring*** and ***evaluation*** of the system to ***determine*** the ***success*** of the system development process and to ***make sure*** it ***continues*** to ***satisfy*** the ***goals*** of the organisation.

System maintenance refers to a ***continuous*** stage of ***system development*** during

which the operational ***system*** is checked and ***changed*** or ***modified*** to ***improve*** it and make it more ***useful*** in terms of ***meeting*** the goals of users and organisations.

We are going to discuss these two steps together as sometimes regular and continued maintenance might be an indication that a review is required, which could lead to a thorough review of the entire system. On the other hand, a proper review will indicate whether maintenance is required or not.

3 SYSTEM REVIEW AND MAINTENANCE APPROACHES

If not monitored and modified on a regular basis, a system will only be relevant and effective for a short period. Review and maintenance are required in order to extend the life of the current system for as long as possible.

In practice, there are two approaches to system review and maintenance:

Time-driven approach: A time-driven procedure is performed periodically. Using this method, the current system is monitored at a specific time. If problems or opportunities are uncovered, maintenance or a new system development cycle may be initiated.

Event-driven approach: An event-driven procedure starts when a problem or opportunity such as an error, a corporate merger, a new market, or new product arises. Sometimes organisations ignore minor problems, but wait until a huge problem or opportunity occurs before a review or change is initiated. However, some organisations make use of an uninterrupted improvement process to review and improve or maintain their system. With this process, an organisation reviews and modifies the system, even when small problems or opportunities arise.

Events can include the following:

- new information needs by users and managers resulting from changes in the industry and new competitors entering the market
- errors, anomalies and problems in the program that were not picked up during the development stages
- business processes that have changed for some reason
- corporate mergers and acquisitions that require the integration of a different system
- changes in technology that result in the use of new hardware
- technical problems with software and hardware
- new government regulations that affect the operational system and requirements
- unforeseen events that result in the need to make changes to the system

Most organisations use a combination of the two approaches.

4 THE SYSTEM REVIEW PROCESS

The system review process has two main objectives:

- In the first place to review whether the system is developed as intended. This type of review is the responsibility of the review team that will consist of the system development team as they were involved in the whole system development process.
- Secondly, the system review process can also be used to review whether the new system really fulfils the user and organisational needs as envisaged. An independent review team usually performs this type of review.

4.1 Review team

If the organisation has already decided to develop a new system, a development team would be the best people to review the current system. (Refer to study unit 14). In a review process, after a new system has been implemented, it would be better if an independent system review team were to carry out the review process. According to Howarth, Stanton and Sinclair-Hunt (2005:135), it can be unwise to use the same team that has set up the new information system to review it, as it could be too close to the system to view it objectively. (The review team is normally also responsible for the resource management review.)

4.2 Factors to consider during the system review process

During a system review, important *factors to consider* are:

- the mission and goals of the organisation
- hardware in use
- software in use
- controls in place
- costs of development and operation

4.3 Different aspects of the review process

The review phase consists of the following two aspects:

4.3.1 Post-implementation review

A while after system implementation (between 1 month and 1 year), the development team needs to initiate a *post-implementation review* to measure the success of the development process, to determine whether the required objectives have been met and if not, why not.

Post-implementation review measures:

- the suitability of the conversion, transfer and introduction procedures
- whether the underlying principles of the changes have been clearly explained
- the suitability and effectiveness of the documentation created during the system implementation process
- whether the user training conducted during the implementation process was effective
- whether there was a closure process with the users and stakeholders

The following questions need to be asked during the post-implementation review:

- Are the users satisfied with the new system and if not, why not? This can be done by talking to top management, operations management and end-users about their satisfaction with the new system.
- Is the new system effective and reliable? This can be ascertained by, for instance, observing employees' work performance or studying system logs indicating down-time. Are the input processing and output procedures accurate, suitable and working properly?
- Have the processing errors been recognised and resolved?
- Are the internal and/or external auditors satisfied with the controls?
- Are the security and control procedures safe and effective?

The post-implementation review is also beneficial for the development team, as it gives

them the opportunity to evaluate their own work and to learn from their mistakes or successes. In future, this will result in more skilled system developers, work satisfaction and satisfied clients.

4.3.2 Resource management review

The resource management review is done to determine the effectiveness of the use of organisational resources during the system development stages.

An internal auditing team will usually do this review; where an internal auditing team does not exist, a senior management team will do the review.

The following *questions* need *to be asked* during the resource management review:

- Was the system development process properly managed and sufficiently coordinated?
- Was the system development process sufficiently communicated to all stakeholders by the development team?
- Was the development cost accurately budgeted?
- Were there any deviations from the budget and, if so, were they justified and authorised?
- Was the system development schedule realistic?
- Were there any deviations from the system development schedule and, if so, were they justified and authorised?

Action to improve the system will be taken if problems arise; then the system will need to be reviewed again. This will go on until the development team is satisfied with the final product.

4.4 Review methods

Howarth et al (2005:133) mention four possible methods for conducting reviews namely:

Questionnaires: This may seem to be a simple method, but it is difficult to word questions in such a way that questions do not lead the respondent to answer the questions in a way that is not totally objective (these are called *leading questions*). An example of a leading question is: ''How frustrated were you when you started to use the new information system?'' This question assumes the user was frustrated.

Focus groups: Small groups come together to discuss issues of concern in the system. In this case, some aspects might be overemphasised while others are ignored.

Performance measures: Using predetermined criteria to evaluate the system. In this case, it might be difficult to agree on such measures.

Carry out a survey: A survey is carried out using a specially devised evaluation tool that enables users to focus on broad areas of interest. For example, weighting the importance of the areas you are focusing on to give a more accurate result.

4.5 The system review report

After the review process has been completed, the facts need to be collected and the development team needs to prepare a formal system review report.

This report will include the following information:

- The background of the system's development
- Details from the evaluation of the system development team including:

- a summary of the system's overall quality,
- an assessment of overall performance and
- a summary of the areas where the system is considered to be unsatisfactory

- Details from the evaluation of how well the objectives of the organisation have been met, including:
  - a cost-benefit analysis comparing the costs and benefits identified and
  - an assessment of the quality of the project's management and how the project objectives have been met

- Details from the evaluation of user and stakeholder satisfaction
- A summary of recommendations for improving the performance of the system and improving future system development projects as well as a conclusion

5 THE SYSTEM MAINTENANCE PROCESS

5.1 The maintenance team

According to organisational policies, the people in the *system maintenance team* may be different staff members from the development team members.

- The team who designed and built the system may also be responsible for maintaining the system, or
- It can be a separate maintenance team.

In practice, the development and implementation team do not normally do the follow-up maintenance of the new system. The control of the system is turned over to the IT department, which is now responsible for the maintenance.

The system maintenance team's *responsibility* will be to ensure that

- system changes are carried out quickly and effectively
- failed hardware is fixed quickly and properly
- existing software is fixed if necessary
- existing software is updated regularly
- existing software is modified when required

5.2 Types of system maintenance

Stair and Reynolds (2008:553) mention the following generally accepted categories signifying the amount of change involved in system maintenance:

- *Slipstream upgrade:* A slipstream upgrade is a minor upgrade, typically a software code adjustment or minor bug fix, which is not worth announcing to users.
- *Patch:* A patch is a minor change to correct a problem or make a small enhancement.
- *Release:* A release is a significant program change that often requires changes in the documentation of the software.
- *Version:* A version is a major program change, typically encompassing many new features.

Activity 17.1

Activity: (Africa Furniture continued from study unit 16)

Read the case study on Africa Furniture in the previous study unit and then complete the following activity.

Africa Furniture implemented their new information system about six months ago and now need to review it in order to determine whether the objectives have been met.

Required:

a. You are requested to advise management on the following:

- The team that should be appointed to manage the system review.
- Possible methods the review team can use.
- What to expect in the review report as drawn up by the review team.

b. The development of this information system was an expensive project and management should ensure that the system remains in use for as long as possible.

You are requested to advise management on the appointment of a maintenance team and to delineate its responsibilities.

Feedback

It is important to use the theory from this study unit and apply it to the Africa Furniture case. For example, the review team needs to be independent and they should use a method that considers the fact that system users are situated all over the country. Will Africa Furniture use a centralised maintenance team or sub-teams for the provinces? You also need to try to make the responsibilities of the maintenance team more applicable to Africa Furniture, implementing a system to submit orders and stock requests to the server from its premises.

5.3 System maintenance documentation and financial implications

In order for system maintenance to be performed, many organisations require a *request for maintenance form* to approve the modification of a system. Consequently, the need for the possible change is recorded and the change priorities identified relative to other work that has been requested. The *request for maintenance form* usually has to be signed by a manager.

The *cost of maintaining* a system forms a large section of the cost involved in the overall system development process. A system that is well designed and documented as efficient, structured and flexible is less expensive to maintain. This means that if more time is spent on design it can result in less time spent on maintenance at a later stage.

6 SUMMARY

System review refers to a continuing process in which the current or new system is reviewed by monitoring how well the system is supporting the goals of the organisation.

The ongoing system maintenance process, on the other hand, guarantees that the system remains effective and relevant for as long as possible.

Sufficient testing of the system can enhance the success of new system implementation and ensure that the current system keeps track of changes in the organisation. Independent reviewers should do the review process, but the same people who developed the system can do maintenance. However, the IT department is usually responsible for maintenance.

In the next part (Part 5), we explain the application of an information system in more detail and will look briefly at some information systems. We also elaborate on electronic commerce.

Self-assessment

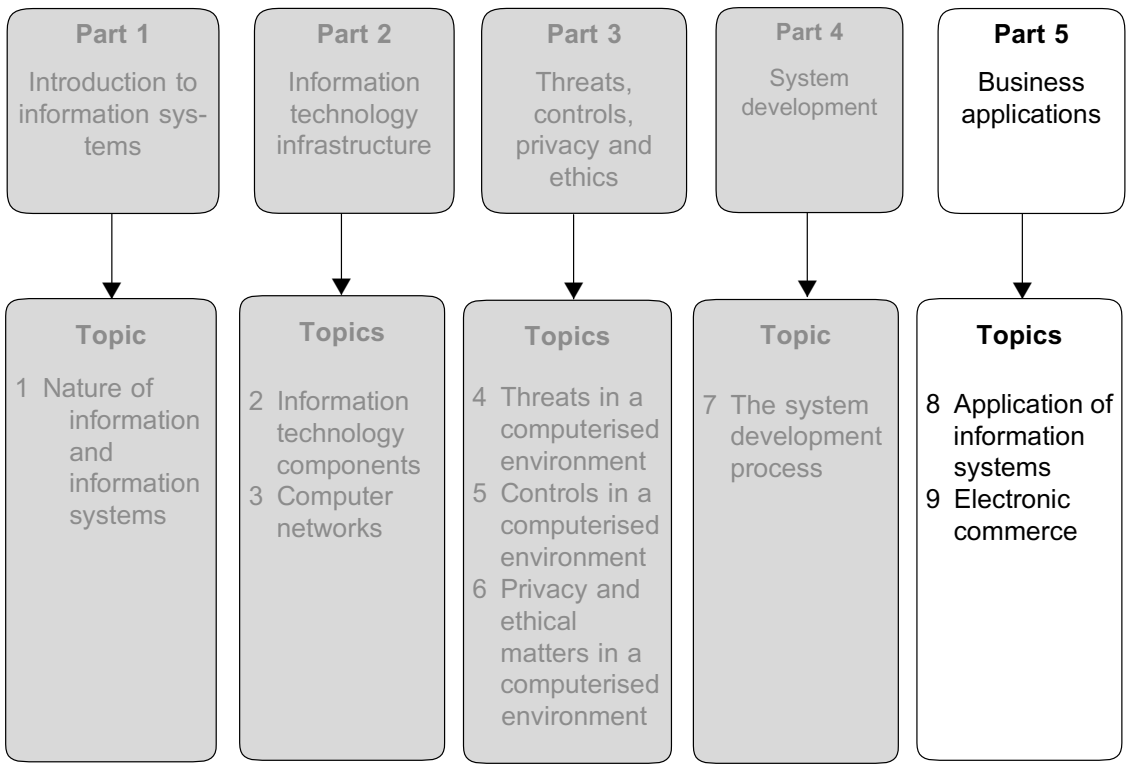
a. Define the terms
   - system review
   - system maintenance

b. Name and describe the two approaches to system review and system maintenance.
c. Name and briefly describe eight events that might trigger system review and maintenance.
d. Name and describe two main objectives of the system review process.
e. Discuss the selection of a review team.
f. Give five important factors that should be considered during the system review process.
g. Name and describe two aspects of the system review phase.
h. Name five aspects that are measured by the post-implementation review.
i. List six questions that need to be asked during the post-implementation review.
j. List six questions that need to be asked during the resource management review.
k. Name and describe four review methods.
l. Define the system review report and list the information that should be included in it.
m. List three responsibilities of the system maintenance team.
n. Differentiate between the four types (categories) of system software maintenance.

Business applications

PURPOSE

An information system play a vital role in the planning, performance measurement, controlling and management of organisations. The purpose of part 5 is to give you a better understanding of the information systems that are available and the various uses to which these systems can be put in the business environment.



