

DIGITAL

Mo Everett
Sonia Stuart

DIGITAL SUPPORT SERVICES: CORE
DIGITAL BUSINESS SERVICES: CORE

T-LEVELS

THE NEXT LEVEL QUALIFICATION

DIGITAL SUPPORT & BUSINESS SERVICES

CORE

Mo Everett
Sonia Stuart



'T-LEVELS' is a registered trade mark of the Department for Education.

'T Level' is a registered trade mark of the Institute for Apprenticeships and Technical Education. The T Level Technical Qualification is a qualification approved and managed by the Institute for Apprenticeships and Technical Education.

Acknowledgements

page 1 © Svitlana – stock.adobe.com, page 59 © pressmaster – stock.adobe.com, page 60
© Antonioguillem – stock.adobe.com, page 63 © KONSTANTIN SHISHKIN – stock.adobe.com,
page 65 © amnaj – stock.adobe.com, page 68 © New Africa – stock.adobe.com, page 70 © CG Bear –
stock.adobe.com, page 73 © NicoElNino – stock.adobe.com, page 91 © Elegant Solution – stock.adobe.com,
page 100 © Prostock-studio – stock.adobe.com, page 106 Claudio Divizia - stock.adobe.com, page 112
© kiri – stock.adobe.com, page 153 © Seventyfour – stock.adobe.com, page 163 © Chansom Pantip –
stock.adobe.com, page 166 © sofiko14 – stock.adobe.com, page 188 © Zerbor – stock.adobe.com,
page 189 © Reneshia – stock.adobe.com, page 216 © Andrey Popov – stock.adobe.com, page 236 © Michael
Traitov – stock.adobe.com, page 250 © rukanoga – stock.adobe.com, page 270 © everythingpossible –
stock.adobe.com, page 272 © leszekglasner – stock.adobe.com, page 276 © DC Studio – stock.adobe.com,
page 279 © Gorodenkoff – stock.adobe.com, page 281 top © Elegant Solution – stock.adobe.com bottom
© MasSept/Shutterstock.com, page 285 © Kostiantyn – stock.adobe.com, page 286 © Mandarin457 –
stock.adobe.com, page 287 © Kostiantyn – stock.adobe.com, page 288 © Aleksandr Bryliaev –
stock.adobe.com, page 289 © Irinabunger - stock.adobe.com

Every effort has been made to trace all copyright holders, but if any have been inadvertently overlooked, the Publishers will be pleased to make the necessary arrangements at the first opportunity.

Although every effort has been made to ensure that website addresses are correct at time of going to press, Hodder Education cannot be held responsible for the content of any website mentioned in this book. It is sometimes possible to find a relocated web page by typing in the address of the home page for a website in the URL window of your browser.

Hachette UK's policy is to use papers that are natural, renewable and recyclable products and made from wood grown in well-managed forests and other controlled sources. The logging and manufacturing processes are expected to conform to the environmental regulations of the country of origin.

Orders: please contact Hachette UK Distribution, Hely Hutchinson Centre, Milton Road, Didcot, Oxfordshire, OX11 7HH. Telephone: +44 (0)1235 827827. Email education@hachette.co.uk Lines are open from 9 a.m. to 5 p.m., Monday to Friday. You can also order through our website: www.hoddereducation.co.uk

ISBN: 978 1 3983 4679 6

© Maureen Everett and Sonia Stuart 2022

First published in 2022 by
Hodder Education,
An Hachette UK Company
Carmelite House
50 Victoria Embankment
London EC4Y 0DZ

www.hoddereducation.co.uk

Impression number 10 9 8 7 6 5 4 3 2 1

Year 2026 2025 2024 2023 2022

All rights reserved. Apart from any use permitted under UK copyright law, no part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, or held within any information storage and retrieval system, without permission in writing from the publisher or under licence from the Copyright Licensing Agency Limited. Further details of such licences (for reprographic reproduction) may be obtained from the Copyright Licensing Agency Limited, www.cla.co.uk

Cover photo © BalanceFormCreative - stock.adobe.com

Illustrations by Aptara Inc.

Typeset in India by Aptara Inc.

Printed in Bosnia & Herzegovina

A catalogue record for this title is available from the British Library



Contents

Guide to the book	iv
-------------------------	----

THE CORE

Core element 1	Business context	1
Core element 2	Culture.....	59
Core element 3	Data	73
Core element 4	Digital analysis.....	100
Core element 5	Digital environments.....	112
Core element 6	Diversity and inclusion	153
Core element 7	Learning	166
Core element 8	Legislation	188
Core element 9	Planning	216
Core element 10	Security	236
Core element 11	Testing.....	270
Core element 12	Tools	279
	Core skills	295
	Assessment.....	303
	Glossary	317
	Index	325

ONLINE MATERIAL

Pathway Core element 1: Careers within the digital support services sector

Pathway Core element 2: Communication in digital support services

Pathway Core element 3: Fault analysis and problem resolution

Access this content at www.hoddereducation.co.uk/digitalsupportservices/pathwaycore

Guide to the book

The following features can be found in this book.

Learning outcomes

Summaries of the knowledge outcomes that you need to learn in each content area.

Case study

Scenarios that place content into real-world contexts.

Key term

Definitions of key terms.

Test yourself

Short questions designed to test your knowledge and understanding.

Industry tip

Tips and advice to help you in the workplace.

Assessment practice

Knowledge-based practice questions to help you to prepare for the core exams.

Important point

Important points that you need to be aware of.

Project practice

Short scenarios and focused activities reflecting one or more of the tasks that you will need to undertake during completion of the employer set project.

Activity

Short activities that encourage you to apply the knowledge and skills covered in the Student Book.

Research

Research-based activities – either stretch-and-challenge activities, enabling you to go beyond the course, or industry placement-based activities encouraging you to discover more about your placement.

Core element 1: Business context

There are many factors, both internal and external, that affect every business, and they can have both a positive and a negative impact on the business. These factors are what makes up the business environment. Factors include human resources, the quality of management, finance, marketing, logistics, research, design and development, as well as the political climate and environmental concerns. The range of factors that can affect the business environment is vast and within this unit you will learn about their common features and whether they are internal or external factors.

There are different types of organisations in a wide variety of sectors. All these businesses need, and must be able to use, digital technologies. Implementing and extending the use of digital technology requires careful strategic and project planning. This means considering not only the hardware, software and storage requirements, but also the needs of the end user, the business and its stakeholders, as well as social, political and legal factors.



Learning outcomes

In this core element you will learn about:

- 1.1** Types of organisations and stakeholders within the business environment
- 1.2** Key factors that can influence the business environment
- 1.3** The measurable value of digitalisation to a business
- 1.4** The influence and impact of digitalisation within a business context and market environment
- 1.5** The role of technical change management in digital operational integrity
- 1.6** The components of technical change management
- 1.7** Factors that drive change and a range of methods organisations can apply in response to change
- 1.8** The steps organisations take to respond to change
- 1.9** The measurable value of digital service to customers and end users
- 1.10** The considerations and value of meeting customer and end user needs within a business context
- 1.11** Risks and implications within a business environment
- 1.12** The purpose and applications of codes of conduct within a business
- 1.13** Types of hackers and the implications of hacking and non-compliance with a code of conduct

1.1 Types of organisations and stakeholders within the business environment

Organisation types

Public

The public sector includes any organisation that is owned and operated by government agencies. Examples of public sector organisations include the local council, Her Majesty's Revenue Collector (HMRC), the passport office, libraries and schools. Although it can be argued that these organisations provide a service, they are not classified in the same category as the tertiary sector that provides services such as banks, supermarkets, cinemas and hairdressers.

Private

Private sector organisations are owned by individuals and are driven by making a profit. This profit benefits the owners of the organisations, their shareholders and investors. Private sector organisations are usually financed by money from shareholders and bank loans. Categories that fall within the private sector are outlined below.

Small or medium enterprises

Businesses with financial turnover, assets and/or a number of employees that are below a certain level are classified as small or medium-sized enterprises (SMEs). The criteria for determining whether a business is an SME varies between countries and in some instances between industries. SMEs have full-time employees to manage their data and information technology (IT) infrastructure. Typical job titles for these people would include system administrator, network manager or IT manager.

Large enterprises

This type of business has a more comprehensive business model and will often have full-time staff who manage the applications and/or part of the IT infrastructure. In addition, they exceed the number of employees, financial turnover and assets that are the benchmark for SMEs.

Non-governmental organisations

These are non-profit organisations that function independently of the government. They are sometimes referred to as 'civic societies' and are organised at local community, national and international levels to serve a social or political goal such as causes for the environment or humanitarian reasons. Some

non-governmental organisations (NGOs) rely on volunteers as their workforce, while others have paid staff. There are two groups of NGOs.

- ▶ **Operational** – these NGOs focus on the design and implementation of development projects.
- ▶ **Advocacy** – these NGOs promote and/or defend a specific cause and seek to influence public policy.

There are some NGOs that come under both categories. Examples include the support of human rights, improving health and living conditions, or encouraging political participation.

NGOs rely on funding from sources such as:

- ▶ membership fees
- ▶ sales of goods and services
- ▶ private donations
- ▶ grants.

Voluntary/charity

These are organisations whose purpose is to benefit society, often without profit as a motive and with little or no government intervention at all. Any money raised or earned by these organisations is usually invested back into the community or the organisation itself. Charities are registered with the Charity Commission and operate purely for charitable purposes. In order to be able to register with the Charity Commission a charity must be:

- ▶ established for a charitable purpose, in other words to provide public benefit
- ▶ subject to the High Court's charity law jurisdiction.

Charities are eligible for various tax exemptions as they do not pay tax on income from donations or rental of premises.

Not for profit

People often confuse 'not for profit' with charities. Not for profit means that the organisation's activities are not for the financial benefit of any individual or board of directors. There are various types of not-for-profit organisations and they do not have a legal structure. The main difference is whether the organisation is eligible to register as a charity with the Charity Commission. The benefit of being a not-for-profit organisation is that there are fewer restrictions on the types of charitable work they can carry out. They are not under the same restrictions as those registered with the Charity Commission.

Stakeholder types

A stakeholder is someone who has an interest in the business, and who can either affect or be affected

by the business's operation and performance. Stakeholders can be internal or external to a business.

Internal

This next section outlines who the internal stakeholders of a business can be.

End users

The internal end users can be owners, the board of directors, employees and departments.

Owners

The owners can be the same people who direct the business and have control over the day-to-day operations and processes. Or they may employ a manager to carry out that role for them or even a board of directors. Regardless of the size of the business, the owner(s) has overall control and decides whether to delegate important functions to others. The owner(s) can earn a monthly wage but is not an employee.

Board of directors

These are people who are elected to represent the shareholders' interests. Every public company must have a board of directors that consists of members who are internal and external to the business. They make decisions about the employing and sacking of personnel, **dividend policies** and pay-outs, and executive compensation. They are also responsible for helping a business set its broad goals and ensuring that the business has adequate and well-managed resources.

A board of directors should represent management and the shareholder interests. An internal member of the board of directors represents the interests of the major shareholders, managers and employees, and has experience within the business that adds value.

They do not normally receive a fee for their activities as they are already a high-level executive, a major shareholder or union representative. External directors are not involved in the day-to-day running of the business and are paid for being a board member. Their role is to bring an independent view to the setting of goals, and to settle any disputes.

Key term

Dividend policy: contains the structure of the pay-outs made to shareholders based on how many shares a shareholder has and the profits made by the business.

Employees

These are people who have an employment contract.

A person can be employed but have a different tax status. It is the responsibility of the employer to establish an employee's status in employment and tax law.

All employees are classified as workers and have additional employment rights and responsibilities that do not apply to people who are workers but not employees (such as contractors or suppliers who come to the business premises). These rights include:

- ▶ statutory sick pay
- ▶ statutory maternity, paternity, adoption and shared parental leave and pay (workers only get leave and not pay)
- ▶ minimum periods of notice if their employment is coming to an end
- ▶ protection against unfair dismissal
- ▶ the right to request flexible work hours
- ▶ time off for emergencies
- ▶ statutory redundancy pay.

Some of these rights are only available after an employee has worked for the business for a set period of time. The timescales are usually included in the contract of employment.

Departments

These are parts of a larger business/organisation/company. They are organised around their different roles. Typical businesses may consist of the following departments:

- ▶ accounting and finance
- ▶ administration
- ▶ human resource management (HR)
- ▶ research and development (R&D)
- ▶ purchasing
- ▶ production
- ▶ sales
- ▶ customer service.

External

External stakeholders do not have a direct relationship with a business. An external stakeholder is normally a person and/or company that is affected by the operations of the business. For example, a company that emits high levels of carbon emissions affects the local area by increasing pollution. In this case, the local area and the people who live there are external stakeholders.

An external stakeholder may also have a direct effect on the business without having any direct link with it. The government is an external stakeholder. Governments will initiate changes in policies (e.g. changes to the acceptable level of carbon emissions); these changes can have an effect on the operations of a business and, in this case, how it controls its carbon emissions in order to comply with legislative policy.

Customers/consumers

Customers are people/organisations who buy, pay for or recommend products and/or services. Customers can also be people who are internal to a business. Customers have an interest in the quality and availability of goods and/or services.

Consumers are also interested in the quality and availability of products and/or services. A customer will pay for a product and/or service but not necessarily be the person who consumes it. A consumer is the person who uses the product and/or service. For example, a mother purchases sweets for her children but only her children eat the sweets. The mother is the customer, and her children are the consumers. A man who buys a car to drive himself. He is the customer and the consumer.

Clients

A client is a person or company that pays for professional support or services from another company. For example, a person who pays for the services of a solicitor is a client, a company that pays for technical support from an IT company is a client. Clients have an interest in the quality and availability of the services provided by a business.

Direct/indirect competitors

Every business can directly or indirectly affect the performance of its competitors.

- ▶ **Direct** competitors sell similar products and/or services as another business. For example, two fast food burger chains are direct competitors.
- ▶ **Indirect** competitors also sell similar products and/or services in the same sector as another business, but they are sufficiently different in that they can act as a substitute for the product and/or service that a company is selling. For example, a pizza restaurant is an indirect competitor to a burger chain.

