

Unit 6: Manage Information Systems

Unit reference number: F/506/1951

QCF level: 4

Credit value: 6

Guided learning hours: 30

Unit summary

Information is the most valuable resource that an organisation possesses. The effective gathering, protection, analysis, processing and dissemination of information is vital to the success of any organisation. As globalisation and the 24-hour economy develop and increase, organisations must ensure that their information systems are reliable, efficient and able to cope with rapid change.

Organisations whose information systems previously dealt purely with data processing have now introduced those supporting strategic management and decision support. Managers at all levels need appropriate and timely information to plan successfully in the short, medium and long term, and that information can have many sources and destinations. As organisations diversify and centralise, information also needs to be available to non-managerial staff in a variety of locations. The logical conclusion is that an organisation is now completely dependent on the effectiveness of its information systems in order to survive and thrive in the 21st century business environment.

In this unit you will learn about the various uses of information systems and how system users and stakeholders interact with hardware, software and information. You will develop skills to analyse and review information system effectiveness and identify where system updates and developments are required to meet the ongoing needs of an organisation. You will demonstrate your ability to manage information systems which includes hardware, software, people and data. This unit requires you to demonstrate your understanding of change relating to information systems as well as the impact these changes have on individuals, teams and the organisation as a whole whilst remaining compliant with relevant and current legislation.

Learning outcomes and assessment criteria

To pass this unit, the learner needs to demonstrate that they can meet all the learning outcomes for the unit. The assessment criteria outline the requirements the learner is expected to meet to achieve the unit.

Learning outcomes	Assessment criteria
<p>1 Understand the management of information systems</p>	<p>1.1 Explain the uses of an information system</p> <p>1.2 Describe typical information system interfaces</p> <p>1.3 Analyse the implications of system updates and system developments to an organisation</p> <p>1.4 Analyse the use of stakeholders' feedback on the effectiveness of an information system</p> <p>1.5 Evaluate the implications of data protection requirements for the management and use of an information system</p>
<p>2 Be able to set up information system processes</p>	<p>2.1 Develop standard operating procedures for administrative processes that meet organisational and legal requirements</p> <p>2.2 Implement management processes that are capable of identifying and resolving problems</p> <p>2.3 Analyse users' training needs for an information system</p>

Learning outcomes	Assessment criteria
<p>3 Be able to manage an information system</p>	<p>3.1 Monitor the quality of information against agreed key performance indicators (KPIs)</p> <p>3.2 Update information systems in line with business and users' needs</p> <p>3.3 Provide training and support in the use of information systems to users and stakeholders</p> <p>3.4 Manage problems in the information system in a way that minimises disruption to business</p> <p>3.5 Evaluate the effectiveness of an information system</p> <p>3.6 Make recommendations for improvements that will enhance the efficiency of an information system</p> <p>3.7 Adhere to organisational policies and procedures, legal and ethical requirements in the management of an information system</p>

Unit amplification

AC1.1: Explain the uses of an information system

- *Information systems:*
 - Definition which includes the differences between data and information
 - Purpose: operational support, e.g. monitoring and controlling activity; analysis, e.g. to identify patterns or trends; decision making, e.g. operational, tactical, strategic; gaining commercial advantage; desired results
 - Features: data; people; hardware; software; telecommunications
 - Uses: capture; transmit; store; retrieve; manipulate; display
- *Types of information system:* management information systems; others, e.g. marketing, sales performance, competitors); financial, e.g. financial costs, investment returns; Human Resources (HR), e.g. staffing, professional development; Customer Relationship Management (CRM); open and closed systems

AC1.2: Describe typical information system interfaces

- *Typical information system interfaces:* definition; function; interface types, e.g. hardware, software, people, telecommunications
- *Features of a typical information system interface:* easy; efficient; user-friendly; logical

AC1.3: Analyse the implications of system updates and system developments to an organisation

- *System updates and developments:* definition; differences between updates and developments; hardware, e.g. increasing power, increasing capacity, sophistication of computer platforms, sophistication of communication technologies; software
- *Reasons for systems updates and developments:* external pressures, e.g. changing regulatory and legal frameworks, keeping up with competitors; enhanced business opportunities, e.g. increasing globalisation, potential for outsourcing, improving customer service; internal factors, e.g. revised policies, procedures and processes, additional information requirements; organisation growth; improving staff productivity and performance
- *Impact:* cost; procedures; staff, e.g. upskilling/training, dealing with redundancies; integration of legacy systems; security; legal requirements, e.g. data protection, copyright; system 'downtime'; continuity of service
- *Benefits:* cost reductions; increased profitability; efficiency; improved customer service

AC1.4: Analyse the use of stakeholders' feedback on the effectiveness of an information system

- *Stakeholders*: internal, e.g. system users, management, information system developers, technical support; external, e.g. customers, product suppliers, service providers, contractors, regulatory bodies
- *Stakeholder feedback*: feedback objectives, e.g. system, teams, business; desired outcome(s); feedback mechanisms; feedback forums, e.g. individuals, focus groups, organisations; frequency; response deadlines; responses
- *Measuring system effectiveness*: system objectives, e.g. desired system outcomes, actual system outcomes; efficiencies, e.g. cost, time, resources; handling information, e.g. input, processing, output, reporting, analysis, storage; system operations, e.g. interfaces, logical processes, usability, technical support; issues, e.g. hardware, software, people, processes, data; recommendations for improvement
- *Use of stakeholder feedback*: value stakeholder opinions; timely resolution of issues; inform change; communication of feedback outcomes, e.g. meetings, reporting, presentation, publishing; staff development

AC1.5: Evaluate the implication of data protection requirements for the design of an information system

- *Legal issues*: relevant and current data protection legislation, e.g. Data Protection Act 1998, Freedom of Information Act 2000; other relevant legislation, e.g. Computer Misuse Act 1990
- *Ethical issues*: codes of practice, e.g. use of email, internet; 'whistle blowing'; organisational policies; information ownership
- *Operational issues*: security of information; backups, e.g. hardware, peripherals, software, storage media, local storage, remote storage, cloud storage; organisational policies, procedures and processes; staff training
- *Implications of data protection*: access; information security, e.g. internal threats, external threats, data corruption; cost; reputation; effects on business sustainability
- *Managing risk*: cyber-crime, e.g. diverting financial assets, communications sabotage, intellectual property theft, denial of service attacks; preventive technologies, e.g. firewalls, access control methods, secure payment systems; disaster recovery