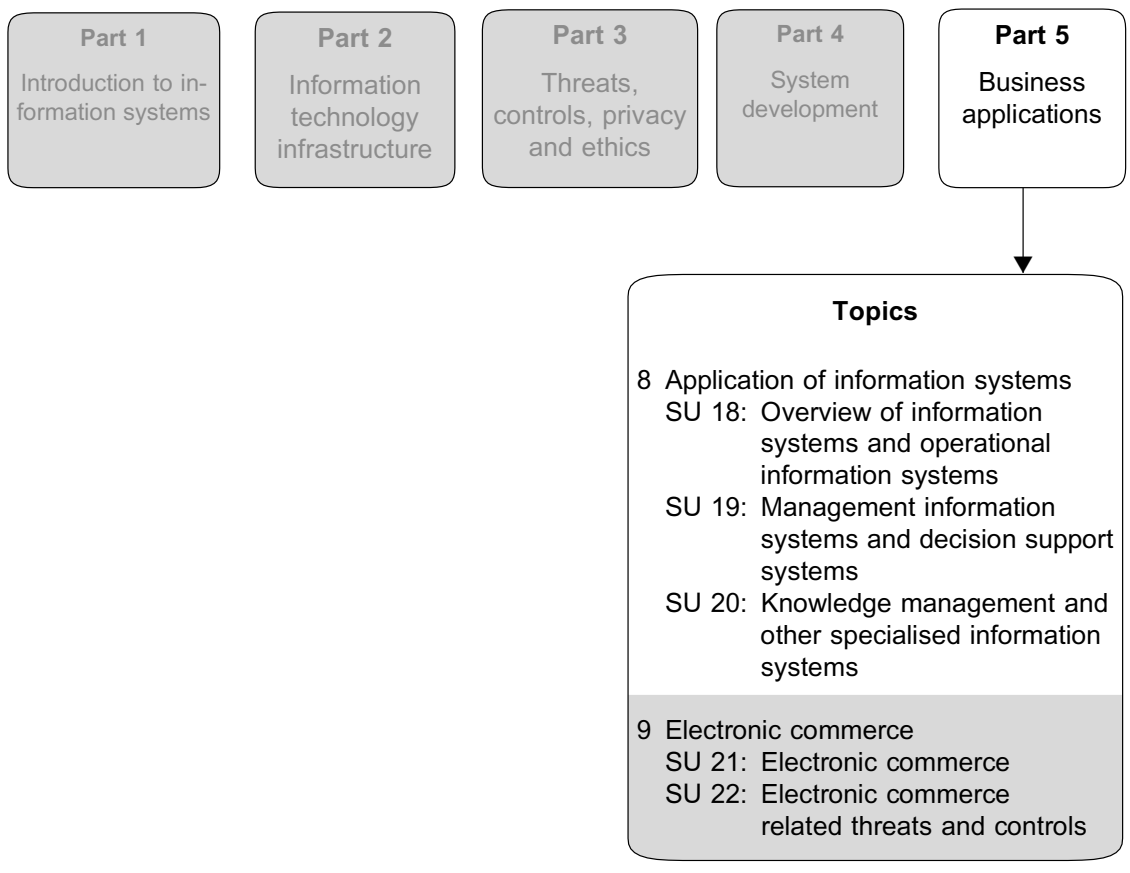
Application of information systems

LEARNING OUTCOMES

After studying this topic, you should be able to

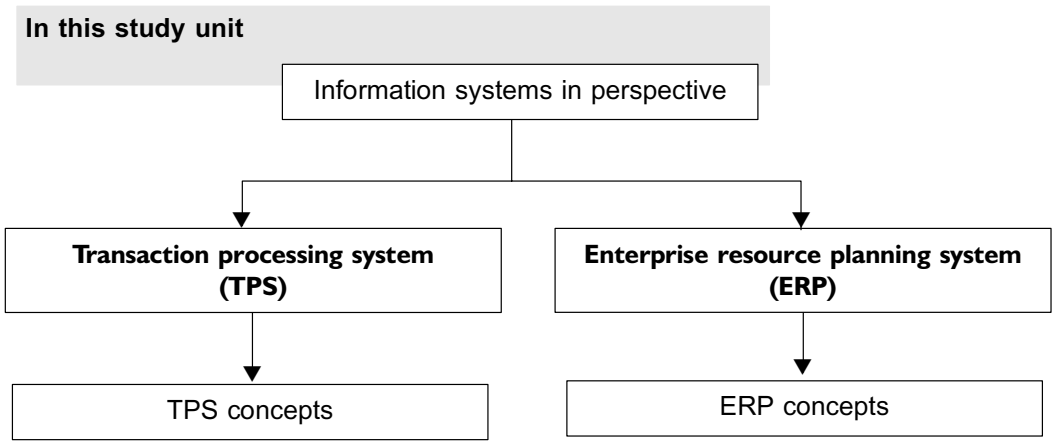
- describe the hierarchy of a business information system
- describe the problem-solving and decision-making process
- define and differentiate between various information systems
- describe the characteristics and applications of various information systems

This topic consists of three study units



STUDY UNIT 18

Overview of information systems and operational information systems



1 INTRODUCTION

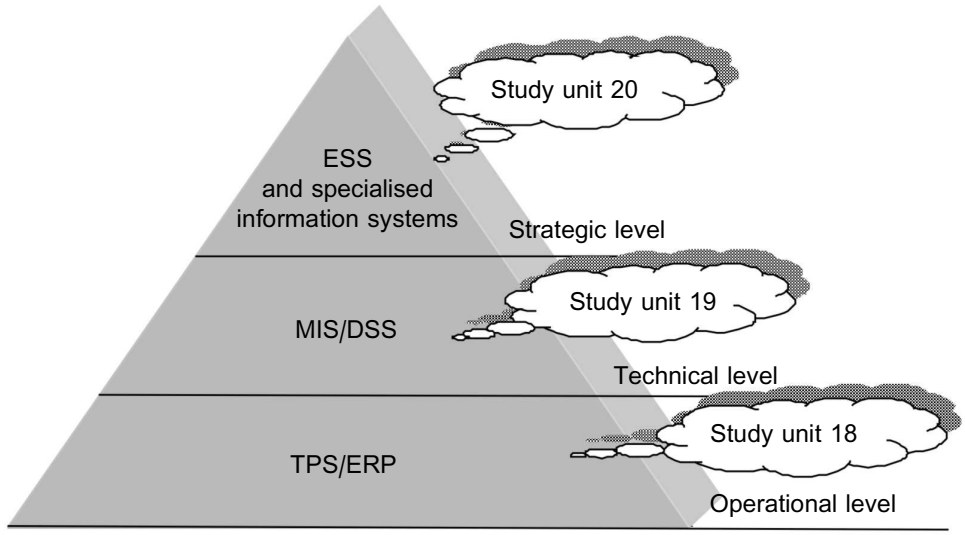
In study unit 2, we discussed the information system and, in part 4, the development of an information system. However, specialised functional areas appear as organisations grow in size and complexity. These areas require specific information for production planning and control, sales forecasting, inventory planning and market analysis. All levels of management often require information that the basic information system do not provide and therefore need to develop a system that fulfil these requirements. An organisation has many information systems. In order to understand these systems and how they fit together, we need to look at the relationship between them.

In this study unit, the information systems generally used at operational level, which include a transaction-processing system and an enterprise resource management system, are discussed briefly.

2 INFORMATION SYSTEMS IN PERSPECTIVE

Organisations use highly integrated information systems that influence all aspects of the business. Without effective and efficient systems, organisations cannot operate, manage, or plan properly to achieve their goals.

Although some systems are used at more than one management level, according to Stair et al (2008:235) information systems can generally be grouped as in fig 18.1:



Source: Stair et al (2008:235) adapted.

FIGURE 18.1: Information system in perspective

Abbreviations in this figure:

Executive support system (ESS)
Management information system (MIS)
Decision support system (DSS)
Transaction processing system (TPS)
Enterprice resource planning system (ERP)

3 TRANSACTION PROCESSING SYSTEM

3.1 What is a transaction processing system (TPS)?

A **TPS collects** an organisation's ***daily business transactions***, processes these into ***useful information***, **stores** the data and information, and ***retrieves*** the transactions (raw data) and information (processed data) to ***provide*** **documents** and ***records*** for business functions.

The following diagram explains the data processing process in the TPS:

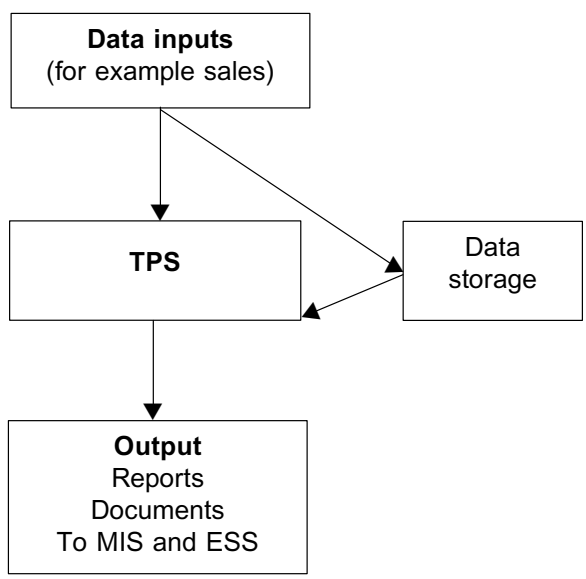


FIGURE 18.2: The data processing process in the TPS

3.2 Business functions

A TPS supports business functions such as

- sales
- purchasing
- accounting

The following table presents an overview of a TPS:

Order processing	Purchasing	Accounting
Processing orders	Purchase order processing	Budget
Sales configuration	Receiving goods	Accounts receivable
Inventory control (finished product)	Inventory	Payroll
Distribution planning and distribution of products	Accounts payable	Asset management
Accounts receivable		General ledger

Source: Stair & Reynolds (2008:357)

A TPS uses *input* from many sources to process this data:

Some possible examples of these inputs are information of

- placed orders
- purchased supplies
- received orders from customers
- payments made
- employees signed in and out

3.3 Advantages of a TPS

The advantages of a TPS are as follows:

- *Excellent customer service:* Use of this computer system assists organisations in providing fast and accurate service; for example, keeping track of goods ordered and of these goods to be delivered.
- *Better supplier relationships*: For example, the up-to-date information supplied by an internet system allows organisations to keep track of any discounts available.
- *Competitive advantage:* Excellent service and consequent improved customer loyalty, as well as better relationships with suppliers, maximise market share and assure better competitive advantage.
- *Accuracy:* The accurate and complete processing of data is vital and a TPS ensures that this is the case.
- *Better productivity of staff*: Manual processing of data is time consuming and nearly impossible nowadays. The use of a TPS reduces these massive labour requirements.
- *Timely user response and reports*: It is vital for organisations to produce data quickly; for example sending invoices to customers.

You will learn more about a TPS and its application in Accounting Information Systems (AIN2601) where you will also learn more about Pastel.

4 AN ENTERPRISE RESOURCE PLANNING SYSTEM (ERP)

4.1 What is an ERP?

Many organisations prefer to use one computer system that integrates all the functions of the organisation and that can be used throughout the organisation.

> An *ERP integrates* the ***data gathering*** and ***data processes*** of departments and functions across an organisation into ***one single system*** of ***integrated applications***. This single system can *handle* the vital *operations* of the *entire organisation* and often *includes* some functions of the *strategic* and *technical level* of the organisation as well.

Examples of an ERP are SAP and Oracle.

The following diagram explains an ERP system:

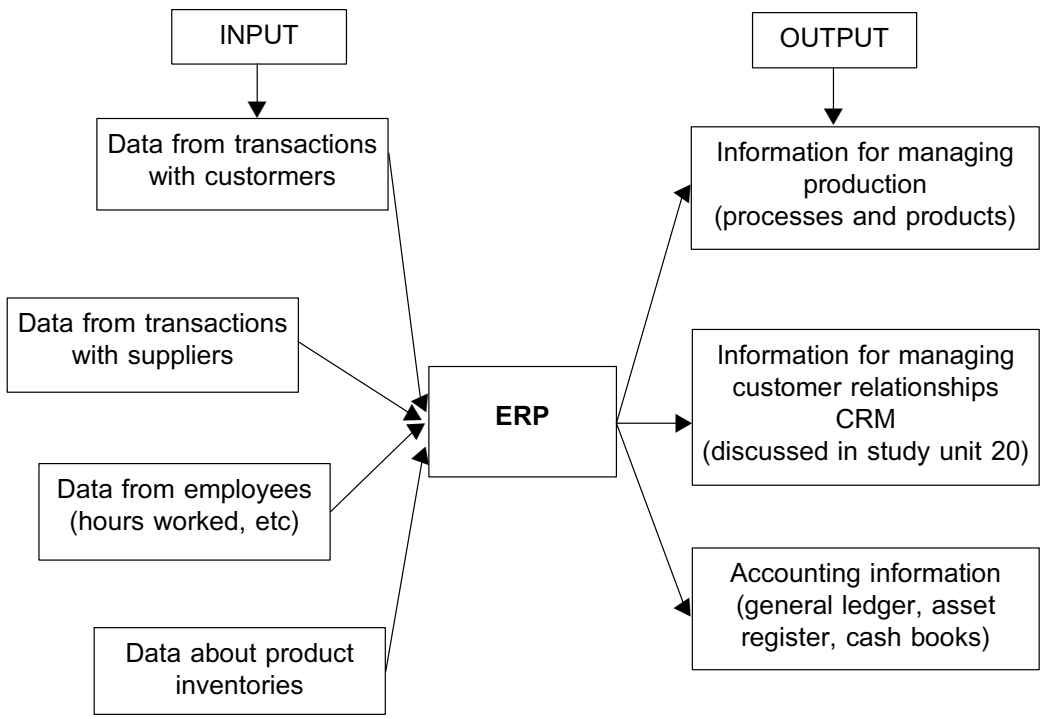


FIGURE 18.3: Explanation of an ERP system

4.2 Advantages and disadvantages of an ERP system

The following table gives the advantages and disadvantages of an ERP:

Advantages	Disadvantages
Any authorised user (restricted to a profile) linked to the server with a computer has access to the authorised information	An ERP is expensive and time consuming to implement
An ERP is a system that is implemented throughout the organisation	It is difficult to implement changes

Advantages	Disadvantages
It makes processes and workflow more efficient	Risks arise when using only one vendor
It eliminates expensive and inflexible system	
Has a familiar interface, menus across all modules	If implementation fails all departments have a problem
It improves tracking and forecasting	
Data only captured once will then be available to all modules connected to ERP	It might fail to live up to expectations; however, this is a risk inherent to any system
It is easier to upgrade only one system	

Activity 18.1

Find out what TPS or ERP system, if any, are used by your employer.