All businesses have an interest in what is happening with other businesses within the sector they are functioning.

Outsourced services and suppliers

Outsourcing is when a business hires another business to carry out tasks, handle operational activities or provide services on its behalf. The outsourced company is sometimes referred to as a service provider or a third-party provider. For example, a business may outsource the IT services from another company, instead of having an in-house IT department.

Suppliers provide goods and/or services to another business. They have an interest in how the business they are providing goods and/or services to is performing. This is because they want regular orders from the business and to receive prompt payment. They can also influence a business's operation through the prices they charge for the products and/or services they provide, changes to delivery times, changes to the quality of their products/services and changes to any credit agreements.

Shareholders

A shareholder is a person, institution or company that owns at least one share of a company's stock. They are subject to **capital gains/losses** and/or **dividend payments** on a business's profit. Shareholders also have the right to vote at shareholder meetings to approve, for example, the members of the board of directors, the distribution of dividends or mergers with other businesses.

Investors

These are people, companies or other entities that provide funds with the expectation that they will get more money back than they invested. Investors may provide loans, buy shares, or act as guarantors, for example to pay creditors or provide labour. Investors can make a commitment in exchange for a fixed return (dividends or interest), to have a share in the business, and can sell their investment later on, in order to make a profit. If two or more companies commit to a joint project/venture and contribute to the overall costs, they are all investors.

Key terms

Capital gains/losses: the profits or losses from selling an asset, financial investments, real estate and so on.

Dividend payments: money paid regularly by a company to the shareholders. These are paid out from the profits of the company.

Funders

These are wealthy organisations or individuals that provide financial backing for projects and/or business ventures. They offer financial support through a grant, an investment or a loan. They have an interest in how the business performs because of the money they have provided to support it.

Government

Government operates on local, national and international levels.

Local

Local authorities (also known as town and district councils) should have a strategy in place that enables them to understand the changing demands of their local communities' habits and demands. This means that they can support local businesses in adapting and creating new business opportunities. The failures of businesses within a local community have a knock-on effect, with the local population having high unemployment. This means that there would be a lack of money to spend in shops and also more people needing benefits.

National

National government is made up of politicians who run a country for the benefit of the population. One of their roles is to encourage businesses to invest and create jobs. The laws that they introduce can have a negative or positive impact on businesses and may cause businesses to invest in other areas or even countries. Governments have to consider the employment rights of current and/or potential employees and not just the development opportunities of the businesses.

Governments have an interest in businesses performing well, so that they can:

- ▶ provide goods and services for the entire country
- ▶ create jobs and improve the wealth of the country's population
- ▶ pay corporation tax.

They can influence the operating of a business by:

- ▶ offering grants to encourage businesses to move to depressed areas where employment prospects and wealth are low
- ▶ introducing or repealing laws that have an impact on businesses
- ▶ increasing or decreasing the amount of corporation tax that businesses have to pay.

International

International government is where the governments of different countries come together and set out regulation and legislation in connection with trade agreements between countries, the environment, import/regulations and so on. All countries want businesses to succeed and for their populations to be able to have access to a wide range of products and services. They also benefit from taxes and import/export duties that have to be paid by businesses trading in the global marketplace.

Business environments

Business to customer

This is where businesses sell products and/or services directly to customers. Business to customer (B2C) originally referred to people who went to shops to buy, for example, clothes or a car, or eat at a restaurant, or pay for a TV subscription. In recent times, it has also referred to the selling of products online. Manufacturers and retailers now sell their products directly to customers over the internet.

Business to business

These are businesses that sell products and/or services to other businesses in order for them to function. For example, a business will sell office furniture, write a software application or sell stationery supplies to another business. Business to business (B2B) businesses have a different target audience to a B2C business. They provide raw materials, finished parts/products, services and consultancy that other businesses need to function, grow and make a profit.

Business to many

These are businesses that sells their products and/or services to other businesses and to customers (a combination of B2C and B2B).

Test yourself

- 1 Explain the difference between a public and a private organisation.
- 2 Describe the role of a board of directors.
- 3 Identify three different types of external stakeholders.
- 4 Describe the type of organisation referred to as an NGO.
- 5 What is the difference between a B2B and a B2C?

1.2 Key factors that influence the business environment

Political factors

Anything that involves the government can have an influence on the business environment. These are outlined below.

Government policy

Government can change the way a business has to function, as well as influencing the economy. This can occur by the government passing new legislation or by changing the way that it spends money or implements taxes. Passing or making amendments to legislation can protect customers and/or the workforce. It may even restrict where businesses can build new premises. When governments spend more money or lower taxes, this can result in more demands being made on the economy resulting in higher outputs and employment. The opposite can also happen if a government increases taxes and reduces its spending.

Foreign trade policy

Changes in a government's trade policy can make it easier or more difficult for businesses to trade across international borders. A trade policy can include import **tariffs** and **subsidies** for local producers, for example farmers and fishers, to provide them with support against international competition. **Quotas** can be implemented on the importing and exporting of certain goods which can (if decreased) have a major impact on a business.

Governments sometimes sign up to a **bilateral** trade agreement with other countries. This is to reduce tariffs and barriers to businesses and to introduce a common market or free trade area. While this can be supportive for businesses in this country, it also increases the competition from other countries. Some countries impose trade **sanctions** and/or **embargos** against other countries.

Tax policy

Taxes include:

- ▶ **Income tax** (tax deducted from an employee's salary). When income tax is increased, the employee has less money to spend.
- ▶ **National Insurance contributions** are deducted from an employee's salary with a contribution also paid by the employer. If these are increased, then

the cost to the employee and the business increases. Any increase in a business's costs can cause **inflation**.

- ▶ **Value added tax (VAT)** is added to goods and services when sold. If it is increased, the prices of goods and services increase. This again means that a business/individual has less 'spare' money to purchase other things.

Key terms

Tariffs: taxes that are charged on the import of goods from other countries. Thus the price of imported goods is increased to try and persuade consumers to buy products made in their own country.

Subsidies: given to businesses in order to support an industry, where it is struggling against international competition or where the international businesses have lowered their prices so that the local businesses cannot make a profit without the subsidy.

Quotas: imposed by the government to restrict the number/monetary value of goods that can be imported and/or exported during a particular period of time. The purpose of quotas is to reduce imports so that there is an increase in domestic production, therefore restricting competition from other countries. Sometimes governments impose quotas when there are concerns about the quality and/or safety of products from another country.

Bilateral: trade agreements made between countries in order to promote trade and commerce. Trade barriers such as tariffs, import quotas and export restrictions are removed. This is to encourage trade and investment between the countries. While bilateral agreements can expand the available market for businesses within a country, they can also result in the closure of smaller businesses who cannot compete with much larger multinational businesses.

Sanctions: political trade restrictions that are implemented against specific countries, with the intention of maintaining or restoring international peace and security.

Embargo: a government order restricting business with a specific country or the exchange of specific goods. An embargo is usually implemented as a result of political or economical issues between different countries. Embargos imposed on a country can have a serious impact on their economy.

Inflation: the increase in the cost of commonly used goods and services, for example food, clothing, transportation and housing. The higher the costs, the less purchasing power (money available to spend) people and businesses have.

- ▶ **Corporation tax** is a tax on an organisation's profits. If corporation tax is increased, there is less profit for the organisation. This can result in reduced investment by the organisation and even a loss of jobs.
- ▶ Local government charges **businesses rates** for premises as well as giving or denying planning permission for the development of new premises.

Cross party focus and agendas

This is where senior members of parliaments and assemblies come together to resolve an issue or agree a particular way forward on an issue. For businesses this may influence their relationships with other countries, for example their treatment of minorities, trading agreements and so on. This is relevant to the IT industry in relation to cyber security, data protection, sharing of technological innovation and the procurement of components. These cross party groups can influence legislation and regulation, and contribute to political pressure on IT organisations to change or modify their behaviour, for example the embargo on firms such as Google providing updates to Android systems to Chinese manufacturers.

Economic factors

Economic factors can have an impact on businesses, how they spend their money and how they make business decisions. These factors affect goods, services and money. The state of the economy on a local and/or global scale can have an impact on how a business operates, taxes that are imposed, the value of assets and consumer demand.

- ▶ **Interest rates** – increases in interest rates mean that businesses that have credit cards and/or loans will have higher interest payments, less disposable income (money available to use for other things) and larger **overheads**. It can result in a business only paying the interest on a loan and not being able to pay the loan off.
- ▶ **Exchange rates** – these can have an impact on businesses that trade with other countries, that is import/export. Changes to exchange rates, for example the value of the pound to the euro or the US dollar, can affect how much money a business has to pay to its international supplier. This in turn can affect any profit the business makes.
- ▶ **Consumer trends** – what products and the quantity of products a consumer buys can be impacted by the state of the economy. The factors that can have a major influence on consumer purchasing include employment, level of wages, prices/inflation,

Key terms

Overheads: ongoing expenses that businesses are required to pay that are not related to the production of goods and/or services.

Consumer confidence: how confident consumers are in the state of the economy and their own personal financial situation.

Economic recession: a decline in economic activity that spreads across the entire economy and lasts more than a few months. It can be related to income, employment, industrial production and retail sales.

interest rates and **consumer confidence**. High unemployment, low wages (or loss of wages), increases in prices, high interest rates and lack of consumer confidence can all have an impact on how much consumers spend, what they buy and how regularly they spend their money.

- ▶ **Periods of recession** – an **economic recession** can change the purchasing attitude of customers. This can result in businesses dropping their prices, trying to produce smaller volumes of products or, in certain cases, going out of business.

Social factors

Social factors include social mobility, market trends, cultural expectations and socioeconomic aspects.

Social mobility

This is a move in a person's individual social status, for example from one status to another. This can be higher, lower, inter-generational or intra-generational. Social mobility can take different forms and people can experience different types of social mobility at different stages of their lives.

- ▶ **Horizontal mobility** – this is when a person changes their occupation but their overall status in society remains the same. For example, a network manager could take up the position of teaching networks in a college. Their occupation has changed, but their social standing remains the same.
- ▶ **Vertical mobility** – this is a change to occupational, political or religious status that also changes a person's position in society. Vertical mobility can be ascending and descending. An example of a descending social mobility is where a businessman is forced to declare bankruptcy and moves to a lower level in society. An example of an ascending social mobility is where a businessman

stands as a Member of Parliament (MP) and successfully wins their parliamentary seat. They move to a higher level in society.

- ▶ **Upward mobility** – you may have heard the term ‘upwardly mobile’; this is what that term is referring to. This is when an individual moves from a lower position in society to a higher one. While it is similar to vertical social mobility, it can come at a cost to the individual. A person who moves upward can often leave behind familiar surroundings, for example family and places, and may also need to change the way they think and/or behave.
- ▶ **Downward mobility** – you may also have heard the term ‘downwardly mobile’. This is when an individual who is in a high social position moves down to a lower social position. This can occur when someone has committed a wrongful act, for example a chairman of an organisation has been caught committing fraud and is removed from his position in the company. Downward mobility is stressful for people who face a rapid decline in their social status. An individual may find it hard to adapt to the change in their environment and the standard of living they are used to due to the money they earned.
- ▶ **Inter-generational mobility** – this is a change in position from one generation to another. The parents of a child worked in a retail outlet while their child was being educated at school. This enabled the child to study hard and become a doctor. This type of social change encourages generations to adopt to a new way of living and thinking. Inter-generational mobility is affected by the differences between parents, their children’s upbringing, changes in the population and changes in occupation.
- ▶ **Intra-generational mobility** – this is when there is a change in the social position during the lifetime of a single generation. It can also refer to a change in position between siblings (brothers and sisters). An example is when a person starts in an organisation as an administrative assistant, they move up through the organisation to become an administrative supervisor, a manager and then possibly a director.

So how does social mobility influence the business environment? Social mobility is an important issue for countries around the world and their economies. In an ideal world, an individual’s future should be determined by their talent and hard

work. Unfortunately, this is not always the case and businesses can play a major role in helping to solve the issue. They can ensure that they have a diverse workforce and provide equal opportunities for all, irrespective of their social standing.

Market trends

The analysis of market trends enables a business to identify any potential changes to their market as well as how the business can stay ahead of their competitors. Businesses identify current and potential changes to their customers’ needs and wants and then consider innovative and new ways of providing their products and/or services.

Cultural expectations

It is a mistake to make assumptions that just because people dress in a similar way that they think in the same way. It is also wrong to assume that because people make similar choices (e.g. the customers buying the products/services), they are the same type of people. People are different, they have different beliefs and their own ways of ‘doing’ things. Businesses who want to work on a global scale must consider the cultural differences with respect to how business is conducted in different countries, how to interact with businesses in other countries and what is considered acceptable and polite practice.

Socioeconomic aspects

These are characteristics that usually influence consumers. They are associated with the quality of people’s lives and determine the behaviours, preferences, tastes and lifestyle of the people within society. These factors can have an impact on businesses because consumers can affect the growth of any business, large or small. Businesses need to identify and consider the socioeconomic factors in order to compete in a market that is forever changing.

- ▶ **Income** – the amount of money people earn and what they have available to spend can have a huge impact on how much people spend and what they spend their money on. The more money people have available, the more money they spend and the more potential there is for them to spend their money on luxury items such as new cars, holidays and so on.
- ▶ **Occupation** – the amount of money an individual earns is largely linked to their occupation. The differences between occupations can determine

the income gaps between consumers. Businesses must identify the occupations of their consumers so that they can make decisions about who to target to enable them to sell their products/services.

- ▶ **Economic growth** – the economic growth and development of countries also has an impact on the social status of their population. If a country experiences high economic growth, then the population has better access to good levels of income. This can attract more investors into the country and increase employment rates, for example when car companies open up new plants to produce their cars. If the economic growth of a country increases, then there is an increase in consumer spending and businesses can grow.

Technological factors

Many businesses use emerging technologies to try and reduce the operational costs, increase efficiency and profits, and improve stakeholder experience. The potential impacts of emerging technologies on businesses are that it:

- ▶ saves time and money by automating and optimising routine processes and tasks
- ▶ increases productivity and operational efficiencies
- ▶ makes faster business decisions based on outputs from cognitive technologies
- ▶ avoids mistakes and 'human error' (provided that the emerging technologies are set up properly)
- ▶ processes vast amounts of data to generate quality information which can be used to expand the business
- ▶ increases revenue by identifying and maximising revenue opportunities.