---

5 SUMMARY

There are a large number of information systems available to organisations and each one plays a different role. On an operational level, a TPS is able to support the business functions of an organisation, while an ERP combine some or all systems in one system. This provides important benefits for the organisation.

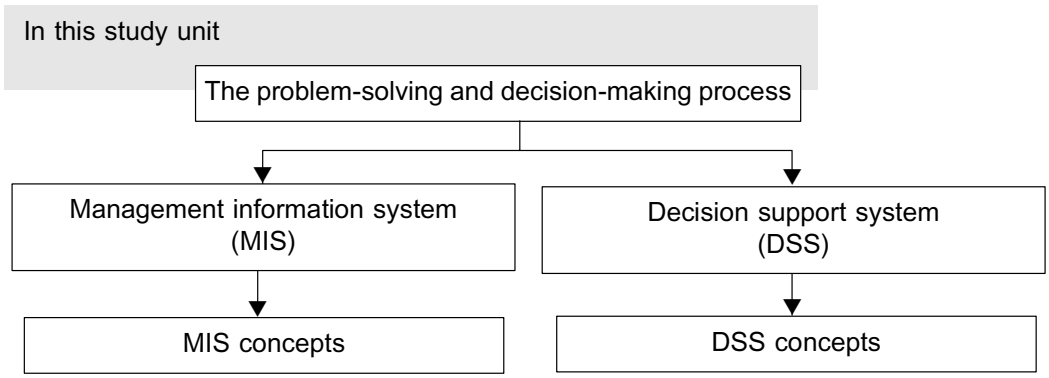
The next study unit (study unit 19) deals with systems generally used by management at the technical level, namely management information systems and decision support systems.

Self-assessment

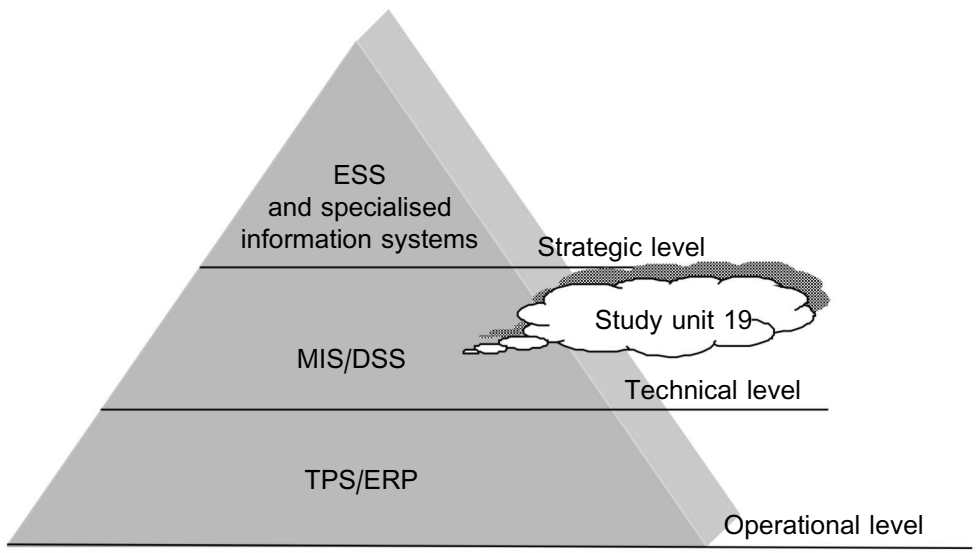
a. Define a TPS.
b. Name three business functions supported by a TPS and give two examples of the data input for each of them.
c. Name and describe six advantages of using a TPS for organisations.
d. Define an ERP.
e. Explain the ERP by means of a diagram.
f. Name six advantages of an ERP.
g. Name five disadvantages of an ERP.

STUDY UNIT 19

Management information systems and decision support systems



1 INTRODUCTION



Source: Stair et al (2008:235). Adapted

FIGURE 19.1: Information systems in perspective

A management information system (MIS) and a decision support system (DSS) are two of the most important support tools on the **technical management level.** Thanks to a MIS and a DSS, managers and employees can access useful information in real time. The vital objective of a MIS and a DSS is to assist managers to make better decisions

and solve key problems. This can result in higher revenues, lower costs and the successful realisation of organisational objectives.

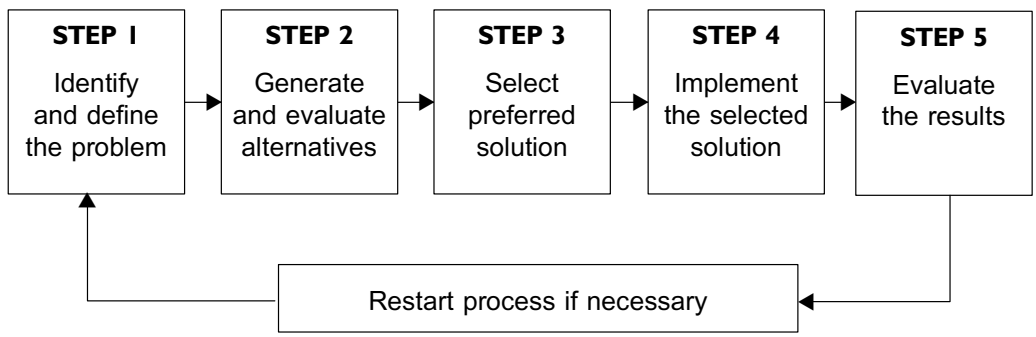
The main components of such a system include a database, people, software and links to external sources of data such as the internet, corporate intranets and other external databases.

In this study unit, we are looking at the problem-solving and decision-making process and we discuss a MIS (only an overview) and a DSS briefly.

2 THE PROBLEM-SOLVING AND DECISION-MAKING PROCESS

As an MIS and a DSS assist management with decision-making, we need to discuss the decision-making process first.

Solving problems is a crucial activity for any organisation. Once a problem has been identified, the problem-solving process begins by making some vital decisions. The problem-solving process can be explained as follows:



Source: Pathways (n.d.)

FIGURE 19.2: An information system in perspective

Identify and define the problem: During this stage, possible problems or opportunities are identified and defined, and information is gathered that relates to the reason for the problem.

Generate and evaluate alternatives: In this stage, different solutions to the problem are generated and their viability is evaluated.

Select preferred solution: To select the preferred solution a plan of action need to be drawn up; if this is not possible, the process will start again from the beginning.

Implement the selected solution: Problem solving goes further than decision-making and includes the implementation of the solution. It is during this phase that the solution is put into effect.

Evaluate the results: This is where the decision makers evaluate the implementation in order to determine whether the predicted results have been achieved. In the light of this new information, the process is then modified.

Activity 19.1

You have been in a car accident and your insurance company has written off your car. You need to buy a new car but have no idea what car to choose.

Required:

Illustrate how you would solve this problem by applying your situation to the steps in the problem-solving process.

---

3 MANAGEMENT INFORMATION SYSTEMS (MIS)

3.1 What is an MIS?

An *MIS* is an *integrated system* that provides management with a wide variety of decision-oriented information in order to accomplish ***organisational*** objectives. An MIS ***converts data*** from ***mainly internal sources*** into ***information*** and offer ***regular reports*** and ***online access*** to the present and past performance of the organisation (BPP-LM-CIMA E1 2009:58). The functions of an MIS are based on the transaction processing system, but extra information is provided to assist the management with decision-making.

The monthly management accounts that are produced with the help of for instance Pastel AccPac, SAP and MS Office are part of the MIS.

> You will learn more about an MIS and the use of Pastel and MS Excel in Practical accounting data processing (AIN 2601).
>
> In Principles of management accounting (MAC 2601) and Principles of strategy, risk & financial management techniques (MAC 2602), you will learn about the financial and non-financial information that managers require in order to control and manage the organisation.

3.2 Characteristics of an MIS

- provides reports using a fixed and standard format; for example, reports for inventory control where different managers can use the same report for different purposes
- provides reports in hard and soft copy; although managers use visual displays on screen, reports are also printed
- provides the potential for users to draw up their own customised reports
- supports decisions at operational and management control levels
- uses mainly internal data from a computer system to provide reports; can also use external data from the Web, including inflation rates, interest rates, share price and information on competitors
- provides exception reports on variances from budget and allows managers to feed back any changes they need to make as a result of these variances
- main focus of an MIS is internal as it is used by management

4 DECISION SUPPORT SYSTEM (DSS)

4.1 What is a DSS?

As the name indicates, a *DSS* ***helps management*** at ***technical*** and ***strategic level*** with ***decision-making*** by ***providing tools*** and ***models*** to ***solve structured***, ***semi-structured*** and ***unstructured problems***. A DSS offers a range of possibilities. It aids decision makers in a *variety of circumstances* and provides

support for all phases of the problem-solving process. A DSS is an interactive computer-based system and subsystem intended to help decision-makers use communication technologies, data, documents, knowledge and/or models to complete decision process tasks.

A decision support system may present information graphically and may include an expert system.

Typical information that a decision support application might gather and present would be:

- accessing all information assets, including legacy and relational data sources
- comparative data figures
- projected figures based on new data or assumptions
- consequences of different decision alternatives, given past experience in a specific context.

According to Nurjuliana (2007:24), a DSS can be categorised into five types:

- *Communication-driven DSS*: Most communication-driven DSSs are targeted at internal teams, including partners. Its aim is to help conduct a meeting, or for users to work together. The most ordinary technology used to deploy the DSS is a web or client server. Examples are chats and instant messaging software, online collaboration and net-meeting system.
- *Data-driven DSS:* Most data-driven DSSs are targeted at managers, staff and product/service suppliers. It is used to query a database or data warehouse to look for specific answers for specific purposes. It is deployed via a mainframe system, client/server link, or via the web. Examples: computer-based databases that have a query system to check the databases.
- *Document-driven DSS:* A document-driven DSS is more common, targeted at a broad base of user groups. The purpose of such a DSS is to search web pages and find documents on a specific set of keywords. The standard technology used to set up a DSS is via the web or a client/server system.
- *Knowledge-driven DSS:* A knowledge-driven DSS is fundamentally used to provide management advice or to choose products/services. The typical technology used to set up such system could be client/server system, the web, or software running on stand-alone PCs.
- *Model-driven DSS:* A model-driven DSS is a complex system that help analyse decisions or choose between different options. It is used by managers and staff members of the business. A model-driven DSS can be deployed through software/hardware in stand-alone PCs, client/server systems, or the web.

The following diagram explains a DSS:

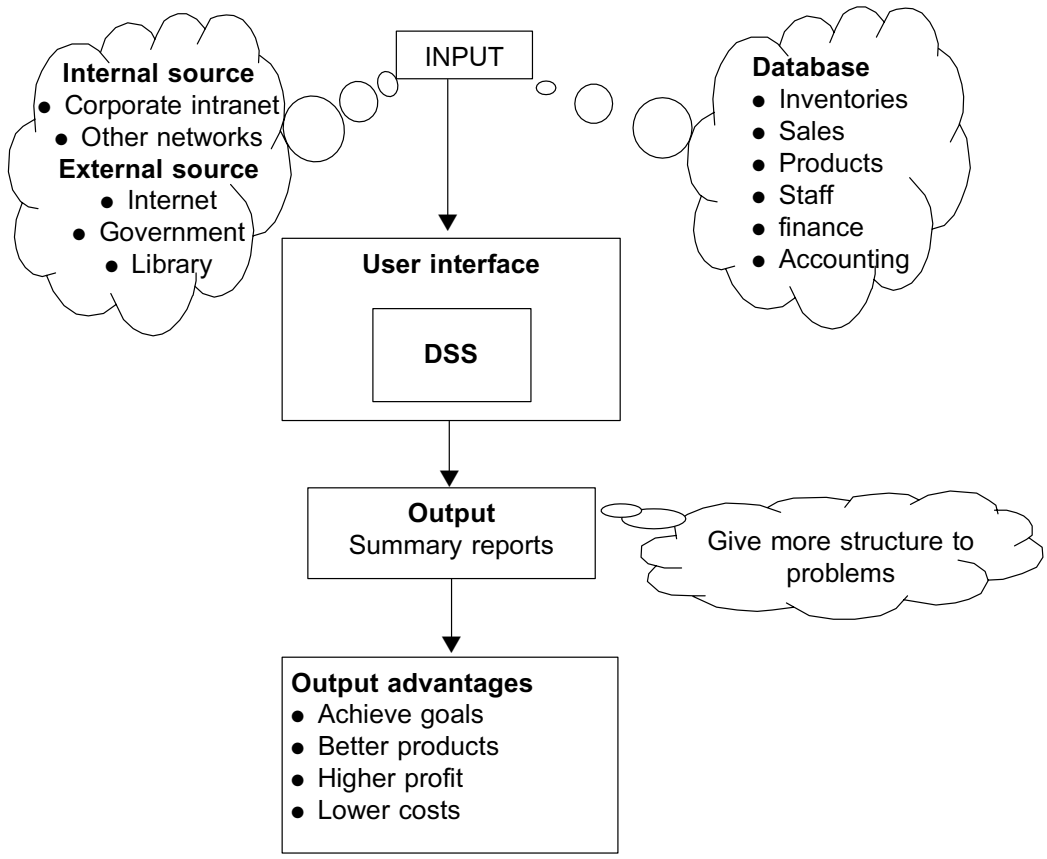


FIGURE 19.3: Explanation of a DSS

4.2 The characteristics of a DSS

The following is a summary of the characteristics of a DSS:

- A DSS is specifically developed to help with decision-making that varies from solving highly structured problems to unstructured problems.
- Managers are assisted with decision-making throughout the different stages of the problem-solving process.
- The decision processes are streamlined, as a DSS helps with decision-making at strategic, tactical and operational levels of the organisation, as well as with once-off decisions and repetitive decisions.
- Information can be generated in a timely manner, because a DSS offers quick access to information.
- Users are allowed to drill down to the organisation's information and a DSS handles huge amounts of data from various sources.
- The DSSs main function is to *support* decision-making rather than to *automate* decision-making.
- The flexibility of a DSS allows managers to customise reports and presentations.
- A DSS is able to react fast to the changing needs of users.
- A DSS helps by performing complicated analyses and comparisons using advanced software packages such as Microsoft Excel, in areas such as 'what-if' analysis, simulation and goal-seeking analysis.

5 THE DIFFERENCES BETWEEN A DSS AND A MIS

DSS	MIS
Aim to solve unstructured problems	Aim to solve structured problems
Users usually more involved in the development of system	Users not so involved in the development – sometimes generic system
Focus is on leadership by providing them with information to make creative and innovative decisions	Focus on all the information gathered from different units and spheres in the organisation and then reported as a unit
Specialised reports as output	More generic reports as output
Special reports as output depending on specific problems, factors and needs of users	Pre-specified periodic generic reports are usually the output of the system.
Reports are generally generated by interactive interfaces that a user can use	Reports are usually not generated by interactive interfaces but through predetermined settings and factors
Reports are generated by using analytical modelling techniques	Reports are usually generated by using averages and basic calculations

6 SUMMARY

In order to reach the organisational goals, managers need insight into the normal operations of the organisation. An MIS helps management with this process, by producing exception reports based on variances from the budgets, long outstanding orders, budgets and processed transactions.

A DSS has more analytical power than any other system. It is used by management and employees to make decisions about issues with high uncertainty.

The following study unit describes the information system predominantly used by managers for planning and strategy on the strategic level, and explains other specific information systems.

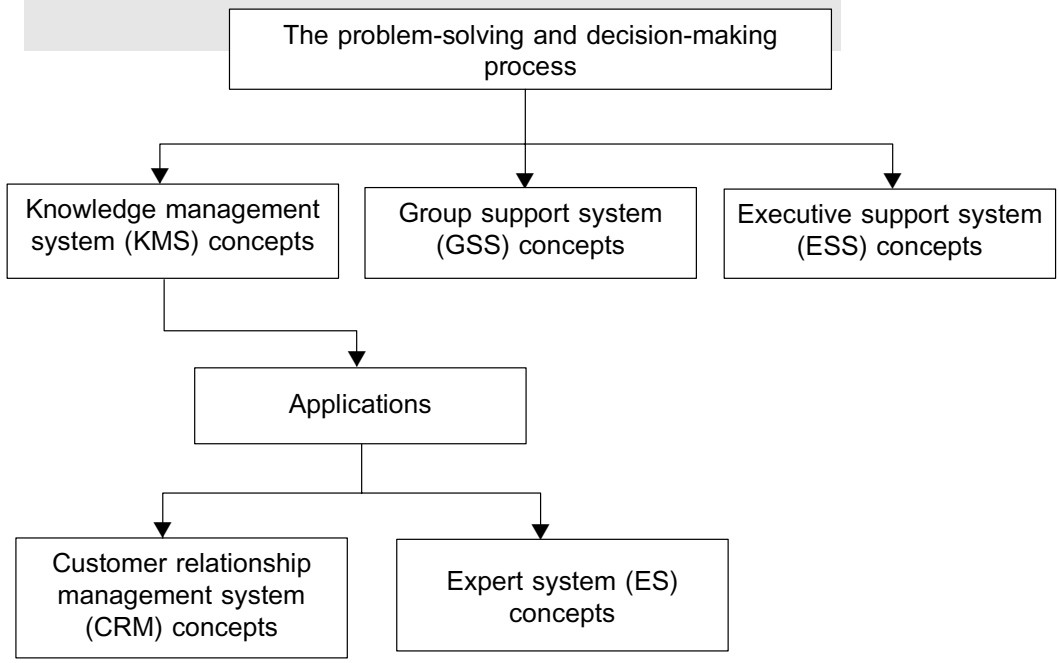
Self-assessment

a. Illustrate the stages of the problem-solving process and briefly explain each stage using a diagram.
b. Define a management information system (MIS).
c. Define a decision support system (DSS).
d. Describe the five types of decision support system (DSS).
e. Describe seven characteristics of an MIS.
f. Describe nine characteristics of a DSS.
g. Explain the difference between a MIS and a DSS in table format.

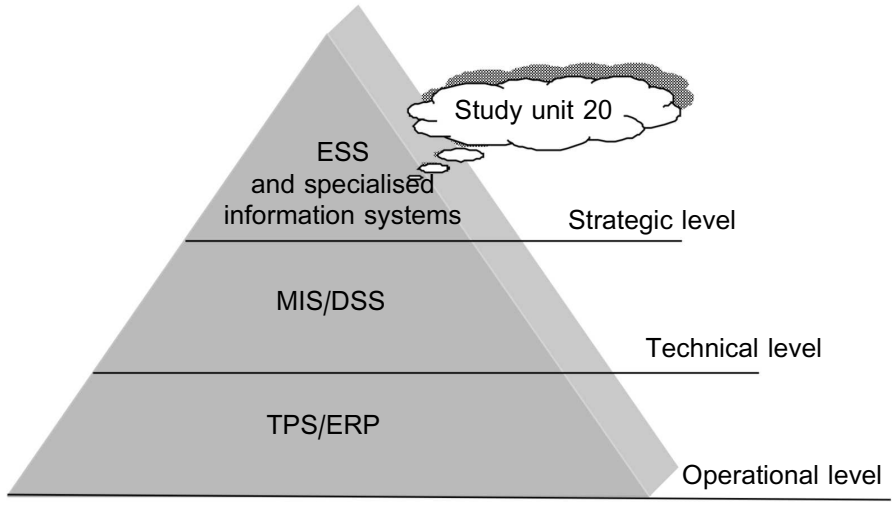
STUDY UNIT 20

Knowledge management and other specialised information systems

In this study unit



1 INTRODUCTION



Source: Stair et al (2008:235)

FIGURE 20.1: Information systems in perspective

In this study unit, we will discuss some systems generally used on the strategic management level. A knowledge management system (KMS) or, more specifically, expert system (ES) and customer relationship management (CRM) system, will be explained. You will also learn more about a group support system (GSS) and an executive support system (ESS).

Systems on the strategic level of management use information captured and processed together with other internal and external information to produce combined reports for vital decision-making and planning. A KMS (ES and CRM system) is used in many industries and knowledge about these systems will help you to discover new ways to use information systems in your workplace. A KMS allows an organisation to share knowledge and experience among its managers and employees. A GSS saves time and improves planning by supporting employees and managers to communicate with each other, schedule meetings on networks and send documents to each other.

2 KNOWLEDGE MANAGEMENT SYSTEM (KMS)

2.1 What is a KMS?

A *KMS* is a system used to ***support*** the ***creation***, capturing, storing and ***distribution*** of ***expertise*** and ***knowledge*** by ***using*** people, ***procedures***, ***software***, ***databases***, and ***devices***. The reason for using a KMS is to provide specific aid in achieving the organisation's objectives (profit maximisation and cost minimisation).

2.2 The characteristics of a KMS

According to Awad and Ghaziri (2008:337), the main characteristics of a KMS are as follows:

- A KMS solves appropriate problems relatively accurately, depending on the complexity of the problem.

- Although a KMS has a high response speed, the speed is likely to degrade as the difficulty of the problem increases.
- Large amounts of pre-processed data need to be submitted to the system.
- Staff running a KMS need to be trained and they require a high level of user knowledge.

2.3 Two applications of a KMS

2.3.1 Customer relationship management (CRM) system

- What is a CRM system?

  A *CRM system* is a form of KMS and involve ***information relevant*** to an ***organisation's customers***. A CRM system ***comprises software*** that ***concentrates*** on ***providing information*** relating to an ***organisation's customers*** and ***products***.

Accordingly, all the knowledge or intelligence gathered about customers is stored in one system or database.

The following diagram explains the CRM system:

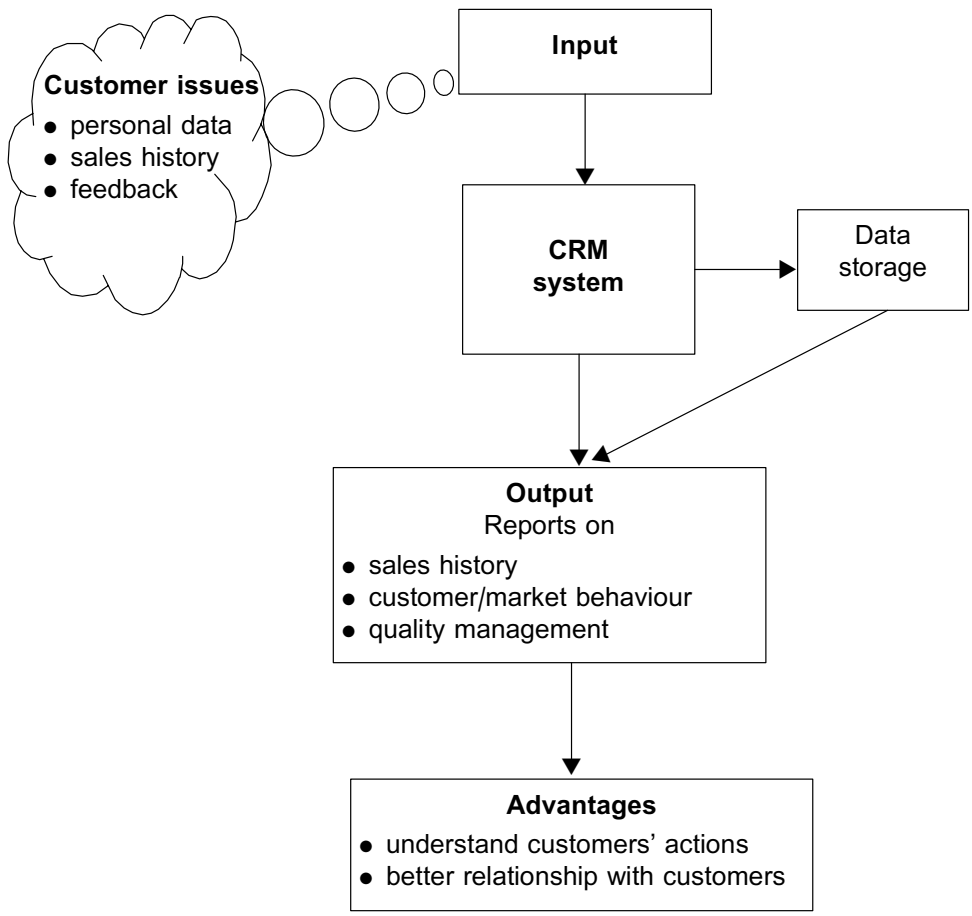


FIGURE 20.2: Explanation of the CRM system

- **Applications for a CRM system**

In order for organisations to improve their knowledge of their customers, the CRM system helps organisations to

- collect data on customers
- retain loyal customers
- use customers' order histories
- contact customers
- handle customer enquiries and complaints
- provide a fast and appropriate response to customers' needs
- obtain market feedback
- advertise new products among customers
- sell products and services to customers

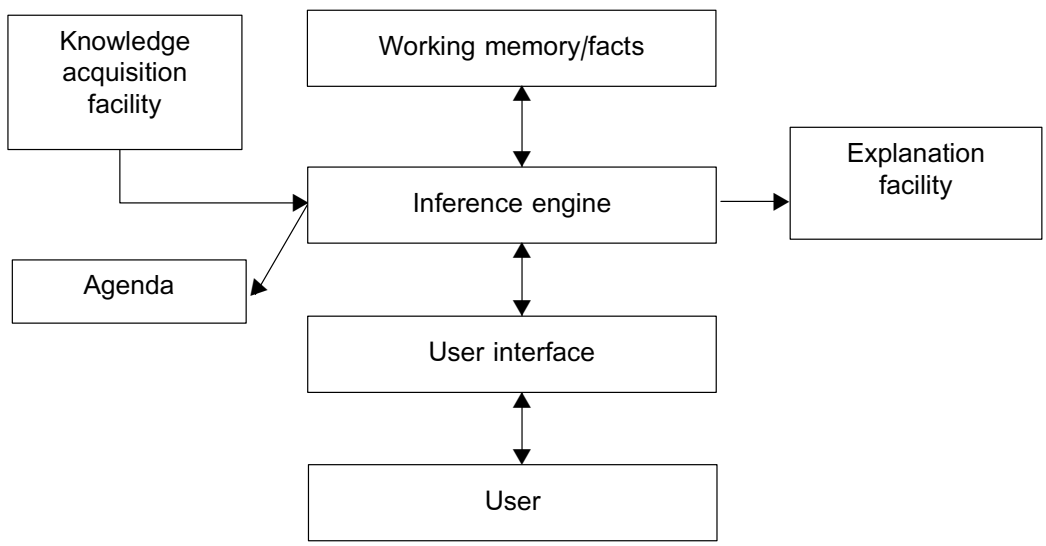
2.3.2 Expert system (ES)

- **What is an ES?**

> An *ES* attempts to *capture* the *knowledge* of *experts* and ***allow*** *users* who are not experts in the field to ***benefit*** from the ***available*** *knowledge*. This system is developed for ***specific*** *expert* use as well as to ***identify*** *problems*, ***forecast potential events***, and ***resolve*** *problems*.