Legal factors

Legal factors influence businesses and how they operate. These can include laws and regulations relating to taxation, employment, contracts, securities, immigration and many more. They affect the way businesses operate and how customers behave.

It is important that businesses have a good understanding of the legal requirements that they must consider and adhere to. Legislation can be introduced, amended and changed. It is important that a business keeps up to date with current legal requirements. Failure to do so can result in heavy fines. These legal factors can determine the success or failure of a business.

All legal factors are important, but some more than others:

- ▶ **Organisational law** – businesses can be registered as a corporation, limited partnership, limited liability partnership, limited liability company and so on. The legal status of a business determines the types of activities it is allowed to carry out, taxation, customs and employment requirements.
- ▶ **Employment law** – employment laws operate differently in different countries. For example, the minimum wage in the UK is different to South Africa and the USA. The minimum wage in South Africa is a lot less than in the UK and the USA. In addition, laws relating to dismissal and discrimination are much stricter in the UK, than in some other countries.
- ▶ **Consumer laws** – these are laws that are used to regulate the legal relationships between consumers and businesses. They have been implemented to protect consumers from fraudulent behaviour. This requires businesses to provide detailed information with respect to the products they produce.
- ▶ **Health and safety legislation** – laws relating to health and safety can also vary greatly between countries. For example, heavy fines can be imposed on a business that creates high volumes of air pollution depending on the country it is based in. Not all legislation is consistent on a global scale. Some countries, such as the UK, ensure that their employees receive clothing and equipment (depending on job role) that is of the highest standard. People who look at computer screens for long periods of time are required to have regular breaks and their eye tests paid by the business. This can have an impact on the financial resources and administrative costs to a business.

Environmental factors

Environmental factors can be internal and external to the business. External factors can include technological, demographical, political and economic factors, while internal factors can include the interrelationships and objectives of the business. Businesses have no control over the external environment, but they can help to improve it.

Carbon footprint

This is the impact that businesses and individuals have on the environment. Carbon footprints are measures of carbon dioxide (CO_2) and are determined by the greenhouse gases that are generated by the actions of the business.

The business sector across the world has always played a major role in the creation and subsequent reduction of greenhouse gases. Businesses are encouraged to prioritise sustainability and reduce the energy they use. An example from within the UK was the introduction of shops having to charge for plastic carrier bags. This was to encourage customers to use their own bags and reduce the amount of waste that was generated by customers throwing their plastic carrier bags away, which ended up in landfill. In many countries there are heavy fines levied at businesses who do not consider the environment.

Here are some of the ways that businesses can reduce their carbon footprint:

- ▶ Use renewable energy, for example use of wind turbines and solar panels to generate energy.
- ▶ Reduce the level of air travel. Businesses are now travelling less and using video conferencing software for meetings and projects.
- ▶ Reduce emissions from road travel by implementing remote working and video conferencing facilities. Businesses that have a fleet of cars and/or lorries could look at more fuel efficient or alternative fuel/electric vehicles. Government grants are available to subsidise the cost of new low-emission vehicles.
- ▶ Training drivers of company vehicles could implement eco driving techniques that can save fuel and reduce emissions. The training could include encouraging drivers to be more aware and anticipate road considerations and consider greater fuel economy.
- ▶ Install more efficient lighting such as light-emitting diode (LED) lights, installing motion sensors so that lights automatically turn on when people enter rooms and automatically turn off when rooms are empty. The installation of dimmable lights can also help to reduce energy costs as not all areas of the building need to have 100% full lighting.
- ▶ Reduce data centre and communication's room energy usage by increasing the cooling systems to a higher temperature. This saves energy and increases the cooling capacity.
- ▶ Implement building temperature controls that will switch on and off at regulated times and time periods.
- ▶ Reuse, reduce, recycle is about how a business considers sustainable purchasing of products. Water, paper, food, mobile technology and

packaging, as well as the manufacture and transportation of these items, all have an impact on a business's carbon footprint. Businesses can use recycled paper and refurbished telephones and IT equipment.

- ▶ When packaging products for sale, businesses should consider the packaging they use and implement a strategy to remove the use of single-use plastic. Businesses should consider alternative packaging that is biodegradable.
- ▶ Reduce printing – businesses consume vast quantities of paper and should consider reducing their printing costs by digitising, for example signing contracts online using digital signatures, and avoiding printing emails and other documents by storing them digitally.

Digital waste

Digital waste, sometimes referred to as e-waste, is any type of digital/electronic equipment that is no longer used and is discarded. The rate at which technology is updated with new devices such as computers, servers, monitors, laptops and smartphones has rapidly increased over the years.

Unlike other recyclable products and waste, digital waste needs careful disposal and compliance with legal requirements. The vast majority of digital waste contains rare earth materials and strong chemicals. Some of the components can be very expensive while others are extremely toxic. Businesses must consider local, national and international regulations (depending on where they are disposing of the equipment) or they can face heavy fines and damage the business's reputation. The correct recycling of digital waste can aid the reclaiming and repurposing of available material within the components as well as properly disposing of hazardous components that can harm the environment and people's health.

As well as the environmental issues surrounding the disposal of digital waste, there are also major security issues. Hard drives and other storage media should not be disposed of in standard landfills when they contain sensitive business or personal information. If a business does not recycle its digital waste properly, it is at risk of exposing confidential information. This is also a breach of legislation and regulation.

Research

In small groups, research the Fairtrade organisation and how it is attempting to improve the social mobility of the cocoa plantation farmers and their employees across the world. Develop a presentation to be delivered to the group of the results of your research. Consider the following:

- ▶ the countries where Fairtrade are trying to improve social mobility
- ▶ the current social mobility of the plantation farmers and their employees
- ▶ how Fairtrade can help to support the farmers and their employees.

Test yourself

- 1 Explain the difference between inter-generational and intra-generational mobility.
- 2 Describe how socioeconomic aspects can influence the business environment.
- 3 Identify three legal factors that can influence a business's operation.
- 4 Discuss the political factors that can influence the business environment.
- 5 Describe the term 'carbon footprint' and explain how businesses can reduce their carbon footprint.

1.3 The measurable value of digitalisation in business

Sales and marketing

Marketing plays an important role for a business when it comes to promoting and selling products and services. Sales are important to a business because this is how the business makes a profit and survives. You cannot sell a product/service without marketing it. Marketing takes place first and includes identifying the needs and wants of the customer. If a product/service is not wanted or needed, then it cannot be sold.

Enhanced market research

Thanks to digitalisation, businesses can transform the way they obtain information about consumers by viewing multiple channels and **touchpoints** as a mechanism to capture relevant data. Businesses can

use the data gathered through digitalisation to analyse consumers' lifestyles, needs and preferences. This enables the businesses to deliver personalised product recommendations, promotions, rewards and content. It also enables businesses to consider how to develop new products/services or improve the products/services they already offer.

Increased opportunities for brand promotion

Businesses can use social media and any other digital device to promote their products and services (**brand**). It allows the businesses to interact with their customers and potential customers more easily. They can quickly answer queries, and share news, promotions and updates. It is a good way of keeping customers engaged and interested. There are many **benefits** to a business when using digital promotion techniques.

- ▶ **Global access** – the use of the internet means that businesses have access to a much wider audience. A business can provide customers with their products/services regardless of where they live (and of course legislation for the relevant countries being adhered to).
- ▶ **Target audience** – it enables businesses to target specific audiences. Depending on the product/service a business provides, it can for example target specific age ranges or locations and so on.
- ▶ **Cost-effective** – digital advertising is more economical (costs less) than more traditional methods, for example television advertisements, billboards and advertisements in newspapers.
- ▶ **Tools** – there are many programs that allow businesses to analyse their effectiveness with respect to promoting their brands. This enables businesses to be more effective when planning their promotional strategy.
- ▶ **Even playing field** – regardless of the size of a business, they all have the same opportunity to promote their brands using digital technology.

Key terms

Customer touchpoints: any point of contact between a business and a customer, for example through email, call centres, websites, social media, advertisements, third-party review sites and so on.

Brand: a type of product manufactured by a particular company under a particular name.

As with all things, there are also **disadvantages** of digitalisation as follows:

- ▶ **Social media** – while social media can be a business's best friend, it can also be a big problem for a business. Once a business has posted, they have little or no control over how that post is accepted by people. An innocent phrase or photograph can be misinterpreted, and the misinterpretation can go viral.
- ▶ **Time and skills** – businesses need to ensure that they have people who are allocated the time and have the skills to manage the marketing and promotions. Therefore, careful consideration needs to be given to the return (the amount of income) that can be generated from using digital marketing and promotional techniques.
- ▶ **Criticisms** – any negative comments from people will be visible to everyone else on the internet. Just as important are the responses made by businesses. It can be difficult not to take negative comments personally and to provide responses that are defensive.
- ▶ **Competition** – all businesses are doing the same thing. A business needs to keep pace with their competitors in order to attract the attention of the target audience.

Increased communication and coverage via social media

Social media is now one of the most important platforms for digital marketing. As stated in the section relating to brand promotion above, it can help businesses reach millions of customers on a global scale. If businesses want to increase their communication and coverage using social media, the following must be considered:

- ▶ What social media channels are the customers using?
- ▶ How can the business target audiences by using these channels?
- ▶ What are the business's objectives for using social media?

Social media can help businesses in the following ways:

- ▶ **channel engagement** – it can boost user engagement across different channels by engaging with more customers and delivering a better online experience
- ▶ **business growth** – the social interaction between businesses and their customers increases sales and improves brand loyalty
- ▶ **brand building** – as stated above, social media can boost a business's visibility with potential customers.

Online opportunities for selling/e-commerce

Due to the increase in the use of digital technology, customers expect fast despatch of the products/services they purchase. In addition, they expect instant access to products/services through accessing websites as well as customer service availability 24/7. Research has shown that people shop online at least once a week. This has resulted in businesses moving their sales operations online (e-commerce). As previously mentioned, this enables them to reach a much larger audience (global access) and increase their brand awareness (brand promotion through social media etc.).

Setting up websites to display products/services and advertising online takes less time and costs less than running what is referred to as a 'bricks and mortar' store or premises. The use of digital technologies such as e-commerce, retail apps, chatbots and marketing automation tools can streamline a business's operations. Many manufacturing industries now use artificial intelligence and **deep learning** as part of their manufacturing process.

Smaller businesses that sell online find it easier to compete with much larger businesses. A business can set up a website very quickly (sometimes within hours). All that is required is a **domain name** and hosting. Free website templates are available for download or businesses can hire the services of a web designer. If businesses are planning to sell their products/services online, they can implement an e-commerce theme.

When businesses use an online platform (sell online), they do not have to consider the cost of rent, utilities (gas/electric, water) or rates as they would if they used a physical building. Customers have access to a business's products and services 24/7 and once the order is placed, the system deals with the rest of the transaction.

Online trading provides customers with a more personalised experience. Websites collect customer data that can then be analysed to create customer mailing lists based on the customers' location, purchase history and

Key terms

Deep learning: an artificial intelligence function that works like the human brain. It is used to process data, detect objects, make decisions, and for speech recognition and language translation. It is able to learn without human supervision.

Domain name: the name of the website, for example google.com.

product preferences as well as many other criteria. This means that businesses can use targeted online advertising with customers (even those who visit the store but either abandon the shopping cart they started or just leave without attempting to purchase anything). Using the analytics obtained from customer data, businesses can then display on their website their best-selling products/services as well as promote those that other customers have bought. This can increase the amount of traffic (number of people accessing the website) and therefore increase sales.

If a business uses a physical store or warehouse and so on then as the business increases, they have to consider purchasing or renting more space. Not only can this be costly, but it may be difficult to find in the correct location. With online selling, businesses can increase the space allocated to their site by increasing their hosting plan and therefore increase availability as their customer base increases.

There are also drawbacks and some of these have been mentioned previously but the most important ones to consider are:

- ▶ **competition** – everyone is using e-commerce these days and it can be difficult to promote and grow a business and be ‘better than the rest’ who offer the same products/services
- ▶ **returns** – customers are unable to ‘try before they buy’ and this can lead to a high return rate (customers returning goods because they do not like them, or they are not what they were anticipating).

Tracking and management of customer/service-user retention

Technology can be used to calculate and track customer/service-user retention rates. So, what is a customer retention rate (CRR)? This is the number of customers a business has retained over a given period. There is a simple formula that is used to calculate the retention rate. Below is an example for a business who had 1000 customers at the beginning of the period and attracted 300 new customers. At the end of the period they had 1000 customers.

$$\frac{1,200 \text{ customers at the end of the period} - 300 \text{ customers acquired}}{1,000 \text{ customers at the beginning of the period}} \times 100 = 90\% \text{ CRR}$$

As can be seen from the results of the formula, the company actually lost 100 customers, so their retention rate was only 90%. This is important information for businesses. They can use it for further analysis to identify why they lost the customers and what they can do to possibly attract the customers back, as well as not lose anymore.

The way that the customers/service-users view a business impacts on the success of the business and potential revenue. If the customer service provided by the business is poor (or in some cases non-existent), customers/service-users will find other businesses to purchase from. This is because they do not feel valued or important to the business. When customers/service-users are happy with the business, then they continue to purchase from them (customer retention).

Personalisation

Customers/service-users will remain loyal to a business if the service that they are provided with is personalised. This approach is important to a business and can make them stand out from other similar businesses. This is how digital technology is useful because by implementing technology such as artificial intelligence (AI) and Internet of Things (IoT), customers’ data can be processed more accurately and faster. This helps businesses to have a better understanding of their customers/service-users and how to provide them with:

- ▶ the best solution for their individual needs, requirements and/or problems
- ▶ more relevant search results
- ▶ personalised product recommendations
- ▶ suggestions and emails based on the individual customer’s buying habits and experience.

An effective way for businesses to build customer/service-user retention is by making customers/service-users feel more valued and appreciated by improving the service offered.