ES has also been used to design new products and systems, establish the best use of lumber, and raise the quality of healthcare.

Savage (2009) explains an ES as follows:



Source: Savage (2009)

FIGURE 20.3: Explanation of the ES

- *User interface.* The means by which the expert system and the users communicate.
- *Explanation facility.* Explains how the ES arrived at the conclusion.

- *Working memory.* A global database where all the facts used, are stored.
- *Inference engine.* Makes inferences by using information, seeking relationships and providing conclusions and suggestions.
- *Agenda.* A prioritised list of rules created by the inference engine, whose patterns are satisfied by facts in working memory.
- *Knowledge acquisition facility.* An automatic way of introducing new knowledge without the necessity of coding it.

- **The characteristics of an ES**
  - The explanation facility of an ES explains how the system arrived at a certain conclusion or result.
  - Information from different sources is used to draw conclusions from difficult relationships.
  - 'Intelligent' behaviour of an ES provides solutions to problems.
  - Expert knowledge is created and made available by an ES.
  - An ES has the capability to deal with uncertainty.

- **Applications of an ES**
  - Organisations can use an ES to help budget, plan and coordinate prototype-testing programmes.
  - Provide legal advice by using rules and processes.
  - Hospitals and medical facilities are using an ES to assist them with a variety of medical conditions.
  - An ES developed specifically for government revenue authorities to provide tax advice.
  - Systems are developed to assist in economic development predictions.
  - Using an ES, organisations can make predictions of customer and market behaviour relatively accurately (more accurate predications as a DSS system because of the usage of the expert knowledge base).
  - Project managers can use an ES to manage specific projects.
  - Determines weaknesses with regard to workers and provides recommendations.

- **An example of an ES process:**

Financial organisations use an ES to deal with simple loan applications. The users enter the information into the system and the system checks the facts against a database to determine the applicant's creditworthiness. The system also performs calculations and compares criteria to determine if the security offered by the applicant is adequate for the loan.

3 GROUP SUPPORT SYSTEM (GSS)

3.1 What is a GSS?

A *GSS*, like groupware, allows users to ***work together on tasks***, ***adjust*** the same documents, ***plan appointments*** on each other's calendars, ***share files*** and ***databases***, have ***electronic meetings*** and ***develop readymade applications***.

The following diagram explains the GSS

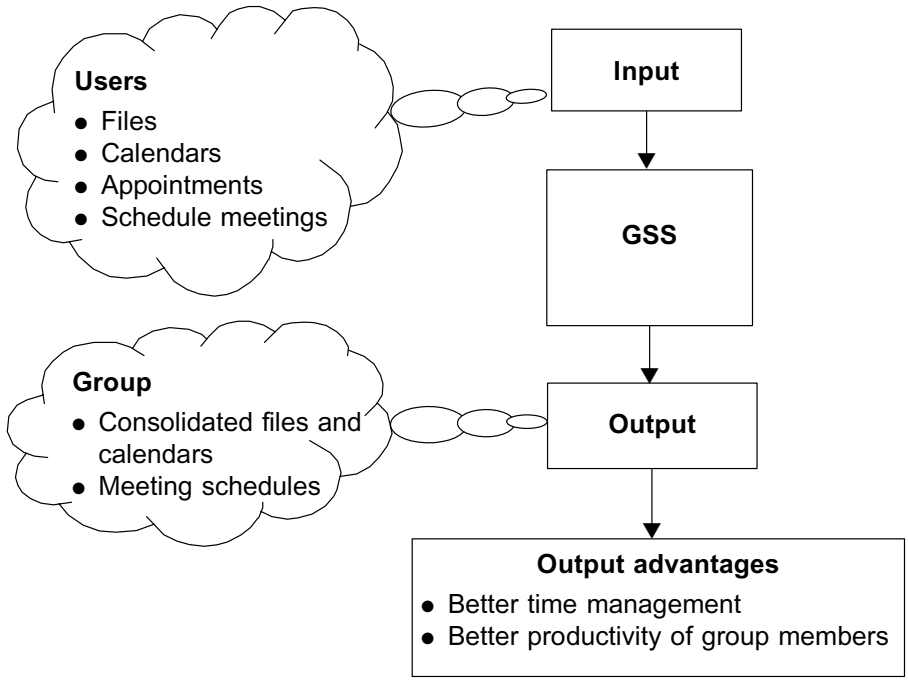


FIGURE 20.4: Explanation of the GSS

A GSS is typically easy to use and offers a variety of decision support. One type of GSS software, called *groupware,* is designed to help generate lists of decision alternatives and to perform data analyses.

3.2 GSS alternatives

- *Decision rooms*, which are ideal for situations in which decision makers are located in the same building or geographic area or decision makers are occasional users of the GSS approach.
- Another alternative is the *local area decision network*, which can be used when members are in the same geographic area and meet frequently.
- The *teleconferencing* alternative, on the other hand, can be used when decision frequency is low and the geographical location of group members is distant.
- The last alternative, *wide area decision network* is used for situations where decision frequency is high and the geographical locations of members are distant.

3.3 The characteristics of a group support system (GSS)

- *Parallel participation.* Everyone can input ideas at once, so in fact everyone is talking at once which leads to better productivity. This makes meetings shorter and saves time.
- *Special design.* A GSS incorporates the fact that unique procedures, devices and approaches are necessary in group decision-making.
- *Availability of data.* The minutes of normal meetings are sometimes incomplete or poorly written. Everything that is keyed in during a GSS meeting is saved and as soon as the meeting is over, a report of the ideas exchanged and decisions made, can be printed.
- *User friendly.* A GSS is easy to learn, understand and use.
- *Anonymity.* Each participant's input remains anonymous. Results are made visible on a central, public view screen so no one knows what input has come from whom. This

means harmful behaviour is reduced and dominant individuals are prevented from taking over the discussions.

- *Flexibility.* As decision-makers have different approaches and styles, a GSS needs to support their unique ways, but enhances compatibility with one another as well.

3.4 Applications for a GSS

- Capture, store and distribute memos, for example Lotus note or MS OneNote.
- Microsoft net meeting software supports multiparty calls.
- Microsoft Exchange allows users to access servers in different locations through the internet.
- Microsoft Outlook supports e-mail messaging, appointment scheduling and the sharing of documents.
- Video conferences are possible using a GSS.

Activity 20.1

Big Braai is a manufacturing organisation that specialises in the manufacturing of braai (barbeque) equipment. The company has a well-managed distribution network to distribute their products all over South Africa. The company currently makes use of various unrelated software in the different departments, namely design, inventory, production, sales and finance.

The geographical location of the warehouses, suppliers and distributors makes communication, meetings and performance measurement a huge challenge.

Recently, NJ Software Designers approached Big Braai and suggested a group support system.

As this will be an expensive project, Big Braai wants you, as one of the senior managers with experience in the IT environment, to explain the viability of a new group support system in the next management meeting.

Required:

a. Explain to the management of Big Braai what a GSS entails.
b. Explain to management why such a system would be beneficial to the organisation.

Feedback

a. Use the definition from the text, but explain a GSS to management by making it more practical.
b. Benefits to Big Braai

To answer this question, use the discussion on the characteristics and applications of a GSS in the text and apply it to the situation at Big Braai.

4 EXECUTIVE SUPPORT SYSTEM (ESS)

4.1 What is an ESS?

An *ESS* is a ***specialised decision support system*** that ***pools data*** from ***internal*** and ***external sources*** and make ***information available*** to ***senior management*** in a ***user-friendly*** manner (BPP-LM-CIMA E1 2009:62). It is used in strategic matters

and for high-level decision-making. An ESS provides top management with a way of tracking critical success factors.

You will learn more about strategy and critical success factors in Principles of strategy, risk & financial management techniques (MAC2602).

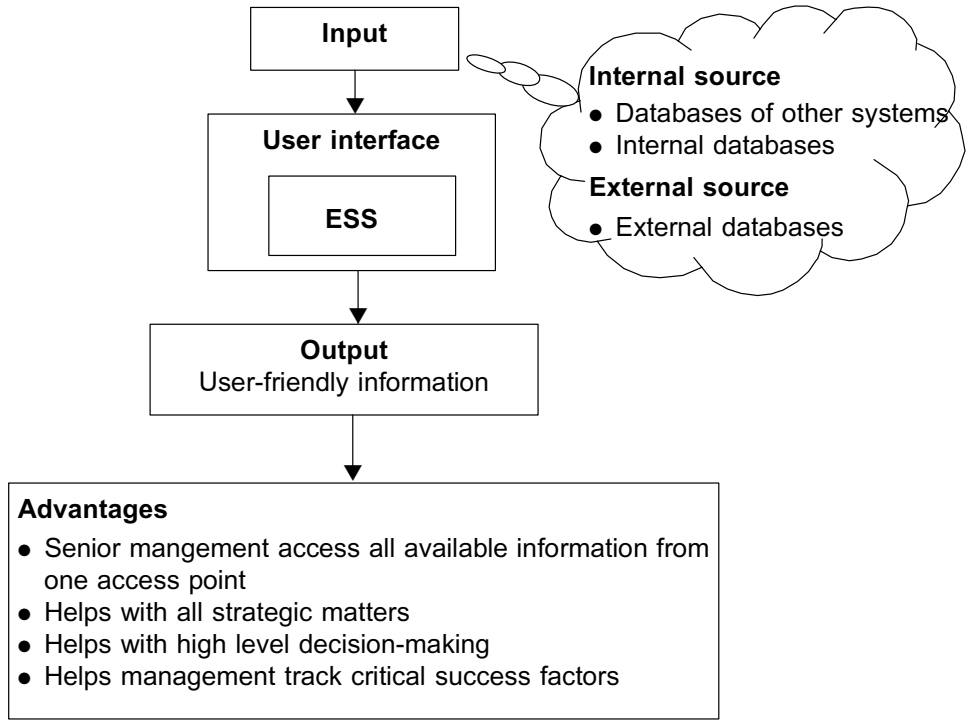


FIGURE 20.5: Explanation of the ESS

4.2 Characteristics of an ESS

- Management can drill down into company reports to establish how information has been produced and to get information that is more detailed.
- The ESS can be approached differently to suit individual executives for their benefit.
- No specific training is required because an ESS is user friendly.
- Using an ESS, management will track information quickly, filter data, deliver a summary of the company's information and save time.

4.3 Applications for an ESS

- Management can use an ESS to assist them in planning the acquisition of new equipment.
- Organisations can analyse merger possibilities using an ESS.
- An ESS takes full advantage of data mining, internet blogs, podcasts and dashboards. Management can gain an overall vision of a situation and an ESS helps them with effective strategic planning.
- An ESS supports strategic organisation, employment and control.
- Information from a wide variety of sources is gathered to help management in making informed top-level decisions.
- Owing to capacity and complexity, an ESS may become slow and hard to manage.

5 SUMMARY

To summarise: A KMS, CRM system and an ES use the knowledge of experts to improve performance and achieve the objectives of the organisation. A CRM system involves all customer activities and handle all information on them, while an ES behaves similarly to human experts, for example; an ES often determines credit limits for credit cards.

A GSS was developed to assist in the decision-making process by taking a DSS and adding software that allows it to be used by groups of individuals with a specific profile. A GSS is the combination of data, analytical models and user-friendly software in one single software system.

Using a user-friendly interface, an ESS offers management instant, relevant information that is easily accessible.

The next topic (topic 9) deals with electronic commerce and the application of an information system in the electronic commerce environment.

Self-assessment

a. Define a KMS.
b. Give four characteristics of a KMS.
c. Define a CRM system.
d. Describe nine applications of a CRM system.
e. Define an ES.
f. Describe the five characteristics of an ES.
g. Give eight applications for an ES and give one practical example.
h. Define a GSS.
i. Describe the seven characteristics of a GSS.
j. Give five applications of a GSS.
k. Define an ESS.
l. Describe nine characteristics of an ESS.
m. Give three applications of an ESS.

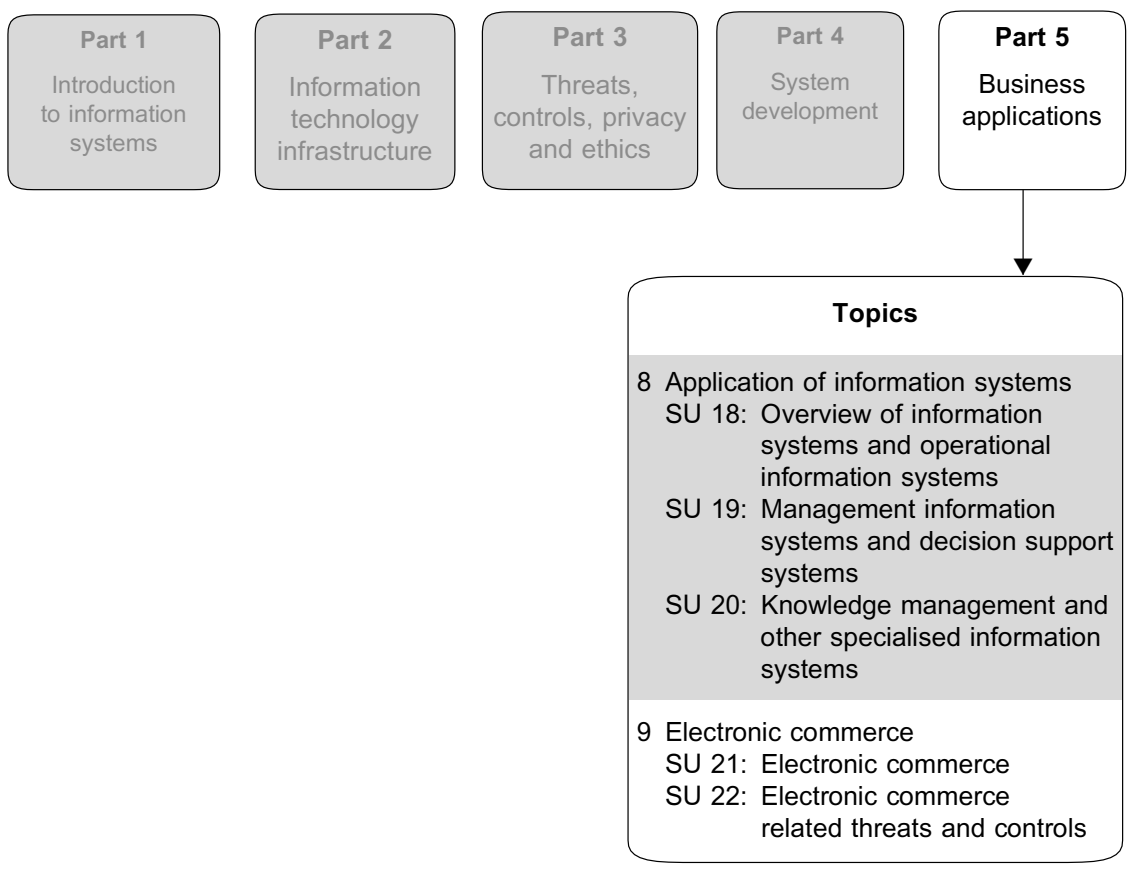
Electronic commerce

LEARNING OUTCOMES

After studying this topic, you should be able to

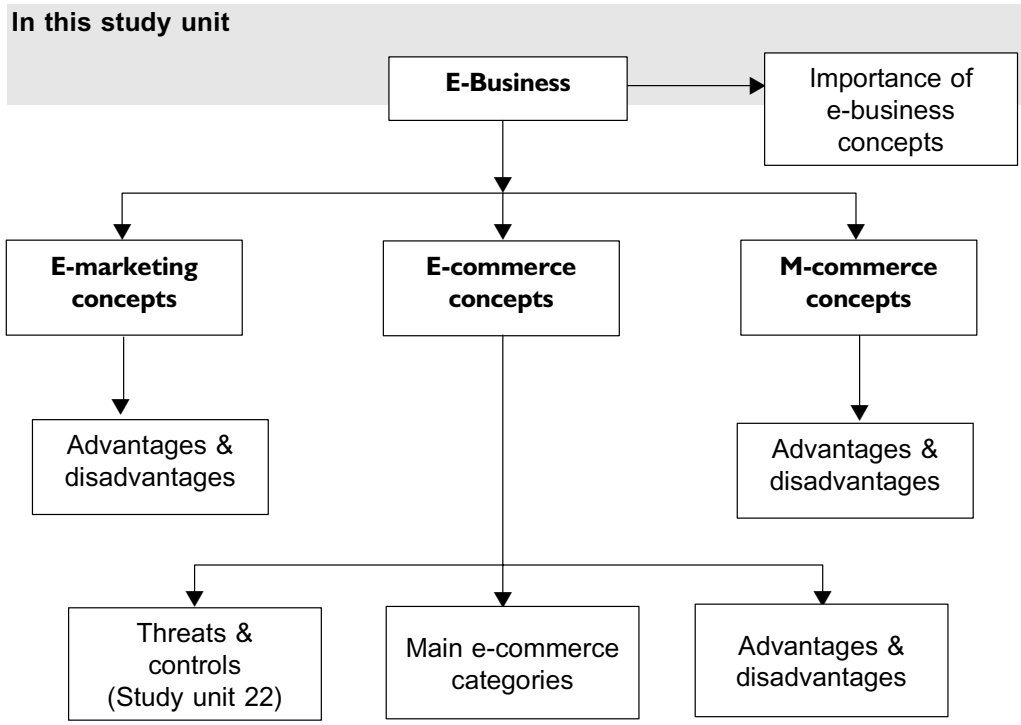
- define e-commerce and m-commerce terminology
- describe the importance of e-commerce concepts
- list and describe various e-commerce categories
- list and describe the advantages and disadvantages of e-commerce and m-commerce
- describe e-commerce threats
- describe controls to mitigate e-commerce threats

This topic consists of 2 study units



STUDY UNIT 21

Electronic commerce



1 INTRODUCTION

The rapid growth in the numbers of internet, cell phone and other mobile technology users has led to a boom in electronic and mobile commerce. This electronic environment levels the playing field between small and big organisations as it allows small organisations instant access to the global marketplace in which they can compete effectively. Most organisations can therefore no longer afford to ignore the opportunities created by this fast-moving environment. In this study unit, we will learn more about electronic commerce (e-commerce) and mobile commerce (m-commerce). To understand e-commerce and m-commerce better, the basic concepts of e-business and e-marketing will be explained as well. We will also learn about the different e-commerce categories and the advantages and disadvantages of both e-commerce and m-commerce. We will end this study unit with a discussion of the role the organisation's accounting function plays in the e-business environment.

2 THE IMPORTANCE OF KNOWLEDGE ABOUT E-BUSINESS CONCEPTS

E-commerce systems are becoming an important way of conducting business; therefore, an appropriate knowledge of e-business is required, for amongst others, the following reasons:

- Firstly and most importantly, a good knowledge of the organisation's e-commerce system and processes is required to be able to determine how each process impacts on different departments. This knowledge will help – for example – to mitigate threats.
- To ensure that proper policies are selected and adhered to. An example is accounting policies.
- Relevant knowledge will aid in understanding that relevant accounting records, audit evidence and audit trails need to be maintained.
- To ensure that relevant threats are mitigated, for example, by adequate firewalls, anti-virus software and an e-commerce business continuity plan.
- To ensure that the organisation complies with all relevant national and international laws and regulations.
- By understanding e-business concepts, you will identify the need for integrating an e-commerce system into the relevant financial or operational system. This will ensure efficient working of the system and that accurate, valid, relevant and timely information is produced by the system.

3 CONCEPTS, ADVANTAGES AND DISADVANTAGES

3.1 E-business, e-marketing, m-commerce and e-commerce

E-commerce and m-commerce are subsections of e-business, therefore to understand e-commerce and m-commerce we first have to have a basic understanding of what e-business is, as well as a basic understanding of e-marketing, one of the other subsections of e-business.

3.1.1 What is e-business?

E-business encompasses ***all business processes*** including ***research*** and ***development***, ***finance***, ***marketing***, ***manufacturing*** and ***human resource*** activities ***enabled by technology***. E-business connects an organisation with all its stakeholders, either internal (employees, management), connected (suppliers, customers, partners, etc) or external (government, pressure groups, etc).

The concept of electronic business (e-business) is much wider than just e-commerce. Many of the systems discussed in topic 8 are the practical application of e-business.

3.1.2 What is e-marketing?

Electronic marketing (e-marketing) uses ***electronic technologies*** to ***create product***, ***company*** and ***brand awareness*** to ***generate leads***, ***provide customer service*** and offer ***incentives*** such as ***discounts*** for ***online purchases***. E-marketing can include virtual advertising campaigns utilising social networks such as Facebook. Other examples of e-marketing are pay-per-click advertising (the organisation pays the hosting organisation every time their advertisement is clicked on a webpage), banner advertisements (an advertisement that is embedded on a webpage), e-mail marketing, and suchlike. E-marketing is a specialised marketing environment, which does not form part of this module. We will therefore only highlight some of the advantages and disadvantages of e-marketing.

Advantages	Disadvantages
Affordable price: E-marketing, in comparison with TV and print marketing gives small and large organisations access to a much larger market at a more affordable price than traditional marketing media such as television and so forth.	*E-marketing overload:* Web users are so flooded with banner ads, e-mail marketing, pop-up ads, and so on, and web pages are so overloaded with information, that web users ignore e-marketing advertisements and sometimes even find them annoying.
Global markets: E-marketing enables even small organisations to market their products and services to the global marketplace (BPP LM-CIMA E3 2010:316).	*Copying of marketing material:* An organisation's marketing material can be easily copied, as it is available on the web.
Personalised marketing: E-mails used in an e-mail marketing campaign can be personalised easily.	*Deliverability:* E-mail marketing is often viewed as spam and delivery of these marketing e-mails are blocked by the firewalls and spam management software of the targeted customer, especially if the targeted customer is using their work e-mail account. Banners and popup advertisements are also often blocked by organisations' internet security settings and ad blocking software.
Real time statistics: Statistics (eg unique visitors, repeat visitors, click-through rate, etc) relating to a marketing campaign are available in real time. This allows management to assess the effectiveness of an e-marketing campaign easily.	

3.1.3 What is m-commerce?

Mobile commerce, also known as m-commerce, is similar to e-commerce.

> *M-commerce* uses ***mobile devices*** such as ***smartphones***, ***cell phones***, ***PDAs*** (Personal digital assistant), ***tablet personal computers*** (eg Apple iPad, BlackBerry playbook) and suchlike to ***sell***, ***deliver***, ***service*** and ***pay*** for ***products*** and ***services***. The difference between m-commerce and e-commerce is that for e-commerce, the consumers use non-mobile devices such as laptops or desktop computers while m-commerce refers to commerce where customers use mobile devices.

A well-known and much used example of m-commerce in South Africa is cell phone banking that allows a consumer to use their cell phone to, among other things, check account balances, pay accounts, transfer funds between accounts and send money.

3.1.4 What is e-commerce?

> *Electronic commerce*, also known as ***e-commerce***, can be defined as ***technology-mediated exchange*** including the ***business process*** of ***selling, buying, delivering***, ***servicing*** and ***paying*** for products and services over ***computer networks***. The objective of e-commerce is to add and expand revenue streams, enhance relationships with customers and business partners and improve efficiency by using computer networks. It is important to remember that, although the largest part of e-commerce is conducted entirely electronically, there will be some manual interaction, as a service rendered or a product sold must be physically transported and delivered to a customer.

3.2 The main e-commerce categories

E-commerce can be divided in five main categories, differentiated according to the participants.

- *Business-to-business (B2B):* Both participants in the electronic transaction are organisations, for example when a wholesaler sells to a retailer. Depending on the e-commerce interface provided by the wholesaler, possibly through its extranet (refer to study unit 9), the retailer will be able to place orders, track the delivery of the orders, search for new products and so on, all online.
- *Business-to-consumer (B2C)*: This is one of the better-known e-commerce categories and involves an organisation selling its product or service directly to the public. You, a Unisa student, can for example electronically order and pay for your prescribed textbooks using www.kalahari.net or www.vanschaik.com. The business Van Schaik Bookstore sells textbooks, the product, directly to you, the Unisa student as customer. Bid or buy (www.bidorbuy .co.za) is another well-known example, where the sellers are often businesses, but is a C2C site as well.
- *Consumer-to-consumer (C2C)*: C2C is an online version of the classified pages of a newspaper where consumers can sell their products or services directly to other consumers. Gumtree and Junkmail are good examples of C2C e-commerce sites.
- *Consumer-to-business (C2B):* This is a less well-known and used category where a consumer can post his request for a product or service online, indicating the details for the product or service needed, that is, amount available, delivery dates and other specifications. Organisations can then review the consumers' requirements and bid on the project. Based on the bids, the consumer can then select the organisation that delivers the product or service.
- *E-government:* This allows governments to transact with organisations, their citizens and other governments. For example, SARS e-filing (www.sarsefiling.co.za) can be used by organisations and citizens to file their tax returns and make payments to SARS. South African citizens can enquire about their ID book, passport and permit application status and can verify their marital and ID status by using the Department of Home Affairs website (www.home-affairs.gov.za).

The interaction between consumers and businesses are shown in the matrix below adapted from BPP LM-CIMA E3 (2010:316).

		Buyer of service or product	
		Business	Consumer/receiver
		B2B	C2B
Seller of service or product	Business sell	Wholesaler selling to a retailer	Consumer to business www.Priceline.com
		B2C	C2C
	Consumer	Business sell to consumer, eg www.kalahari.net www.vanschaik. com www.kulula.com	Consumer to consumer, eg www.gumtree.co.za www.kalahariads.net

Activity 21.1

a. Log on to the internet and search for e-commerce websites not already mentioned in this study guide. Tip – think about online banking; where to buy tickets; online grocery shopping websites and so on.
b. Speak to your friends and family.
   - Enquire about which e-commerce websites they use.
   - Into which of the main categories would you categorise the e-commerce websites they use?

c. Do you or a family member submit your tax return electronically using the SARS e-filing system?
d. Visit http://www.jump.co.za/awards/2011/ to see the winners of the South African e-commerce awards.