Customer experience

AI is widely used to improve the service and customer experience. This includes the use of **virtual assistants** and **bots** for tasks that are repetitive and simple. This allows businesses to:

- ▶ provide customers/service-users with more relevant product recommendations

Key terms

Virtual assistants: bots that perform various tasks that include understanding the users’ questions, providing relevant information and creating product descriptions. These are available 24/7 for the customers/service-users and improve their overall customer experience.

Bots: used by businesses online to provide answers to customers’/service-users’ questions, as well as product information and suggestions for products they can buy or articles that they can read.

- ▶ give immediate answers and information about prices and the availability of the products/service
- ▶ identify any delivery charges based on a customer's location.

AI bots can provide human-like intelligence to keep customers engaged and increase customer satisfaction.

Automated processes

Customers are impatient and expect immediate responses, so the use of virtual assistants and bots that are available 24/7 is important. Also, multiple customer enquiries can be responded to simultaneously. By using technology, employees can focus on more productive tasks as opposed to the more repetitive ones.

Digital analytics

Digital analytics is the collection, measurement, analysis, visualisation and interpretation of digital data that indicates the users' (customers/service-users) behaviours when accessing a business's website, mobile sites, mobile applications, social media and so on.

It is often used to improve customer experiences, attract new audiences and convert them into customers. The analytics produces insights into how a business is performing in the digital marketplace. The information gathered from the analysis allows the business to track the way their products/services are performing, information relating to the audience, and how to change or enhance the promotion of their products/services. This can help businesses to develop efficient plans and make appropriate business decisions.

Operations

Digitalisation improves the operations within a business. It enables automation, an increase in data quality, as well as the collection and structure of data. This helps a business to work better and smarter.

Enhanced communication channels

Digital technology can help a business to improve business communications with internal and external stakeholders.

- ▶ **Accessibility** – messages can be sent and received 24 hours a day from anywhere in the world. This can be through emails, social media, websites and text. People can work remotely thanks to mobile technology and are no longer required to always be on the premises of the organisation. Businesses that carry out research and/or carry out projects can now conduct this process online and are able to bring

relevant people/experts together regardless of where they are located in the world. Human resource departments can promote potential vacancies to a wider audience online and also receive applications online.

- ▶ **Reliability** – messages can get lost in translation easily, for example a receptionist misunderstands a message from a customer and therefore an incorrect message is passed on, which results in a customer not receiving the service they expect. Relying on web-based communication software ensures that the message is delivered instantly.
- ▶ **Marketing exposure** – digital technology expands the scope of organisations marketing their products and/or services. The use of social media and websites has enabled organisations to access a much wider audience and gather data on how many people are looking at their business.
- ▶ **Training** – employees can be trained online instead of attending training sessions on the premises or travelling for sessions in other locations. This makes training more widely available and reduces overall training costs.

Automation of internal processes

This involves using digital technology to make processes run themselves. This makes the processes more efficient and improves reporting. There are a number of benefits of automating business processes:

- ▶ **Operational efficiency** – automated software does not require someone to be continually working on a task as it progresses from one stage to the next. For example, a customer places an order online and the automated process will process this order through to the warehouse for the warehouse staff to select the product and arrange for despatch. Automation of processes can also help to identify and support the correction of errors and **bottlenecks** in workflow.
- ▶ **Document/file management** – the maintenance of documents, files and data can be very difficult and time-consuming for any business. Moving data, documents and files manually can introduce errors.

Key term

Bottleneck: when congestion occurs within a production system, for example a computer network or an assembly line in a factory. It occurs when the workloads arrive at such a speed that the production process has difficulty in processing them quickly enough.

With automation, document and file management requires less effort and the organisation and retrieval of data is simplified. Confidential data can be made more secure by implementing levels of access (through the use of usernames and passwords, people can be provided with levels of access – who can access what). Information is more accurate and can be transferred between different processes, which in turn increases employee productivity (how much work they do).

- ▶ **Improved customer experiences** – by automating the internal business processes, the customer experience is improved. This is because products/services can be made readily available to the customer/service end user. The quality levels of the products/services and customer service itself can be maintained and standardised thereby improving efficiency. Virtual assistants and bots have already been discussed and how they can be used to resolve customer/service end user cases quickly, efficiently and accurately.
- ▶ **Improved employee morale** – the automation of processes allows employees to work more efficiently because the work environment is less tedious (there are fewer repetitive tasks). The activities within the workplace can be streamlined, remove potential bottlenecks and decrease the risk of human error. This provides more time for employees to focus on other work which may be more valuable to the business (and more interesting to the employees).

Remote working functionality

Mobile and remote working is now more accessible to a wider range of people. Organisations with a larger remote workforce require less office space, and fewer materials and utilities, which in turn reduces costs. The drawback of remote and mobile working is the work/life balance and an employee's mental health. Remote workers can find it difficult to 'switch-off' at the end of the working day as everything is still accessible to them and they can be contacted. In addition, remote workers can be lonely, and therefore good communication through enhanced technology allows them to communicate effectively with their colleagues. In this way, their quality of work and productivity will not suffer.

Finance

The automation of core processes and transactions frees up the finance team so that they can focus on

strategic business performance and at the same time improve the service to other key functional areas using the digital reporting tools that are available.

The effective use of financial software solutions ensures that current information is readily available to support the business when making up-to-date strategic decisions. Technology also enables the finance functional area to assess the current situation of how the business is performing against the set budget. This provides an overview of the financial health of the organisation as well as a detailed analysis of any business-critical areas posing a risk to its viability.

Technology increases the speed of critical financial business tasks such as the production of:

- ▶ quarterly financial reports
- ▶ profit and loss statements
- ▶ balance sheets
- ▶ payroll runs (weekly, monthly or both).

Finance software is often hosted in the cloud. This means that a finance team can access information that they require wherever they may be situated. The latest technology can also gather and consolidate data and information from other systems within the organisation wherever they are. The benefits in timesaving alone are enormous. The use of technology by the finance functional area has resulted in greater collaboration across functional areas regardless of their location.

Increased fiscal performance

The fiscal policies implemented by the government in relation to taxation and spending can have an impact on every business. A fiscal policy includes the actions that governments take to influence the economy. This can include new taxation and spending policies. The objectives are to stabilise the growth of the economy, keep inflation low and to stimulate growth during recessions. There are different types of fiscal policies:

- ▶ **expansionary** – this is where governments spend more and lower taxes, but it requires governments to borrow more money
- ▶ **contractionary** – this is when the government cuts spending and raises taxes. With higher taxes, people spend less money. This type of policy improves the budget (money available to governments) through the collection of more money through higher taxes.

Fiscal policies are controlled by the government and relate to government spending and taxation.

Government spending

Government spending within the UK can cover a wide range of different programmes. Government spending is divided into different categories:

- ▶ **infrastructure spending** – this can include the building of hospitals, prisons and roads
- ▶ **current spending** – this is the spending of money that has been allocated to services provided by the state (government) and includes healthcare and education
- ▶ **transfer payments** – this includes other types of payments and includes state pensions (money paid to people when they retire) and other welfare benefits, for example family tax credits, income support and so on.

How a government spends money has an impact on the economy and what is referred to as 'consumer confidence'. The more money that the government spends on infrastructure and welfare payments (expansionary policy), the more consumer confidence is boosted. Any increase in government spending can also increase government jobs and this results in wider spending.

Infrastructure projects require the use of contractors and this also boosts the economy as more jobs become available. This has a positive impact on businesses as there are greater demands for the products/services they provide as people have more money to spend and feel more positive about the future.

It is therefore clear that contractionary spending has the opposite effect. People do not have money available to spend and they lose confidence in the economy and are less positive about their future situation with respect to employment, money and so on.

Taxation

Taxation is used to:

- ▶ increase revenue (money coming into the government) to pay for the increased spending
- ▶ correct issues within the market
- ▶ manage income and wealth distribution.

When a fiscal policy is expansionary, taxes are reduced and businesses make more profit. During a contractionary fiscal policy, taxes are higher, there is reduced spending and businesses make less money.

Through digitalisation, governments have greater access to information relating to how businesses in different sectors are performing, the wages employees receive and so on. This allows them to make quicker decisions based on what is happening in the economy and adapt to the needs of the economy promptly.

Increased reporting options and functionality

The two main responsibilities of the finance functional area are **accounts receivable** and **accounts payable**.

This functional area is also responsible for the payroll – making sure that the employees are paid accurately and on time.

Another function involves the planning required to obtain capital finance and management of the organisation's fund. Within the finance functional area, finance managers plan for short-term and long-term financial capital needs and analyse any impact that the borrowing of money can have on the organisation. This functional area produces reports and financial statements that can be used for budgeting, forecasting and other decision-making processes.

The automation of core processes and transactions frees up the finance team so that they can focus on strategic business performance and at the same time improve the service to other key functional areas using the digital reporting tools that are available.

The effective use of financial software solutions ensures that current information is readily available to support the business when making up-to-date strategic decisions. Technology also enables the finance functional area to assess the current situation of how the business is performing against the set budget. This provides an overview of the financial health of the organisation as well as a detailed analysis of any business-critical areas posing a risk to its viability.

Technology increases the speed of critical financial business tasks such as the production of:

- ▶ quarterly financial reports
- ▶ profit and loss statements
- ▶ balance sheets
- ▶ payroll runs (weekly, monthly or both).

Key terms

Accounts receivable: money that is coming into the organisation.

Accounts payable: money that is paid out by the organisation.

Reduced operating costs

Manually carrying out business processes can lead to a waste of resources. Processing takes time and while employees are working through the processing

activities, they are not available for other tasks that may be just as important. Automation uses resources such as the workforce more effectively and efficiently, therefore reducing waste. If the cost of processing operations is reduced, then a business's profit margins increase.

The use of digital technologies and analytics can help a business to increase productivity through the implementation of more streamlined operations. Information-intensive processes are important to digitalise as it can reduce business costs by up to 90%.

With the increase in remote working, employers are providing their employees with the digital tools to work smarter and not harder. This allows for increased productivity, collaboration and improvement in communication. This results in a reduction of costs to a business with respect to travel expenses to meetings, wasted time and so on.

Key performance indicators

These are measurable values that indicate how effectively a business is achieving its key business objectives. There are two forms of key performance indicators (KPIs):

- ▶ high-level KPIs which focus on the overall performance of the business
- ▶ low-level KPIs which focus on the processes within departments, for example sales, marketing, production and so on.

Easier to monitor

Customisable **dashboards** provided by many automated software packages allows things such as KPIs to be monitored easily and quickly for multiple processes that may be running. Reports can be produced indicating clearly where certain areas may need improving. It also enables the efficient monitoring of tasks and encourages employees to be responsible and answerable for the tasks they are involved with.

Key terms

Dashboard: a digital interface that is used to obtain, combine and analyse data across a business. It provides an in-depth analysis of the business as well as providing a real-time indication of the function of the different departments within the business. This can include productivity, trends and activities as well as the key performance indicators.

Research

Amazon constantly undergoes digital transformation. It started as a small mail-order bookstore in 1994 and now it is a global business with over \$1.7 trillion of revenue in July 2021.

Research how Amazon stays ahead of its competitors by implementing the latest digital technologies. Consider the following:

- ▶ how technology has improved its operations
- ▶ what the manufacturing industry could learn from Amazon
- ▶ how Amazon Business has implemented digital technology to work with other businesses (B2B).

Prepare a report of the results of your research.

Test yourself

- 1 Discuss how the implementation of digital technology can help businesses improve the promotion of their brand.
- 2 Describe how digital technology can reduce business costs.
- 3 Explain how digital technology can increase reporting options and functionality.
- 4 Compare the two types of fiscal policy.
- 5 Explain how digital technology can support remote working.

1.4 The influence and impact of digitalisation within a business context and market environment

Brand differentiation

Brand differentiation can be created by using one or more of the following ideas when marketing your product or service:

- ▶ physical characteristics

Brand differentiation: this is what sets your brand apart from the competition. Why should customers look at your brand before others? (Think of Richard Branson and Virgin, or Jeff Bezos and Amazon.) That is brand differentiation.

- ▶ emotional response by the customers to brand triggers (think of the John Lewis Christmas advertisements and charity advertisements using those who receive their funds and services, for example injured animals or victims of natural disasters, to encourage generous donations)
- ▶ presentation of the brand (think of Compare the Market campaigns using meerkats)
- ▶ altering the price of the goods and services to differentiate your brand from others (think of Lidl and Aldi who claim the best quality at the least price)
- ▶ the story behind the brand (think Jimmy Choo shoes)
- ▶ the overall customer experience of the brand: was the advertising an accurate reflection of the quality and presentation of the product or service? Are returning customers given special discounts? Does the offer include free shipping and free returns? These are experiences that determine whether customers will buy your products or services.

Research

Select one service such as a holiday firm and one product such as a smartphone and research how each one has differentiated itself from its competitor.

Use the six bullets highlighted above to start the process and consider whether you can identify any other methods of brand differentiation.

Brand values

Brand values are what the company stands for and what the customer thinks when they see the logo or website and so on. They may think it is beautifully designed, very funny or serious, but these are not reasons why a customer will purchase from a company or remain loyal to a company. To do this they must be:

- ▶ **memorable** – when they see the logo or name, do they immediately remember what they stand for?
- ▶ **timeless** – although as times change it might be necessary for a business to adjust some of its values; they should be designed to remain tough and constant over the years so that its reputation grows
- ▶ **exclusive** – it should not be a version of another company's brand values. It must be unique to the business and its values of customer service, inclusivity, quality and so on.
- ▶ **actionable** – the brand values must be things which the company and its employees expect to deliver in every interaction with customers and the world in general. Therefore, the words used must be action

verbs with examples of how these will be achieved for example:

'We meet your targets for using only renewable energy by our installation of solar panels and wind turbines at our storage facility and are working with renewal energy companies to identify new opportunities to expand this provision to our local outlets.'

A business should also supply a glossary of brand values. To ensure that all business staff and their customers understand their values the business should write them down and publish them.

Research

Select two organisations, one a national company and one an international company, and for each one identify their brand values.

Compare and contrast the two sets of values and explain how being a national or international company may influence their brand values.