3.3 Advantages and disadvantages of e-commerce and m-commerce

There are both advantages and disadvantages to using e-commerce and m-commerce for customers and organisations. Some of these are the following:

Advantages	Disadvantages
Direct customer relations: Organisations can interact directly with their customers thereby eliminating third parties (ie the intermediary). Through this direct contact with customers, organisations can obtain knowledge of their customers' buying behaviour and preferences. Using this intimate customer knowledge, customer service can be enhanced and customer loyalty increased. A further effect of the elimination of third parties is that services and products can be offered to customers at reduced cost.	*Product expectations not met:* Customers are not physically able to touch or see the products, as only pictures and/or descriptions of the products and goods are available on the business website. The customers' expectations of the product/service bought and then actually received may be materially different. This can cause customer complaints and negatively affect the organisation's reputation. The Consumer Protection Act no 68 of 2008 protects customers where products delivered are not the promised product.
Always open for business: While most traditional business are limited to working hours, organisations using e-commerce are open 24/7, ie 24 hours seven days a week. These prolonged shopping hours make it more convenient for their customers.	*Technological costs:* Appropriate hardware, software and staff with the correct technical skills are needed to set up and operate an effective e-commerce site. The costs to obtain and maintain these items can be material.
Access to global markets: Through e-commerce, organisations can reach customers anywhere in the world as long as the customer can have internet access. This allows an organisation to explore new markets and opportunities, as it is not limited to the geographical area in which the organisation has physical stores. Global access offers opportunities for developing organisations and countries and levels the playing field.	

Advantages	Disadvantages
Reduce costs: E-commerce can reduce labour costs, as no human interaction is needed for orders and in some instances deliveries (eg e-books, etc). This decreases costs for customer information, acquisition costs and marketing costs. As it can also reduce the need to keep finished goods in stock, the costs of carrying inventory can also be reduced. You will learn more about this in MAC2601 and MAC2602.	*Limited access:* Access is limited to customers who have the applicable technological knowledge to interact electronically, as well as access to the necessary hardware and software. If an organisation only interacts and markets electronically, it might exclude a large number of customers who do not have access to the internet and therefore the organisation.
Increased competitiveness: Owing to the reduction in costs, organisations may reduce selling prices; with a better knowledge of their customers, the competitiveness of an organisation in the marketplace can be increased. You will learn more about this in MAC2601 and MAC2602.	
Data accuracy: As customers enter their own data, for example product specifications, order quantities, delivery address and other corporate information, the data is more likely to be accurate as human-error on the part of the organisation is eliminated.	*Delayed delivery time:* In comparison to a physical shop, in an e-commerce transaction the customer does not receive the physical product immediately. This allows time for *buyer's remorse* and can result in customers cancelling a transaction.
Flow of information: Owing to the technological connections, the flow of information between the organisation and its customers is easier and the speed of the flow is increased.	
More choices available: Organisations do not necessarily need to keep stock. Organisations can purchase items as soon as they have the order from the customer.	

Specific m-commerce advantages and disadvantages

Over and above the already mentioned advantages and disadvantages (paragraph e) which are applicable to m-commerce, certain advantages and disadvantages specific to m-commerce are mentioned below.

Advantages	Disadvantages
Real-time information: Update on information is available immediately ie the latest sports score or stock prices or the breaking news story. Access to updated information is immediate, as the customer does not physically need to be in front of a computer connected to the internet.	*Screen limitations:* Mobile device screens are usually very small and can therefore only display limited text and pictures. Very few websites are geared to mobile users making it difficult to navigate.
Location: Owing to positioning system technology, such as GPS, organisations can target consumers in a specific geographical area.	*Input device limitations:* Small and limited keyboards makes entering text into a web page tiresome and usually with several errors.

Advantages	Disadvantages
Personalisation: A mobile device can be personalised to meet the user's specific needs and wants.	*Speed*: Mobile devices usually have less processing power and less bandwidth, making them much slower to use than desktop computers.

4 SUMMARY

In this study unit, we learnt the basic concepts of e-business and e-marketing, as this increased our understanding of e-commerce and m-commerce. We then looked in more detail at e-commerce and m-commerce, specifically the five main e-commerce categories, as well as the advantages and disadvantages of e-commerce and m-commerce. We also looked at the role of the organisation's accountant in an e-business environment.

In the next study unit, we will look at some of the unique threats faced by e-commerce and the possible steps an organisation can take to mitigate these threats.

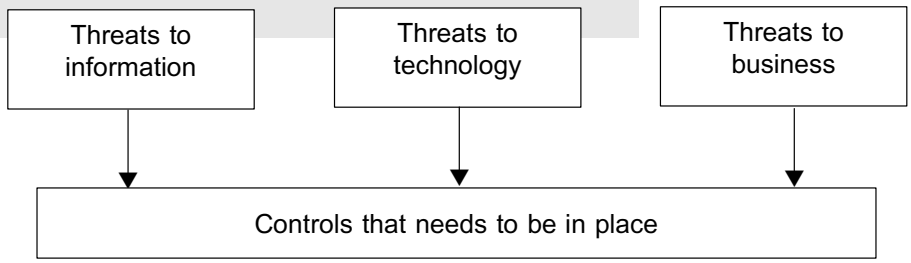
Self-assessment

a. List six reasons why it is important to have knowledge of e-business concepts.
b. Explain the concepts of e-business, e-marketing, m-commerce and e-commerce.
c. Give one example of e-marketing.
d. List and briefly explain the advantages and disadvantages of using e-marketing.
e. List and describe the five main e-commerce categories.
f. List and briefly explain the advantages of e-commerce.
g. List and briefly explain the disadvantages of e-commerce.
h. List and briefly explain the specific m-commerce advantages and disadvantages.

STUDY UNIT 22

Electronic commerce related threats and controls

In this study unit



1 INTRODUCTION

In study unit 21, we obtained an understanding of e-commerce, m-commerce and e-marketing. In study unit 10, we learnt about vulnerability, threats, exposures and risks, and focused on the possible threats that exist in a computerised information system. In study unit 11, we looked at controls to mitigate the threats to a computerised information system. These threats (study unit 10) and controls (study unit 11) are applicable to e-commerce and m-commerce as well. Although using e- and m-commerce may have major advantages for business and customers, their use also creates unique threats for both parties. In this study unit, we are going to look at some of the unique threats faced by e-commerce and the possible steps an organisation can take to mitigate these threats.

2 E-COMMERCE SPECIFIC THREATS

E-commerce exposes all participants in the e-commerce transaction to threats. Miller and Engemann (1999:719–721) classify these threats into three main categories, namely information, technology and business threats. The category classification is not clear-cut as some threats can be classified in more than one category. As technology advances, the threats to a computer system and e-commerce will advance as well. The threats discussed are therefore not a complete list.

Remember, e-commerce websites are also subject to the common information system threats as discussed in study unit 10.

2.1 Information threats

Information threats entail all ***threats associated*** with the ***availability of data*** and ***information on websites***, and the misuse and the possible corruption of such information and data (Miller & Engemann 1999:719–721).

Some examples of these information threats are the following:

- *Data alteration.* Data, such as price lists and catalogues, can be deliberately or accidentally altered, destroyed or copied by third parties who obtain authorised (customers or business partners) or unauthorised (hackers) access.
- *Copyright, patent, or trade secret infringements* are made easier with the product and service information available on websites. Examples include downloading music or movies from the internet without paying for them or third parties copying a product design from an e-commerce site and creating their own, *copied* product using the information obtained.
- *Incorrect website information* about products, services, or prices can result in financial loss, legal action, commercial embarrassment, or damage to an organisation's brand image. For example, an incorrect price list can result in an organisation selling products at a financial loss. One of the world's largest PC vendors, Dell's, Taiwan e-commerce website on 25 June 2009 offered 19-inch LCD monitors for only NT$500 instead of the intended price of NT$4 800 (Modine, 2009). A few days later, this website was struck by the same error again when it offered Dell Latitude E4300 laptops that normally cost NT$69 000 for just NT$18 500. Dell had to shut down its Taiwan e-commerce website until it fixed the issue and also had to compensate affected customers (Dan Nystedt, 2009).
- *Website vandalism* occurs when an organisation's corporate image or web messages are illegally changed resulting in commercial embarrassment or damage to an organisation's brand image.

2.2 Technology threats

Technology threats include ***threats involving*** the ***technologies*** used in the ***e-commerce*** process such as ***hardware***, ***software***, ***telecommunication*** and ***databases*** (Miller & Engemann 1999:719–721).

Some examples of technology threats are the following:

- A *denial-of-service attack (DoS)* involves flooding the target website with phony data, messages, or requests resulting in an extremely slow website response or crashing the e-commerce website completely. The aim of a DoS attack is to interrupt the organisation's normal business by preventing the effective functioning of the e-commerce website temporarily or indefinitely. Twitter was unavailable for a few hours on 6 August 2009 because of a DoS attack (Twitter, 2009). MasterCard's website was successfully crashed on 8 December 2010 when a group calling themselves Anonymous launched an orchestrated DoS attack on the MasterCard website. This DoS attack was part of a project called Operation Payback that was launched in support of Julian Assange, the founder of WikiLeaks, and the WikiLeaks website (Addley & Halliday, 2010).
- *Pharming* redirects a website's traffic from the actual website to a fraudulent website, without the organisation or the user's knowledge.
- An *inadequately designed website* makes navigating the website and finding the required information frustrating. Customer satisfaction will decrease resulting in customers buying from a competitor or an increase in customer complaints.
- *Insufficient hardware and/or bandwidth* that cannot deal with the internet traffic

requirements will make the e-commerce website slow to respond and frustrating for customers to use. As a result, an organisation can lose sales, as customers might prefer to use a competitor's website. See also the previous section on incorrect website info.

- *Flawed e-commerce system integration* with the other systems in the organisation, eg operational, financial, and so on, can lead to incorrect data being transferred between the different systems in the organisation. Flawed integration of product codes can for example lead to another product being manufactured and/or delivered to the customer rather than the one originally ordered by the customer
- Many organisations' websites contain *hyperlinks,* which take a user to a website page of another organisation. The organisation linking to the other organisation does not control the content of the page it is linked to and the content can change without the organisation's knowledge. If the content on the linked page contains defamatory material it can cause commercial embarrassment, damage to an organisation's brand image and even lawsuits. See also the discussion in the next section.

2.3 Business threats

Business threats include ***threats*** surrounding the ***internet*** relationship between ***customers*** and ***organisation***, other ***contractual relationships*** and the threats with regard to ***products*** and ***services marketed*** and ***distributed*** over the internet (Miller & Engemann 1999:719–721).

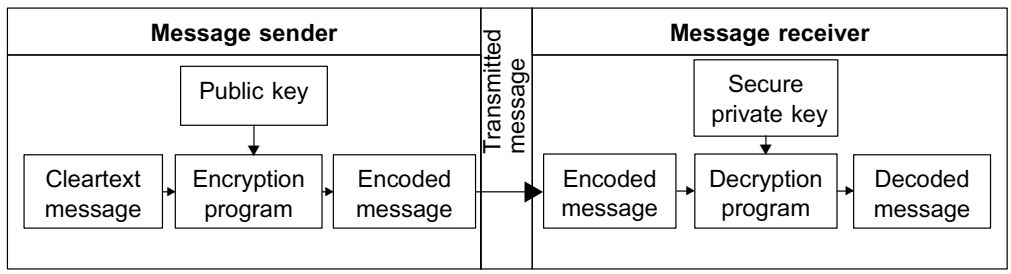
Some examples of business threats are the following:

- Through e-commerce, organisations can conduct business in different countries, each with their own laws and regulations. This creates *global legal and regulatory exposure,* as an organisation can unwittingly be in breach of these laws and regulations, exposing them to legal action or criminal prosecution. For example, a marketing sweepstake game can be legal in one country but illegal in another.
- An organisation's *reputation* can easily be destroyed or damaged through negative postings and media. Although most postings on a website are accurate, some of these postings contain dishonest and fabricated information or only partial information. Social networking sites, such as Facebook, make campaigns to discredit, rightly or not, an organisation very easily. Websites, such as Hellopeter (www.hello-peter.com), where customers can post complaints can damage an organisation's reputation if it receives a huge number of complaints or if complaints are not satisfactorily resolved.
- A number of organisations have e-commerce website message boards and chat rooms where third parties can publish comments. If these message boards and chat rooms are not properly managed and the necessary suitable disclaimers are not prominently stated, an organisation can be exposed to liability or commercial embarrassment as a result of a *slanderous* post by a third party.
- Organisations need to ensure that electronic contracts and transactions processed through the e-commerce website are binding and enforceable.
- Some organisations use *outsourced service providers* such as internet service providers (ISPs), application service providers (ASPs) and data hosting companies to provide all or some of their e-commerce information technology abilities. Organisations might also use other third-party organisations to complete the transaction with the customers, for example an online bookstore using a courier company to deliver books directly to a customer. Customers see these outsourced service providers as an extension of the organisation and any failure to deliver on the part of the service provider will reflect negatively on the organisation. This can cause commercial embarrassment, damage to an organisation's brand image or even lawsuits.