Virtualisation/cloud services enabling scaling and elastic computing solutions

Types of virtualisation

Types of **virtualisation** enabling scalability include:

- ▶ **Server virtualisation** – enables one physical server to run multiple operating servers as virtual machines. The benefits are:
 - more efficient use of IT equipment

Key terms

Brand values: these are at the centre of any brand and are incorporated into the look of the brand, the marketing content and language used, and the relationships that are built with customers through good customer service. Brand values are the beliefs that the company or individual holds as essential to delivering the products or services they provide.

Virtualisation: using their own physical hardware, a company can create and use virtual resources such as servers, devices, or computing resources. The results are: reduction in costs of hardware, associated infrastructure and maintenance; reduction in operating costs; reduction in downtime due to security or other risks; and improved reliability as different host machines share the load.

- faster workload distribution
- better application operation
- improved server access
- reduced operating costs.

- ▶ **Network virtualisation** – reproduces the physical network requirements as a virtual network to allow applications to run in exactly the same way as on the physical network but with logical rather than physical ports, devices, routers, firewalls and so on.
- ▶ **Desktop virtualisation** – enables organisations to provide software configured for the specific needs of the particular workplace or individual. Any changes or upgrades can be rolled out quickly and easily from the IT department to all relevant locations. It also allows easy rollout to mobile or remote workers who may be using iOS, Android, Windows or any other permitted operating system.

Cloud solutions enabling elastic computing solutions

Cloud solutions deliver computing services such as servers, storage and networking over the internet. Data storage and processing occurs remotely from a location which may be anywhere in the world. Cloud solutions provide:

- ▶ **Connectivity** – employees are connected to the business at any time and anywhere in the world, using any device available. This reduces the danger of important files being stored on individual computers with risk of loss, theft or damage.
- ▶ **Faster implementation** – installing a cloud solution can take as little as a few hours rather than the months or even years it takes to deploy a physical solution.
- ▶ **Improved collaboration** – the improved connectivity allows workers to work together wherever they are and using whatever facilities are available at their location. This allows them to concentrate on the business needs rather than those of their IT equipment.
- ▶ **Reduced risk of data loss** – better backup facilities at distant locations avoiding local natural disasters and cyber attacks.
- ▶ **Security** – cloud facility providers employ highly trained and experienced computer security staff and spend far more on security hardware and software than individual organisations can afford.
- ▶ **Cost saving** – reduces the costs of physical servers, physical data storage and processing power.

So, from a business viewpoint, these approaches provide two of the three possible ways that business can be supported by information technology and digitisation.

The first way would be for the business to have its own hardware, software and internet resources which are expensive but will also be costly in terms of the space and personnel needed to run and maintain the system. Many of these roles such as programmers, developers and maintenance engineers are highly skilled roles which are in high demand; attracting and holding on to these staff may be difficult, and costly when a key member leaves the organisation. Other issues include security of the facilities, and problems caused by security and hardware or software failures that can cause long periods of shutdown which will have a negative impact on the company's standing with their customers.

The second way is virtualisation as this will reduce the costs in some areas such as power consumption and the number of servers, but the company still needs to make a major investment in hardware to support the virtual environment. The company, through its virtual machines, can give guest access which prevents guests accessing sensitive data. One issue with virtualisation is that **scalability** is limited because of the configuration of virtual machines and a failure on one machine can have a knock-on effect on all other connected machines.

The third way, cloud solutions, reduce the IT budget considerably as hardware and software costs and purchases are much reduced.

Key terms

Cloud services: a wide range of services delivered on demand to businesses and individuals over the internet. They are designed to provide easy and affordable access to applications and resources such as file storage, without the need for internal infrastructure or hardware.

Elastic computing solutions: provision of variable service levels based on the changing needs of the business.

Scalability: the ability of a digital system to respond to variable amounts of load (users, requests, connections, etc.) while maintaining good performance in a cost-efficient way.

Case study

The managing director of your company has asked you to produce a case for moving to a cloud or virtualisation approach to IT delivery. The company sells building designs to the global market and has to decide whether to upgrade its own IT systems or make use of the virtualisation or cloud options available.

- ▶ Research the positive and negative aspects of each approach.
- ▶ Write a report to the managing director comparing the approaches and explaining the differences and similarities that could influence the decision that the company makes.

Digital innovations

Digital innovation is simply using digital technology to solve or improve existing business problems. Clearly, to understand how to ensure that a business remains competitive and responds to changing environments and trends, the technology needs to collect and interpret very large amounts of data from a wide range of sources. By using digital technology such as dashboards, which automatically identify, locate, collect and present data, companies can have an instantaneous update on the state of the company and that of its competitors. These tools can also be used to:

- ▶ identify why customers turn to the business for particular products or services
- ▶ identify unique selling points
- ▶ provide insights into how the uniqueness can be maintained over time.

Business intelligence and insight

Business intelligence uses software and other tools to interpret data so that a business identifies problems, such as losing sales to competitors, or trends, such as customers preferring a new smartphone format rather than the current version on offer. The reports, charts and graphs generated provide insight into the issues and identify potential ways of dealing with them.

Unique selling points

A unique selling point (USP) is the core reason why customers prefer the product or service of one company rather than that of its competitors. It gives the company a distinct position in the marketplace as it clearly demonstrates a special benefit that it can provide which others do not. This may include the value of the product for its price or the solution it provides to a particular business problem.

Processes and business models

A process is not the same as a model. However, in business the terms are sometimes used interchangeably.

- ▶ **Business processes** – the business as a whole and its various departments all have their own business processes. These are the practical and/or technical steps that must be followed to produce the required outcome. These steps form the systems which ensure that the business operates effectively and efficiently. Each process or system will collect data on its performance which it can analyse so that it can improve or correct the way in which it works.
- ▶ **Business models** – these are simply the plans that businesses devise to ensure that they make a profit. A business model will identify the products and services which a business offers to generate a profit, its target market and the expenses or costs involved in achieving the profit. The target market is the type of individuals or companies which they need to buy their products or services. Business models must be updated regularly to check that they are still fit for purpose.

Digital manufacturing

This is the use of IT systems for the production of products or services for a company. It enables the organisation to integrate its processes and systems across the organisation, from the initial design stage to the final product or service offer. This approach has advantages such as:

- ▶ reduction in the loss of data resulting in mistakes and errors
- ▶ development of a virtual process which can be tested and corrected before time and money is spent on the physical implementation of the systems
- ▶ it speeds up new innovations or redesigns of the service or product and subsequent implementation.

Financial

Business finance includes:

- ▶ paying salaries and suppliers
- ▶ receiving payments from customers
- ▶ ensuring that the company meets its legal obligations in terms of tax and insurance payments
- ▶ the production of predictions on the future financial position of the company
- ▶ quarterly, half-yearly and annual reports on the company's financial position.

Many of the tasks are carried out manually and are repetitive and straightforward. As a result, digital technology enables companies to automate these tasks, saving time and effort. Scanning technology allows cheques, expense receipts and similar documents to be easily captured without having to be keyed in by an individual.

Research

Businesses need to understand their competitors, the marketplace, their customers, government policies and any international events. To enable this understanding, businesses carry out research. Market research is one example where customer views, sales figures, competitors' success or failure, customer aspirations and local culture are just some of the elements which enable companies and their marketing department to measure the success of its marketing approach. This allows a business to devise new marketing strategies and increase its market share.

Companies can gather their own information from their own research and draw on data and findings from secondary sources such as government agencies and published information from other companies. Digital technology has enabled companies to work with online research companies who collect data into huge databases which form big data sets. The data is continuously updated, and detailed information can be put together for companies in a shorter period of time.

Therefore, digital technology has enabled companies to access a far wider range of data than they could with their own resources and with a reduction in costs and time.

Wider access

The aim of every business is to keep its existing customers while attracting new customers. The business must work to ensure that their customers are happy to stay customers. An important element of achieving this is communication. It is important that any communication is positively received, and this means avoiding causing offence or seeming to belittle the intelligence, personality and so on of the customer.

Customer base

This term is used to describe a business's most loyal and involved customers: those who regularly purchase products or services and match its target market. Digitalisation allows the business to widen the potential customer base by increasing its presence such

as creating a website to enable customers to purchase products and services from international locations.

Customer relationship management (CRM) systems, for example, enable a business to collect information on all customers very quickly by storing and analysing customer information from age, ethnicity, location, income and lifestyle to purchasing behaviour and feedback such as star ratings. This allows businesses to continuously adjust their products and/or services to maintain and increase their customer base.

Range of products and services

This refers to the types of product or service which a company provides and may include a very wide range such as those offered by businesses, for example Amazon and Marks and Spencer, to very specialist services which sell only one type of product, for example a florist.

Digitalisation can support the business in producing and delivering its range of products or services in various ways. Digital manufacturing systems such as robotic production lines, monitoring software for quality control and augmented reality and three-dimensional (3D) modelling and printing can support the building of the products.

Digital services can be built using big data, data modelling techniques, automated data collection and storage techniques, providing better accounting or investment opportunities which meet the customer needs. These techniques support the business by reducing the costs of developing new products and/or services, as well as customising products and services and delivering them to the customer in a timely way.

Contextualising customer behaviour

Contextualising means that the business considers the circumstances of the individual customer. How old are they? Are they working? Are they studying? What can they afford to spend? Where do they live? What is their favourite sport? With answers to questions like these, the business can design their communication to match the circumstances of the individual. So, if the business is selling books, they could send out marketing information to someone studying with the words

'The new academic year will soon be here.
Have you managed to collect all the textbooks
you need for the next stage of your course?
Check our digital bookshelves now.'

Digital personalisation

This is a step beyond contextualisation which is aimed at a group of customers. Personalisation means that the communication is written to a particular person. So, using the example above, the business could use the name of the customer, which they have on their customer database, together with the fact that their course of study is medicine, to produce a communication which speaks to them personally.

'Dear Adam, you are off to study Medicine in September. We have a wide selection of medical textbooks available, and *Gray's Anatomy* is currently on special offer. Good luck with your studies.'

Platform interoperability

Customers use a range of computer hardware, software and operating system (OS) platforms, for example iPads, other tablets, smartphones, desktops, laptops, smart TVs and iOS, Windows, Linux, Android to name but a few. Businesses cannot be certain what their customers and potential customers use and do not wish to lose customers or fail to reach those on different platforms. Interoperability means the ability of different devices and software to communicate with each other without the customer being aware.

Open standards

Open standards allow people to share data freely. They prevent the lock-in and barriers to interoperability and allow choices to be made between suppliers and technology solutions. It promotes free competition in the IT market by ensuring that businesses and people find it easy to move their data between different system solutions.

Using non-platform specific digital identity

A digital identity of a person can refer to:

- ▶ username and password
- ▶ date of birth
- ▶ social security number
- ▶ purchasing behaviour/history
- ▶ online search activities, for example electronic transactions.

People can use a variety of platforms when registering themselves for an account, for example with an e-commerce retailer, or to use a banking app. The businesses must ensure that there are no barriers to customers and potential customers accessing their products and services due to using the variety of different platforms.

The European Union (EU) demands that EU countries have interoperability for digital identity across the EU. However, although governments have signed up to the concept of non-platform specific digital identity, the ability to create a single digital identity, regardless of which software or hardware platforms it was designed upon, and which can be used on any system in any country or situation, has not yet been achieved.

Test yourself

- 1 Describe the term 'brand differentiation'.
- 2 Discuss the use of virtualisation and cloud solutions by businesses and how they enable scalability and elastic computing solutions.
- 3 Explain how unique selling points (USPs) provide useful intelligence to businesses.
- 4 Describe the term 'customer base'.
- 5 Explain the difference between contextualising customer behaviour and digital personalisation.

1.5 The role of technical change management in digital operational integrity

Organisational change means a change, reorganisation or replacement with respect to processes, methods, systems, operations, technologies and structure of an organisation. This change can be **developmental**, **transitional** and **transformational**.

So how does change occur and what causes the change? There may be one or more factors which can create the need for change. These can be financial, economic, technological, social, political, legal, staff related and so on.

Key terms

Developmental: concerned with the development of someone, something or even both.

Transitional: the transition (movement) from one position, stage, state or concept to another.

Transformational: producing a change or improvement in a situation.

Preparation and planning

Preparation

Any digital change can be a very complex process and therefore careful preparation is required to ensure that it is successful. The following are examples of the steps that should be taken by an organisation preparing for digital change.

Choosing the appropriate digital change strategy to meet the goals of the organisation

It is important for organisations to identify where digital change is needed and not invest in digital technology just for the sake of it. It is important that organisations carefully consider the overall business goals and objectives they want to achieve. This includes short term, medium term and long term, followed by an assessment of what digital technology is required to achieve the goals and objectives that have been identified. An example could be that an organisation has a goal to expand into new markets. It is therefore more important to focus on the technology required, for example to implement a solid cloud infrastructure to support processes from multiple locations as opposed to investing in AI technology to trial a new production idea.

Investing in technology

Digital change means different things for different businesses in different contexts. Spending a lot of money on digital technology does not always guarantee success. Research has shown that there are three forms of digital technology that can have an impact on the operational functions of organisations:

- ▶ the Internet of Things – because it can provide **operational intelligence**
- ▶ the cloud – because of its scalability
- ▶ big data analytics – which can transform vast amounts of data into predictive and actionable information.

Key term

Operational intelligence: this is data relating to the operational performance of the business that is captured in real-time. It enables a business to analyse its operations and make them more effective. The analysis of this real time data is usually automated and therefore is immediately available for consideration by relevant personnel within the business.

It is therefore important that organisations invest in the digital technology to meet their specific needs.

Communicating the benefits and rationale of the change

Once an organisation has identified how digital change can support the overall business goals, it has to convince the stakeholders. This is because digital change strategies change the way businesses function. There is an impact on people's jobs, how they work together and how they complete tasks.

Engaging the stakeholders is not always an easy task for organisations. All staff from the boardroom to the 'shop floor' need to believe that they have a personal and professional interest in the changes being made. It is important that they can understand the reason for the investment so that there is less resistance to new processes. This is extremely important when digital technology is being used to automate processes that would otherwise be carried out by people or when the investment in technology will deliver a profitable return.

Using data to enhance the decision making

It is well known that organisations collect huge amounts of data. But it is important that the data is used to provide insights into the industry, guide the changes that need to take place and even identify new revenue opportunities. Data analytics provides organisations with critical information relating to customer trends, market predictions and how products/services are performing.