3 CONTROLS TO MITIGATE E-COMMERCE THREATS

Organisations cannot eliminate e-commerce threats altogether, but can implement controls to reduce exposure to these threats. The controls below are specifically applicable to an e-commerce website. *(The controls already discussed in study unit 11 are also applicable to e-commerce).*

- Install *firewalls, anti-virus, anti-spam and anti-spyware software* and update this software regularly with the latest patches and updates.
- E-commerce website *disclaimers* must be appropriately worded and prominently displayed on the applicable website pages. For example, appropriately worded disclaimers must be placed on pages containing hyperlinks.
- Install *reputation management software.* This is software that checks for specific keywords on the organisation and third parties' websites, blogs, forums, and so on, or contract a reputation management service provider, to do so on your behalf. Establish response strategies for attacks on the organisation's reputation. You can learn more about reputation management by logging onto www.brandprotect.com and downloading the 'Internet Reputation Management Guidelines, Building a Roadmap for Continued Success' document.
- Establish an e-commerce *business continuity plan* for all critical e-commerce components. For example, what back-up plan does an organisation have if its e-commerce server were to fail (crash), or be destroyed?
- Organisations must install *strong authentication processes*. These processes must entail more than just a simple password. For example, when logging onto Investec's online banking site, users receive a once-off security code which is valid for a limited time and sent to a predetermined cell phone number. Users must enter this security code with their normal password to log on to the online banking system.
- When encrypting an electronic message, the electronic message is converted into a form that can only be understood by the intended recipient. *Public-key encryption* is the most commonly used method for encrypting a message or authenticating a message sender. Public-key encryption consists of two matched encryption keys, a public and a private encryption key. The public and private keys correspond to one another but are not the same. The public key, used for encoding the message, is public and can be used by anyone, while the private key, used for decoding the message, is private and is only known to the party possessing the key (Hall 2011:540)



Source: Hall (2011:541)

- A *digital certificate* is a sender's public key that has been digitally signed by a trusted third party, called a certification authority (CA), (eg VeriSign, Thawte Digital Certificates, GeoTrust). A digital certificate is sent with the encrypted message to verify the message sender's authenticity. Digital certificates create trust between trading parties. Below is an example of myUnisa's digital certificate that was issued by VeriSign. You can view the digital certificate of a website by clicking on the locked padlock (see next bullet point) on a secure website and selecting ''view certificate''.

Source: Screenshot obtained from www.my.unisa.ac.za

- It is important to know that when we submit sensitive data, such as bank information, credit card details, passwords, login details, and so on, through an internet website that the transmitted data is secure and will not be misused or stolen. Organisations use secure sockets layer (SSL) protocol, an internet security protocol that encrypts the information transmitted, to secure sensitive data transmitted via their website. The *https* prefix before a website address indicates that the website implements SSL protocol. The locked padlock next to the URL address bar also indicates a secure website. When we click on the locked padlock, we can view the *digital certificate* of that website. The SSL protocols with a valid digital certificate indicate that the website is secure. SSL protocol provides both the organisation and the customer with peace of mind when transacting online as customers know their information is safe from misuse. It is extremely important to remember to process sensitive data on a secure website only, otherwise you can easily fall victim to identity theft, fraud, and so forth.

Source: Screenshot obtained from www.my.unisa.ac.za

Activity 22.1

a. Visit any e-commerce website and go to the checkout basket for online shopping or to the login page for internet banking. Do the following:
b. Determine whether this website is protected by SSL.
c. View the digital certificate and note down who the CA is.
d. For what term is the certificate valid?
e. By referring back to the information given above, decide whether the website is a secure website or not.
f. For more information with regard to security and privacy, go to the following website: http://www.microsoft.com/about/corporatecitizen/giving/programs/up/digitalliteracy/gbr/curriculum2.mspx and complete the Computer Security and Privacy module.

4 SUMMARY

In this study unit, we looked at the unique threats an organisation faces when using e-commerce and the steps and controls such an organisation can take to mitigate these threats.

Self-assessment

a. List and describe the three main e-commerce risk categories.
b. List and briefly explain four e-commerce information threats.
c. List and briefly explain six e-commerce technology threats.
d. List and briefly explain five e-commerce business threats.
e. Give an example of a denial-of-service attack (DoS).
f. Give an example where incorrect website information resulted in embarrassment for an organisation.
g. List and briefly explain the actions that an organisation can take to mitigate threats.

Bibliography

About us: Spyhecker. 2011, May 16. Retrieved June 10, 2011, from www.spyhecker.com: http://www.spychecker.com/spyware.html

Addley, E & Halliday, J. 2010, *December 8. "Operation payback cripples MasterCard site in revenge for WikiLeaks ban". The Guardian (London).* Retrieved July 05, 2011, from www.guardian.co.uk: http://www.guardian.co.uk/media/2010/dec/08/operation-payback-mastercard-website-wikileaks

Awad, EM & Ghaziri, HM. 2008. *Knowledge management.* New Delhi: Dorling Kindersley (India).

Baldauf, K & Stair, R. (2011) *Succeeding with Technology,* 4th Edition. Boston: Course Technology: Cengage learning.

Beth, G. 2011, April 1. *About us: Privacy Rights Clearinghouse*. Retrieved April 16, 2011, from Privacyrights.org: https://www.privacyrights.org

Boczko, T. 2007. *Corporate accounting information system.* Harlow, UK: Pearson Education Limited.

Bodnar, GH & Hopwood, WS. (2004). *Accounting information system* (9th ed.). Upper Saddle River, NJ: Pearson Prentice Hall.

BPP-LM-CIMA E1. 2009. *Enterprise paper E1: Enterprise Operations.* London: BPP Learning Media.

BPP-LM-CIMA E2. 2007. *Enterprise paper E2: Enterprise Strategy.* London: BPP Learning Media.

BPP-LM-CIMA E2. 2009. *Enterprise paper E2: Enterprise Strategy.* London: BPP Learning Media.

BPP-LM-CIMA E3. 2009. *Management Accounting – Risk and control strategy.* London: BPP.

BPP-LM-CIMA E3. 2010. *Strategic paper E3: Enterprise Strategy.* London: BPP Learning Media Ltd.

BPP-LM-CIMA P3. 2010. *Strategic paper P3: Performance Strategy.* London: BPP Learning Media Ltd.

BPP-LM-CIMA P3, & Strategy, MA. 2009. *BPP-LM-CIMA P3; Management Accounting Strategy.* London: BPP Publishers.

Carroll, J. 1995. *Computer security.* USA: Elsevier.

Coetzee, PG & Plant, K. 2010. *An introduction to internal auditing.* (3–88). Pretoria: The Southern African Accounting Association: 2010 North Gauteng regional conference proceedings.

Dan Nystedt, IN. 2009, July 8. *www.pcworld.com*. Retrieved July 14, 2011, from PC World: http://www.pcworld.com/businesscenter/article/168035/dell_apologizes_for_price_mishaps

Dull, RB, Gelinas, UJ & Wheeler, PR. 2010. *Accounting information system: foundations in enterprise risk management* (9th ed). International edition, Canada: Cengage Learning.

Eccles, MG, Julyan, FW, Boot, G & Van Belle, JP. 2000. *Principals of Business computing,* 5th Ed. South Africa: Juta & Co. Ltd.

Explainthatstuff – Laser printers. (nd). Retrieved April 19, 2011, from Explainthatstuff: http://www.explainthatstuff.com/laserprinters.html

FCIT. (nd). Retrieved March 5, 2011, from Florida Centre for Instructional Technology: http://fcit.usf.edu/network/chap4/chap4.htm

Filiol, E. 2005. *Computer viruses.* France: Springer.

Hall, J. 2011. *Accounting Information System.* 7th ed. Mason OH: Cengage Learning.

Hicks, D. 2005. *Phishing and pharming: helping consumers avoid internet fraud*. Brochure. Federal reserve bank of Boston. USA. *Autumn,* 29–30.

Howarth, A, Stanton, B & Sinclair-Hunt, M. 2005. *Information system management.* Harpenden, Hertfordshire UK: Select Knowledge Ltd.

HowStuffWorks. (nd). Retrieved January 5, 2011, from HowStuffWorks: http:// computer. howstuffworks.com/operating-system3.htm

http://en.wikipedia.org. (nd). Retrieved June 23, 2011, from Wikipedia: http://en.wikipedia.org/wiki/Computer_crimeI

FAC. 2007, June 30. *www.ifac.org.* Retrieved May 16, 2011, from https:// www.ifac.org/media/publications/8/...and.../defining-and-developing-an.pdf.

South African Institute of Chartered Accountants (SAICA), 2011. IAPS 1013 Electronic commerce effect on the audit of financial statements. *Handbook of International Quality Control, Auditing, Review, Other Assurance and Related Services Pronouncements*

Information Security Forum Homepage. *http://isf.b22222.com/*. Retrieved August 2011.

Janakiraman, VS & Sarukesi, K. 2006. *Decision support system.* New Delhi: Prentice-Hall of India.

Jonker, W & Petkovic, M. 2007. *Security, privacy and trust in modern data management.* New York: Springer.

Microsoft. (nd). *Microsoft Digital Literacy/Computer security and privacy.* Retrieved July 19, 2011, from Microsoft Digital Literacy: http://www.microsoft.com/about/ corporatecitizenship/citizenship/giving/programs/up/digitalliteracy/gbr/ curriculum2.mspx

Miller, HE & Engemann, KJ. 1999. Managing risks in electronic commerce. *Proceedings of the 30th Annual Meeting of the Decision Sciences Institute Volume 2* (pp. 719–721). New Orleans.

Modine, A. 2009, July 1. www.channelregister.co.uk. Retrieved July 14, 2011, from Channel Register: http://www.channelregister.co.uk/2009/07/01/dell_ordered_ to_honor_taiwan_monitor_mixup/

Moore, D. 2005. *Information ethics: privacy, property and power.* USA: University of Washington Press.

Nurjuliana, B. 2007. *Decision support system framework for feasibility study in construction projects.* Malaysia: University of technology of Malaysia.

Oak, M. (nd). *Buzzle.com/articles*. Retrieved May 25, 2011, from Buzzle.com: http:// www.buzzle.com/articles/types-of-computer-crimes.html

OpenProjects – Software definition. (nd). Retrieved April 13, 2011, from OpenProjects: http://www.openprojects.org/software-definition.htm

Pathway.s (nd) Retrieved October 13, 2011, from pathways: http/www.pathways.cu.edu.eg/subpage/training_courses/Problem%20Solving/Chapter2

Perry, B. 2009. *Enterprise Operations.* Oxford: Elsevier.

Power, DJ. 2002. *Decision support system: concepts and resources for managers.* Westport: Greenwood Publishing Group.

Rajeswari, R (nd). *www.articlesbase.com/ecommerce-articles*. Retrieved May 30, 2011, from Articlesbase: http://www.articlesbase.com/ecommerce-articles/mcommerce-and-its-applications-1011452.html

Ransome, R. 2005. *Instant messaging security.* US: Elsevier.

Rommey, MB & Steinbart, PJ. 2009. *Accounting information system.* 11th Ed. London: Pearson Education.

SAICA. 2009, June 30. *About us: South Africa Institute of Chartered Accountants.* Retrieved April 16, 2011, from SAICA website: http://www.saica.co.za

Sandra Cleary, MH. 2008. *Communication: a hands-on approach.* Landowne: Juta.

Savage, J. 2009. *A hybrid System with Symbolic AI and Statistical Methods for Speech Recognition*. Retrleved 10 13, 2011, from HITL Publications: http//www.hitl.washington.edu/publications/dissertations/Savage/28.html

Security Solutions/news/Unsecured USB Flash Drives Still a Risk, Survey Shows. 2008, April. Retrieved August 4, 2011, from Security Solutions: http://securitysolutions.com/news/unsecured-usb-risk-0422/

Software Methodologies. (2009, AprIL 10). Retrieved October 12, 2011, from Software Methodologies: http://softwaremethodologies.blogspot.com/2009/04/advantages-disadvantages-of-various.html

Solomon, D. 2006. *Foundations of computer security.* London: Springer.

Stair, R & Reynolds, G. 2008. *Principles of information system.* 8th ed. Canada: Thomson Course Technology.

Stair, R, Reynolds, G & Chesney, T. 2008. *Principles of business information system.* North Way: Course Technology: Cengage Learning.

Techterms. (nd). Retrieved January 5, 2011, from Techterms: http://www.techterms.com/definition/compression

Twitter. 2009. Retrieved July 5, 2011, from http://status.twitter.com: http://status.twitter.com/post/157191978/ongoing-denial-of-service-attack

Van Wyk, C. 2006. The development of an education management information system from a sense making perspective and the application of quantitative methods to analyse education data sets. University of Stellenbosch.

Wessels, P, Grobbelaar, E, Mc Gee, A & Prinsloo, G. 2007. *Information system in a business environment.* 4th ed. Durban: LexisNexis.

Wessels, P, Mc Gee, A, Prinsloo, G, Mc Gee, E & Van der Poll, H. 2010. *Information system in a business environment.* 5th ed. Durban: LexisNexis.

WikiAnswers What is the difference between primary memory and secondary memory? (nd). Retrieved 04 23, 2011, from WikiAnswers.com: http://wiki.answers.com/Q/What_is_the_difference_between_primary_memory_and_secondary_memory

Wikibooks Communication mediums. (nd). Retrieved July 7, 2011, from Wikibooks: http://en.wikibooks.org/wiki/Communication_Systems/Communication_Mediums

www.absa.co.za. (nd). Retrieved July 27, 2011, from ABSA internet banking: https://ib.absa.co.za/ib/ib.jsp

ZSecurity. (nd). Retrieved July 28, 2011, from http://www.zsecurity.com:http://www.zsecurity.com/articles-rootkits.php