Re-evaluating the digital change strategy

A digital change within any organisation is never complete as new technologies are launched continuously. This can be robots to complete production line tasks quicker than humans or it can be machines which can solve equipment issues without human intervention. It is therefore important for organisations to constantly adapt the digital change strategy as new possibilities arise. They need to reassess the digital journey being taken and consider the rate at which the digital change is taking place. Does it meet customer expectations? Does it meet the business goals? If the answers are 'no', then it is possible the digital technology needs to change.

Managing and reinforcing digital change

When managing and reinforcing digital change, there are a number of key concepts that should be considered by organisations.

Getting 'buy in' from all areas of the business affected by change

The vision is the future aspirations of the business and what it hopes to achieve. A business, for example, might want to move to a fully automated warehouse, migrate all its IT systems to the cloud or enable 50% of the workforce to work remotely.

An initial vision meeting is held to ensure that all relevant interested parties e.g. managers, workforce, stakeholders etc. understand the business' vision and any impact it may have on the way they work or the working relationships with their clients/customers/ suppliers. Regular vision meetings are then held to facilitate the development of a shared vision by all parties and to identify any changes that may need to be made as it progresses through the change cycle.

Designing the digital change roadmap

It is important that any form of digital change is communicated to all interested parties across the business. This includes the customers and the workforce. The customers need to be made aware of any digital change that is going to have an impact on how they secure products and/or services, communicate/ interact with the business, how their information is being securely stored, how payments will be processed. By making customers aware of how any digital changes will impact on how they interact with the business, it is hoped that this will retain customer confidence. As far as the workforce is concerned, they will need to know the impacts these changes will have on their job role. This includes whether their job will change, what it means as far as the tasks they do on a daily basis. Will there be a requirement for training in order to upskill, will they still have a job? It is therefore important that the workforce is made aware of any changes and to provide them with a degree of confidence in the direction the business is going and what it means to them personally.

Developing the teams and resource acquisition

This is the stage where the main team members are identified and recruited. Each member of the team is selected based on their expertise and knowledge. The team members can be internal to the organisation or hired specialists, e.g. software developers, systems analysts, engineers, depending on what the change is

for. Resources also include things such as hardware, software or equipment that may be required to support the changes. The teams will attend meetings and provide feedback on how their particular tasks are progressing, any issues identified and how they may need to be addressed (or were addressed). These meetings ensure that any digital change remains on track and still meets the goals of the organisation.

Launching and monitoring

The previous sections relate to the key considerations that must be made when carrying out any digital change transformation. Time needs to be given to each of these considerations prior to launching the actual digital transformational change. Once all considerations have been analysed, considered, adopted, then the digital change process can be launched.

Once the digital change process has been launched, it should be monitored closely to ensure that it is still aligned with the documented considerations. There is always the possibility that further considerations materialise and things need to be adapted or amended to address any potential problems/issues. This careful monitoring will ensure that the organisation vision can be achieved even if the end result has to be slightly adapted.

Planning

Planning can be categorised into two groups: planned-for factors and unforeseen/Previously unpreventable factors.

Planned-for factors

Planned change is the preparation of the organisation either as a whole or a part of it, for new goals or a new direction for the business to go in.

Adding additional features and/or services

This is where an organisation identifies the need to include additional features and/or services such as additional ways that a customer can communicate with the organisation. For example, this might be by using social media or implementing chatbots on the website. It usually relates to improving business processes and the stakeholder experience.

Diversification

This is when an organisation develops a new product or expands into a new market. Usually, diversification is a way that an organisation manages risk by minimising any potential harm to the business during potential economic downturns. Consider how many high street stores now provide online access to their

products and/or services due to the lack of customers using the high street to shop. Business diversification is also a strategy for growth.

Scaling

This is implemented to support the growth of a business. It enables a business to grow without, or with at least minimal, barriers. Scaling requires careful planning, finance, appropriate systems, staff, processes, technology and if appropriate partners.

Rebranding

This is the process of changing the corporate image of the organisation. It is usually a marketing strategy of giving a new name, logo or change in the style of a brand which is already established. The purpose of rebranding is to create a different identity within the marketplace.

Innovations within digital technology

As we all know, technology evolves at a fast pace. It is important that organisations adopt new technologies for the following reasons:

- ▶ **Competitive advantage** – organisations that gain a competitive advantage do not just do one thing. Organisations aim to be ahead of their competitors and to stay ahead by adapting to new technologies and using them in an innovative way.
- ▶ **Avoid possible extinction** – organisations that do not adapt to change, especially in relation to technology, can become extinct. An example of this is when the iPhone hit the market and many mobile phone companies lost their position in the smartphone industry.
- ▶ **Prevent potential financial loss** – the executives within an organisation that do not encourage the managers and employees to embrace new technology can cause the business to lose its standing within the marketplace. This can lead to a loss of reputation, a loss of finance (profit) or even going out of business. Adapting to new technology of course can have the opposite effect and show that the business is a market leader, thereby increasing profits through more customers.
- ▶ **Changes in legislation** – these are imposed changes that are mandatory. Organisations must always be compliant when it comes to legislation to avoid severe penalties. Finance and utility industries are very carefully regulated. Organisations may need to reorganise their business processes and systems to maintain compliance with a change in legislation.

- ▶ **Response to competition** – it is important that an organisation understands what its customers want and need, and to react quickly, so that its competitors do not gain competitive advantage. To remain competitive, an organisation must ensure that its main focus is on its customers. Organisations must also understand the strengths and weaknesses of its competitors and how well they react to their customers' needs and changes within the industry. Organisations need to ensure that they are one step ahead of their competitors while complying with regulation and **competition law**.

Unforeseen or previously unpreventable factors

Crisis

This is when bad things happen requiring all kinds of changes by an organisation. This can include natural disasters such as floods, terrorism and cyber attacks.

Key term

Competition law: the purpose of this law is to promote healthy competition. It makes it illegal for anticompetitive agreements to be in place between two or more organisations, for example to share markets and fix prices. It also makes it illegal for businesses to abuse their dominant market position.

Zero-day vulnerabilities

This is a vulnerability in a system or device that has been identified but not yet resolved. Somebody who makes use of and benefits from a zero-day vulnerability is called a 'zero-day exploit'. Zero-day vulnerabilities pose a higher risk to organisations and users because they have been discovered before security researchers and software developers become aware of them and can issue a patch. Cyber criminals are quick to exploit these types of vulnerabilities, and vulnerable systems are exposed until an appropriate patch has been issued.

Data corruption

Damaged files and/or corrupt data can be inevitable and not a matter of 'if' it happens but 'when' it happens. There are several possible causes of data corruption:

- ▶ malware/virus infections
- ▶ sudden loss of power forcing a power shutdown
- ▶ voltage spikes
- ▶ physical hardware issues

- ▶ bad program exits
- ▶ any interruption in the normal processes being carried out by the IT system
- ▶ over-sized databases
- ▶ Network transmission issues for example attenuation, where there is a loss of signal strength. Within WiFi technology this can occur as the device is moved further away from the router. With wired networks it can be as a result of signal loss within the network cables and the connectors. Potentially, any degradation in the quality of the signal can result in transmission errors and the corruption of data. Packets of data can be dropped meaning that although they are transmitted, they do not arrive at their intended destination.

System failures

System failures can occur through hardware and/or software faults and/or cyber-attacks. There is also the possibility for the system to fail due to human error. When a system failure occurs, it may not always display an error message and the system may freeze, reboot or stop functioning altogether. Any system failure can cause major issues for a business and can result in it being unable to function until the problem is rectified. This can take time, while the reason for the failure is investigated and a solution is identified and implemented. The results of the investigation into any system failure can trigger an unforeseen change in a business. It can result in:

- ▶ new equipment and/or software having to be sourced and installed
- ▶ legal, ethical and moral repercussions of a cyber-attack such as a restriction in operations leading to customer dissatisfaction e.g. if there is a system failure with a bank, then its customers may not be able to pay their bills or access their money
- ▶ changes to operating processes
- ▶ additional staff training
- ▶ loss of business, either because of downtime or reputational damage

The types of change that are triggered within a business and the timescales available to implement the change(s), depends on the severity of the system failure.

Operations

Operations is how a business functions – the processes, procedures and tools needed to conduct daily business. It is important that whenever there is a technical change, that the upgrade/new technology/equipment, processes or procedures allow the business to function to its maximum potential.

Interaction of new or upgraded tools and processes into current digital ecosystem

A digital ecosystem is a group of interconnected digital resources that functions as a unit. It consists of:

- ▶ suppliers
- ▶ customers
- ▶ trading partners
- ▶ applications
- ▶ third-party data service providers
- ▶ other relevant technologies.

All these components must be able to function as a combined unit. The integration of business to business practices, applications and data within an ecosystem allows an organisation to control new and old technologies and build automated processes around them that allows the business to continue to grow.

Digital ecosystems enable businesses to implement more efficient business processes and manage them more effectively. They provide business value by:

- ▶ creating new sources of revenue allowing businesses to track and analyse comprehensive data flowing through the business. This data can be used to create new products/services.
- ▶ lowering costs through improved business processes by improving workflow efficiency and improving relationships with customers and partners. It also reduces operational costs due to the automation of data processing.
- ▶ increasing the speed of technology adoption by taking advantage of cloud services and **software as a service (SaaS)** solutions as opposed to relying on outdated software that can no longer support modern business processes.

Key term

Software as a service (SaaS): a cloud-based service where software is accessed via a browser as opposed to being downloaded onto a network or PC.

Establishing best practice for use of new or upgraded tools and processes

One of the most important components when establishing best practice is communication. The information for the implementation and use of new/upgraded tools and processes must be clear and concise. The people involved must know what the best practices are and why they are important to the business.

Once key people within the organisation are aware of the best practices, they must implement them and identify the employees that will be responsible for carrying out these best practices.

A plan should be created to assess and evaluate the success of the practices to ensure that they are not only being carried out, but that they are effective. Best practices evolve and change over time and in the case of digital transformation are critical to the overall success of the change. The identification of best practices will be dependent on what new or upgraded tools/processes have been implemented and the desired impact that is required for the business.

Facilitating processes and business models

It is important to define the processes involved for the automation of business processes in detail. This is achieved by analysing and documenting the current workflows with the intention of designing more efficient processes. The digital transformation can be implemented through the use of digital tools to improve the current business processes.

Digital technology provides new ways of creating and capturing **value** in **business model innovation**. The changes to business models can be classified into three categories:

- ▶ **automation** – the use of digital technology to automate existing workflow processes and activities
- ▶ **extension** – the use of digital technology to support new ways of conducting business activities which add to rather than replace existing processes
- ▶ **transformation** – the use of digital technology to support new ways of conducting business activities by replacing the existing processes.

Key terms

Value: there are two forms of value in the business model. The value proposition made by the business of the value to the external stakeholders for accepting the digital transformation, and the business values shared with the internal stakeholders and the benefits that the digital transformation will have for the business and for them as individuals.

Business model innovation: improving advantage and value creation by making simultaneous and mutually supportive changes to the business's value proposition to external stakeholders and its operating model.

Downtime: the time when a computer system or IT system is unavailable, offline or not operational.

Applying fixes

Businesses need to be able to continue to function while the change management process is taking place. The implementation of new/upgraded technology and revised processes must not have a negative impact on the business and prevent it from continuing with its daily role. It is therefore important that any work that is carried out on the systems does not cause any **downtime** to the business. This can create many issues for the business such as loss of income and loss of customers.

This can be addressed by carrying out work that would cause downtime to be implemented outside the standard working hours of the business. Banks will often inform their customers that the 'system is being updated between ...' and that those services such as online banking will not be available. There are a number of ways that fixes can be applied so as not to disrupt the operation of the business:

- ▶ **Parallel** – this involves operating the old and the new system simultaneously over a period of time. This ensures that any major issues can be identified and rectified without any loss of data, functionality and/or production. This also allows end users to familiarise themselves with the changed system/process.
- ▶ **Phased** – this is where changes are made in stages, that is not all changes are made at the same time. This is to ensure that the changes are functioning as intended before implementing further changes and, as with the parallel method, ensure that there is a reduced risk of data loss, and to operation and production. The phased method can also be used in conjunction with the parallel method.
- ▶ **Direct** – this is where the changes are implemented directly into the system already in place or a new system/technology is installed but is not phased or parallel.
- ▶ **Pilot** – the pilot is used to test the change deliverables as they are being used. This is to identify any problems which can be fed back to the technical working group to address. The pilot is usually carried out by end users who have experience in using the current system. Microsoft would often ask people to trial their new version of Windows (beta versions) and feed back any issues they identified.

It is also important that when applying any fixes there is a rollback plan in place. This is the most important aspect of any change management process to ensure that there will not be any impact on how the organisations function. The rollback plan helps to prevent potential downtime as data can be restored quickly from a backup if problems should arise. The

plan will include the detailed steps to be followed should there be a need to roll back the changes to the state before the changes were made.

Test yourself

- 1 Identify the three types of operational change.
- 2 Explain why it is important for businesses to choose the appropriate digital change strategy.
- 3 Describe one example of an unforeseen or previously unpreventable factor when planning digital change.
- 4 Explain the importance of getting 'buy in' from all areas of the business who are affected by the digital change.
- 5 Describe the term 'digital ecosystem'.

1.6 The components of technical change management

Change management does not just happen, it has to be approved, have clear objectives and be planned for carefully.

Change advisory board

This is a group of people who hold change advisory board (CAB) meetings to assess, prioritise, authorise and schedule changes as part of the change control process. The CAB board should include at least one person from each group of people affected by the changes. This would include non-IT groups as appropriate. It can include managers and non-managers, for example a network engineer or business user. It will also include people from the operational and technical areas of the business.

The CAB carry out the following functions:

- ▶ **Prioritise and review change requests** – the CAB review the requests for change and use knowledge, experience and background information to assess the changes for risks and any unintended consequences. They will ask questions to ensure that the proposed changes are fully understood and then evaluate the changes for risks and mitigation, and make sure that the business outcomes are documented. They may also ask for revisions to the original change proposals to address any perceived issues or to seek further clarification. Once this is completed, the changes can be scheduled and prioritised.

- ▶ **Monitor the change process** – the CAB will monitor the proposed changes to ensure that the intended outcomes do not negatively impact the business and ensure that the proposed time schedule does not conflict with the business's needs to operate. In addition, they ensure that the technical and architectural standards are met and determine the possibility of any unintended impacts. During the change process, they will make recommendations to reduce any risks, minimise any negative impact on the business and increase the likelihood of success. Quarterly CAB meetings will be held to review outstanding changes and monitor progress.
- ▶ **Provide feedback** – the CAB team will provide managerial feedback. Feedback is ongoing by the CAB team during the change management process. It begins with the submission of the request for change documentation. As previously mentioned, this is reviewed by the CAB and feedback provided. This may be whether further information is required, whether any adaptations need to be made to the proposal, whether the request for change has been accepted and the timescales when it can be carried out. During the change, the CAB will provide feedback based on their analysis of the monitoring of the change. Finally, they will provide feedback on completion after evaluating the effectiveness of the implementation of the change, the issues that may have occurred, the impact on the business and so on.

Request for change

A request for change is a formal request to make changes to a product or system. The request for change is submitted to the CAB for consideration.

There are different types of requests for change as follows:

- ▶ **Major changes** – these changes may mean a significant change to hardware, software, a product and/or operational processes. These are usually made because of unexpected changes/issues with the technology or a change in strategic planning within the business.
- ▶ **Minor changes** – this is when the CAB have requested minor changes to the request.
- ▶ **Scheduled changes** – business usually have set periods of time when systems, processes and so on are reviewed. The results of these reviews may well identify the need for change. Scheduled changes are predictable and therefore manageable.

- ▶ **Spontaneous changes** – these usually occur when meetings have been held and feedback has been provided about the progress or further identified issues. These should always be kept to a minimum.

Viability

When considering a request for change the viability of the change must be considered carefully.

- ▶ **Finance** – depending on the type of change, the cost of the change can vary considerably. But whatever the cost, it is important that the benefit for the business outweighs the cost. In some cases, the change will cover the costs incurred and possibly increase profits. There is no point implementing a change if it is not cost-effective for the business.
- ▶ **Resources** – resources can be human resources, for example employees from different departments, as well as hardware, software, time and so on. Implementing change management can take time and may involve many people. Depending on the type of change, the people involved may not be able to carry out their normal work activities while working on the change. So, questions have to be answered as to whether there are other people available who could carry out these additional work activities, and whether there will be costs involved. Will the business processes weaken or fail if these people are busy implementing the change? Will there be an impact on the use of the current hardware/software system that will again have an impact on the functioning of the business? It is important to remember that with any change management situation, the business must be able to operate normally, or it will lose money.

Analysis of benefits of implementing the change request

Change requests must be carefully analysed. The impact of each proposed change must be analysed at a high level in order for a decision to be made whether to implement the change or not. When analysing a request for change the following should be carried out:

- ▶ Fact-finding to ensure that the benefits for implementing the change are fully understood.
- ▶ The impact of the change on processes, procedures, documents, workforce and customers should be traced through the entire business to ensure that any impact does not have a negative effect.
- ▶ The impact of the change should be checked with all stakeholders, team members and other relevant people.

- ▶ Identify if the solution is practical and ensure the cost of implementing the change includes the timescales and resources involved.

Stages of approval

The approval procedure for a request for change is an important part of the change management process. This is when the people approving the change request have the authority to determine its fate and either reject it or authorise it.

The **first stage** is to have the request for change accepted for consideration by the CAB. Once it has been accepted for consideration, it moves to the second phase. It is during the **second phase** that the appropriate people who have been included in the CAB look at the request and consider if there are any red flags. This can include the following:

- ▶ Is there a clear strategy to implement the change? If the proposed planning for the change is not well thought out (or does not exist), then this causes confusion as no one can visualise the purpose for the proposed change.
- ▶ Does the entire business understand what the proposed change is, why it needs to take place, who will be impacted by the change, the expected outcome from the change and the tactics used to reach the goal?
- ▶ Is there too much focus on the systems as opposed to the people? The people who will implement the change as well as use and support the changes are as important as the system and technology to be implemented. Any changes should benefit the workforce and increase the efficiency of the organisation.
- ▶ Is there a lack of 'buy in' from people within the business? Every level of the business is crucial to the successful implementation of change. If senior managers do not understand or have confidence in the change, it will definitely be rejected. If middle management, supervisors and team leaders do not 'buy in', then the implementation and execution of the change will suffer and possibly create failure.

The CAB will verify that stakeholders have been properly informed and that all proposed changes align with the business's objectives. The goal is to minimise the risk of downtime and loss. Once this phase has been successfully completed and the CAB can approve the request, it moves to the **third phase** where the changes are implemented.

Setting SMARTER objectives

To give a business direction and for it to have a purpose for its daily activities, it must have aims and objectives. A business aim is the overall goal for the business and the objectives are the steps a business needs to take to achieve the business aim. For example, a business may have a business aim to sell its products worldwide. An objective may be to sell in Europe within the first 12 months, Africa in the following 12 months and so on. Business aims fall into two main categories: financial and non-financial.

Smarter objectives are:

Specific

Objectives that are specific have a better chance of being achieved. To make a goal specific the following should be considered:

- ▶ Who is involved in this objective?
- ▶ What do we want to accomplish?
- ▶ Where is the objective to be achieved?
- ▶ When does this have to be achieved?

Measurable

This is the criteria for measuring progress. A business must be able to track progress and the following should be considered:

- ▶ How much time is required?
- ▶ How will the business know the objective has been achieved?
- ▶ What will the indicator be that progress has been made?

Achievable

An objective must be achievable and attainable. This allows a business to determine how to achieve the objective and work towards it. The following should be considered:

- ▶ Are the required resources and skills available to achieve the objective? What is missing?
- ▶ Have the same or similar objectives been achieved before?

Realistic

A realistic objective is one that can be achieved with the time and resources that are available. The following should be considered:

- ▶ Can the objective be achieved with the resources and time available?
- ▶ Is the business able to commit the resources and time to achieve the objective?

Time-bound

An objective must have a start date and an end date (be time-bound). If there are no time constraints, there is no sense of urgency and therefore there will be a lack of motivation to achieve the objective. A business must consider:

- ▶ Does the objective have a deadline?
- ▶ When must the objective be achieved by?

Evaluate

Objectives should be evaluated on a daily basis. It is important for the business to monitor progress against the SMART indicators as this provides an opportunity to address any issues that may have arisen and/or mitigate any potential problems. The types of questions to be asked are:

- ▶ Are the tasks involved successfully working towards achieving the objective? If not, why not?
- ▶ Can changes be made to remove tasks or make them work more effectively?
- ▶ What is working well and not so well?

Re-evaluate

When adjustments are made to the tasks and objectives, it must never be assumed that it will have rectified a problem or increased the chance of success. In some instances, the changes may make things worse. A business should always re-evaluate the objectives because things can change, such as time and workloads, and also what works today, may not work tomorrow.

Test yourself

- 1 Discuss the role of the change advisory board.
- 2 Explain the purpose of a request for change.
- 3 Describe the stages of approval for the request for change.
- 4 Identify three questions that a business should consider when setting specific objectives.
- 5 Describe the meaning of a time-bound objective.

Risks

Resistance to change from staff/teams

Once a business has identified how digital change can support the overall business goals, it has to convince the stakeholders. This is because digital change strategies change the way a business functions. There is an impact on people's jobs, how they work

together and how they complete tasks. Engaging the stakeholders is not always an easy task for organisations. All staff/teams from the boardroom to the 'shop floor' need to believe that they have a personal and professional interest in the changes being made. It is important that they can understand the reason for the investment so that there is less resistance to new processes. This is extremely important when digital technology is being used to automate processes that would otherwise be carried out by people or when the investment in technology will deliver a profitable return.

Misuse of the new tools and processes

There is always a risk when new technology is implemented that there will be some people who will misuse the technology or not follow the processes correctly. A simple example would be to provide an employee with a smartphone that is purely for work-related purposes. The employee may use it for personal use as well, such as calling friends and/or family, or spend their time on social media or playing games. It is always important that staff are fully aware of:

- ▶ the purpose of the changes
- ▶ why they have been implemented
- ▶ how to use any new equipment/technology
- ▶ the processes to follow
- ▶ the consequences if the correct processes and procedures are not followed.

Inadequate support, infrastructure, or resources

In order to efficiently and effectively implement change management, it is important within the planning stages to give careful consideration to the support, infrastructure and resources.

- ▶ The correct support mechanisms must be put in place and can include regular communication, training on new technology and processes, as well as obtaining feedback from the people involved.
- ▶ Infrastructure can refer to the physical infrastructure such as the technology (networks, equipment, etc.) and buildings, as well as organisational (people's roles and responsibilities when managing and implementing the change).
- ▶ Resources relates to the tools people use, any raw materials used for production and the people involved and the time allocated to them. If these are not carefully planned for and sufficient, then there is a risk that any change will fail or at the very least not be as effective as intended.

Change stalling or impeding workflows

Any change that is implemented should not stall or impede the workflow (overall operation) of the business. A business must continue to make money while these changes are implemented. It is therefore important that consideration is given to how these changes will be implemented. Should the changes be adaptive, where small gradual and iterative changes are made that do not have a negative impact by delaying or preventing the normal workflow to continue? Is there a risk to the daily workflow if there are major transformational changes made over a short period of time? These need to be planned for and implemented in such a way that they minimise any risk to the operational functions of the business.

Knowledge management and single sources of dependencies

Knowledge management is the process of identifying, organising, storing and sharing information, processes and skills within a business. It is a business risk if important knowledge is only known by one person. What if this person leaves the business or is sick, or away on holiday? The business must still be able to function and intended changes must be implemented. When knowledge is not available because a person is not available, it can be very costly to a business as time has to be spent 'finding out' the information as opposed to spending the time on completing the required tasks.

Impact

Forecasting the impact of change implementation on the operational environment

When planning any change within a business, it is important that an impact analysis is carried out. There are three areas of detail to be considered when carrying out an impact analysis:

- 1 The possible implications of making the change.
- 2 The identification of all files, documents and operational processes that may require modification if the change goes ahead.
- 3 The identification of the tasks/activities that are required to implement the change and the time and effort needed to complete them.

Impact analysis is very important for proposed changes where quality and safety could be affected. It is important that the requirements and features that will need to be re-tested after the change has been implemented are fully understood.

Measuring negative and positive impact

There are a number of ways that the impact of change can be measured. This can include using:

- ▶ surveys/questionnaires – given to all relevant stakeholders to obtain feedback
- ▶ data
 - number of sales
 - number of products produced
 - time take to complete tasks
 - costs involved
 - customers – retainment, new customers, customer enquiries, complaints.

It is always important to monitor any change carefully to identify the positive and negative impacts on the business. The monitoring should take place during the implementation of the change as well as after the change has been completed.

Analysis of positive and negative impact

It is no good obtaining information and data from monitoring the impacts of change unless they are analysed and the implications to the business are considered. Analysis of the measurement data and information will enable a business to consider how effective the changes are going to be/have been and whether there are any negative impacts that need to be addressed promptly. Prompt action can ensure that the overall business does not suffer from a financial and/or commercial point of view. If the measuring of the impacts is conducted during the implementation of the changes and the results carefully analysed, it provides a business with the opportunity to re-evaluate the change/changes and implement alternative solutions or address any weaknesses. The analysis can help to establish:

- ▶ any reduction in costs
- ▶ any increase in revenue
- ▶ efficiency of the processes involved
- ▶ speed of any transactions
- ▶ usage rate of the system(s)
- ▶ productivity of the employees
- ▶ customer satisfaction.

Configuration of digital system impacted by the change

Current and proposed

Whenever there are changes implemented in the business environment there are impacts on the digital system(s) involved. The proposed change may be in relation to upgrading or renewing digital systems, or it could be purely process related. It is

therefore important that configuration management is conducted during the change management process. Configuration management is the process of managing the components and/or resources of a digital system on which software runs and configuring them to ensure they maintain a consistent rate of functionality (referred to as the baseline). The components of configuration management are:

- ▶ Identify the items that require configuration, for example networks, servers, digital devices and so on.
- ▶ Label the items requiring configuration with version numbers (this helps with the identification of them).
- ▶ Protect configurable items that are to be used for any upgrading or replacement purposes so that they are securely stored and cannot be accessed or changed by any unauthorised person.
- ▶ Retain baseline and any other relevant information with respect to the configurable items. Records should be kept of when they were implemented, what was changed during implementation and who made the changes. The records should also include the location of the configurable item, what the proposed configuration changes are and the person responsible for carrying out the configuration changes.
- ▶ There should be a configuration verification and audit log that confirms that the configurable items are checked regularly to ensure that they are in the consistent state (baseline) and function as intended.

Rollback planning – recovering to a previous stable configuration

Have you ever used system restore on your computer, laptop or smartphone? If you have, you have rolled back your device to a previous stable configuration. A rollback plan is a recovery plan that allows the system to be restored to its 'last known good state'. A rollback plan is an emergency escape to restore the system if something goes wrong (especially if it stops functioning as intended).

Backup methodology

A system backup ensures that not only is the organisation's data saved, but also the operational condition of the system. This is useful when restoring a system to the last saved state along with all selected backup data. The system backup is carried out using backup software and the generated system backup is known as the 'snapshot'/image'. In a networked environment, the system backup file/image/snapshot

is routinely uploaded and updated on a local/remote storage server.

There are four main types of backup:

- 1 Full backup** – this is a complete backup of every file and folder stored on the system. They take up more space and require more time to carry out than other types of backup. They are, however, the most comprehensive form of backup. It is much faster to restore lost data from a full backup.
- 2 Incremental backup** – an initial full backup of the system is created. All subsequent backups only backup files where there has been a change since the previous backup. Many organisations use full and incremental backups to store files during different backup windows.
- 3 Differential backup** – this creates an initial full backup of the system and then every following backup only stores the files that have changed. The same changed file will continue to be backed up until there is another full backup carried out.
- 4 Mirror backup** – this stores an identical copy of the source data. It is an exact copy of the system at a given time and is much faster to backup.

Local/cloud

- ▶ **Hot site** – this is a backup site which runs continuously. It enables an organisation to continue with its business functions and processes quickly should an issue occur such as a system failure and so on. A hot site can be configured at local level (within the premises of the organisation), a data centre or in the cloud. A hot site must always be online and available. In addition, it must be equipped with the required hardware, software, network and internet connectivity. Organisational data is regularly backed up and replicated on the hot site so that it is readily available should a disaster occur. The hot site must be located far away from its original site location so that it can not be affected by the same disaster as the main site.
- ▶ **Warm site** – this is also a backup site, but it is not equipped in the same way as a hot site. A warm site is configured with phones, power, network and so on and may have many servers and other resources. However, it is not available for immediate switchover should a disaster occur. While it is not as fast to switch over as the hot site, it does cost less.
- ▶ **Cold site** – this contains fewer facilities than either the hot site or the warm site. It takes longer to switch across to a cold site as opposed to the hot site

and warm site should a disaster occur. However, it is the cheapest option.

Disaster recovery planning

This is a formal documented plan created by a business that provides instructions on how to respond to an unplanned incident with the digital systems. These could be environmental factors (e.g. flood or fire), cyber attacks, power outages or any other incident that is disruptive to the operational functionality of the business. The aim is to enable a business to be restored to normal key operations as quickly as possible.

Any interruption in the functioning of a business can result in a loss of revenue, business reputation/brand damage and customer dissatisfaction. Therefore, a well written, careful thought-out disaster recovery plan is extremely important.

Reproducibility

Replicating change across other departments or businesses

Change management can be in relation to one particular aspect of the business, or it can be a major change across the entire organisation. It is therefore important that the proposed changes are planned carefully with the same care and consideration to ensure that there is no disruption to any department or associated business. Lessons learned from implementing change in one department may need to be taken into consideration when implementing the change within other departments or businesses involved.

Test environment – servers and software

The test environment is often referred to as the 'sandbox'. It is an environment that includes the technologies and software required for the business to operate effectively and efficiently and will of course include any new or upgraded hardware and software.

Refer to section 11.1, p.271 – the purpose of testing digital components.

Traceability

It is important for any digital change management that the requirements are clearly defined. There are two important questions that need to be asked:

- ▶ Who has the authority to change the requirements?
- ▶ What is the impact of the change?

In order to answer these questions, a business needs requirement traceability. Requirements need to be traceable (forward and backward) through every stage of the change that the requirements have an impact on. Traceability also tracks the workflows that create, relate and change the requirements and components/processes and so on. Having all of this information in one document allows flexibility, user access and traceability. Without traceability, it cannot be proved that a specific requirement has been met and as intended.

Responsibility

Within the traceability for change there are people who have specific responsibilities with respect to providing input, monitoring, analysing and keeping the document up to date. Below are typical roles and responsibilities that may be used for the management of traceability.

- ▶ **Creator** of the management traceability record – this is usually a business analyst with supporting input from the project manager.
- ▶ The traceability log is usually approved by relevant personnel from the various areas of the change management process. For example, if part of the change is to install new digital production equipment, then the production manager would be involved.
- ▶ **Business experts** who were involved with the instigation of the proposed change and requirements will also have responsibilities within the traceability log, whether it is to provide information and/or to review content and confirm its relevance and accuracy.
- ▶ The **business analyst** will collect, analyse and document the requirements.
- ▶ The '**change designer(s)**' will use the requirements to design the solutions.
- ▶ The **developer(s)** will develop the solutions based on the design to the determined requirements.
- ▶ The **testers** will verify that the solution(s) satisfies the requirements.
- ▶ The **change manager** will provide reports on the status of the change management.
- ▶ There may be a **change management analyst** who will determine the organisational change due to the requirements. Depending on the size of the business, this may be carried out by the change manager.
- ▶ The **business analyst** will maintain the traceability log.

Accountability

When people are given roles and responsibilities within a change management project, they are all accountable for the aspects of the change that they are responsible for. This also includes being accountable for the actions of anyone in their team. If, for example, there is new digital equipment being installed on a production line, then the production manager has accountability to ensure that their staff receive appropriate training on how to use the equipment and relevant software, that they are monitored and provided with support and so on.

Auditing

Auditing allows the business to use traceability to ensure that requirements/requests have been met and to identify any non-conformances/deviations in the delivered outcomes.

Document

Documentation for change management is extremely important. A document control system should be in place to ensure that when a change takes place, the process and the documented process are the same. Documentation reviews should take place to ensure that all relevant documents are still accurate and apply to the processes implemented.

Maintaining up-to-date information

As stated above, it is important that any information is kept up to date. This can relate to the changes made to processes, the details of any upgrades, additions or changes to equipment as well as the stages of the entire change management process. Up-to-date information ensures that not only can the stages of the change be tracked and monitored more effectively, but it can also help to identify where something has gone wrong.

Recording all decisions

All decisions within a change management process must be recorded. This is not only the decisions prior to the change being implemented, but also while the change is taking place. This also has to include any decisions that were made where adaptations to the planned change were required. It is important to be able to look back through the stages of the change process and monitor the decisions that were made, and, if amendments were implemented, when, why and by whom these decisions were made.

Retaining change documentation

Any documentation relating to change management should be retained for future reference. It may be required if a situation occurs which has a negative impact on the business. By reviewing the change management documentation, it can be used to consider:

- ▶ whether this negative impact could have been avoided
- ▶ if it had been previously identified, what within the change management process had not addressed the problem
- ▶ whether any adaptations to the change management implementation had caused the problem.

User training materials

Whenever there is a change to processes, equipment, software and so on there should be training materials available for the people who have to implement the new processes and/or use the equipment/software. They can be used as a resource to enable the workforce to 'check up' if they are unsure or come across a problem. User training materials must not be too technical, so that the user can understand them. Not all users are technical experts.

Version control

Documents should always state what version of the document it is, the date it was changed and who made the changes as a minimum. There should also be a version control log to record the details of the document that has been changed, its new version, the date and so on. This helps to ensure that only the current documentation is being referred to.

Version control is always important when documents are being created and for any record where there are numerous revisions. It not only helps to track changes, it also identifies when key decisions were made. This is especially important for electronic documentation that may be reviewed by different people. It is always important to know what version of the document they need to work on.

Test yourself

- 1 Identify three possible results from the analysis of positive and negative impacts of change.
- 2 Compare and contrast the different backup methodologies.
- 3 Describe the term 'traceability'.
- 4 Explain the purpose of version control.
- 5 Describe disaster recovery planning.

1.7 Factors that drive change and a range of methods organisations can apply in response to change

There are many factors that drive change within an organisation. Organisations must select appropriate methods to implement changes. The method used will be very much dependent on the type of change, for example developmental, transitional and transformational.

Internal factors

Restructuring

Businesses may consider restructuring to remain in business and competitive. A restructure is a change to how the business is managed, the job roles involved and the responsibilities within the job roles. Restructuring can be required when there is a change in the marketplace, changes in customer demands, planned growth, introduction of new technology, change of location and so on. Restructuring may not be the entire business but just a department; however, what changes in one department can affect another.

When considering a restructure, the business needs to consider whether there will be any shortage of staffing in any area as well as any skills shortages. The job roles should be based on what the business needs to operate effectively. When planning a restructure, businesses must consider:

- ▶ Will there be any redundancies?
- ▶ Will there be a need to recruit more staff?
- ▶ Will staff need additional training and support (to address any skills gaps or change in operational processes)?

Expansion/growth

Expansion/growth within a business can also mean that the business must consider a restructure (as explained above). As a business increases its customer base/products/services, it may need to consider changes that will enable the business to:

- ▶ sustain its place in the marketplace
- ▶ retain its customers
- ▶ provide its products/services effectively and efficiently.

This can include changes to:

- ▶ digital systems for processing and storing data and information

- ▶ production processes by implementing new and emerging technology
- ▶ interaction with customers, developers, designers and so on.

Downsizing

Downsizing is not necessarily a negative change for a business. It may just mean that the business has changed the way it operates. Consider a business that had many bricks and mortar retail outlets. Recent changes to customer behaviour and the necessity to sell online has resulted in the business making changes to the way it operates. It may reduce the number of premises that it uses (or dispose of them altogether) as it moves to selling online only.

When emerging digital technology is implemented, it can mean that there is a reduction in the number of staff that are required to perform certain job roles. This can mean that staff are redeployed to other areas within the business or made redundant as their job role no longer exists.

New strategic objectives

Strategic objectives are the overall goals of a business. They describe what the business will do to achieve its overall aim. They are usually associated with some form of performance goal such as:

- ▶ launching a new product/service
- ▶ increasing profits
- ▶ expanding the market presence for its products/services.

New strategic objects involve change in some way or another. They may require the implementation of upgraded/new digital technology or changes to operational processes and so on.

External factors

Political

The political environment has an impact on the economic environment of businesses. In section 1.2

Research

Research the impact Brexit has had on international trade deals. Consider the following:

- ▶ What has the impact been on businesses within the UK?
- ▶ How has this driven them to make changes to the way they operate?

Produce a report on the results of your research.

you learned about a number of political factors that can influence the business environment. The impacts that these have on a business can drive change.

Change in government

With any change of government, there is usually a change of policy and regulation. These changes can be in relation to:

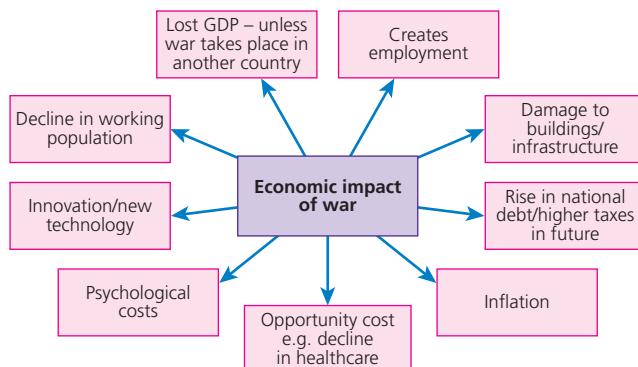
- ▶ local and international trade
- ▶ taxes such as import and export duties
- ▶ minimum wage levels for employees
- ▶ VAT and taxes.

These can all have an impact on the business environment, some in a positive and some in a negative way.

Refer to section 1.2, p. 6 where political factors that influence the business environment is covered.

War

As well as the loss of human life, war can have a serious economic impact that can therefore have an impact on the business environment. Figure 1.1 shows the negative and positive impacts war can have on the business environment.



▲ **Figure 1.1** The positive and negative impacts of war on the business environment

The impact depends on whether the war is in the country where the business is or in another country.

Activity

Have a group discussion about the different ways that war can impact on the business environment and the types of changes that businesses may need to implement in order to survive.

Make notes and prepare a newspaper article entitled: 'War and the impact on the business environment – why businesses need to implement change'

Economic

In section 1.2 you learned about the economic factors that influence the business environment and the impact that they can have on a business. These impacts have to be carefully considered by businesses and what changes they may need to make in their operations in order to remain viable.

Meeting new funding/revenue streams

Revenue streams are various sources from which a business can earn money from the sale of goods/services. The types of revenue/funding depend on the types of activities carried out. In order to improve the business with respect to operations and profit, a business must consider the following:

- ▶ How does the business make money?
- ▶ Are the current revenue streams the most appropriate for the product/service?
- ▶ How can the current streams be changed to increase the income to the business?

The revenue stream will usually depend on the products/services offered by a business and the spending behaviours of the customers. Revenue streams may include:

- ▶ income from the sale of goods/services
- ▶ interest revenue – money earned from investments such as debt securities
- ▶ rent revenue earned from renting out buildings and equipment
- ▶ dividend revenue earned from holding shares in other companies. If the company that a business holds shares in makes a profit, then the shareholders are paid a dividend (given a percentage of the profits based on the number of shares they hold).

Funding streams are the sources of finance available to businesses. There are two main ways that they are financed, debt or equity.

- ▶ **Debt** financing includes business loans (for major business purchases, for example very expensive equipment/technology, buildings) and short-term loans to finance the cost of new equipment over a shorter time period. These types of funding streams require the business to repay scheduled payments, for example monthly.
- ▶ **Equity** finance is provided in exchange for the sale of ownership interest to another person or group of people. These can be in the form of selling shares on the stock market or from private investors.

Businesses may want to use these sources of funding in order to drive the change within the business operations

in order to purchase for example new equipment to produce newly designed products. In order to access any form of funding, a business would have to prove that:

- ▶ it is currently viable
- ▶ it is making a profit
- ▶ the proposed change or changes will enhance the business further.

Recession, inflation and consumer trends

Economic factors can have a positive and negative impact on businesses. It is important that they study them carefully and consider how they can implement change into the business in order to operate at the highest possible level and maintain good profit margins.

Refer to section 1.2, p. 7 – economic factors.

Social

Change in human behaviour

Human behaviour can change based on the political and economic environment. These factors have been discussed previously in section 1.2 and within previous sections of 1.7. Human behaviour can mean a changing market with changing needs. Customers will need to consider this and the changes that may be needed so that they can continue to function as a sustainable business.

The changes in birth rate can also drive change within the business environment. A change in the demographics of the world's population is one of the biggest changes to the global economy. Table 1.1 contains some of these challenges.

Market/social trends

Society continually changes, for example changes to tastes in fashion. In addition, the ever-increasing popularity of social media among younger people means that the younger consumers have 'grown up' using digital technology such as smartphones, tablets and computers. People who use digital technology tend to shop online whereas older people will continue to visit shops. These changing factors drive change within businesses in order to continue to reach their customer market. The number of businesses implementing change to provide online shopping platforms continues to increase.

Market trends also change continually. Market trends are anything that changes the market in which a business operates. Consider digital technology and how this has changed over the last two decades. It would be bad business practice to continue to produce and sell outdated technology. Businesses need to

Challenge	Impact
Reduced workforce	If birth rates fall, the working-age population will eventually fall. This will lead to a shortage in labour in countries where there is a decline in the working-age population. This slows down the growth in many of the different industries and has a negative impact on the country's economic competitiveness. If birth rates were to increase, then the impact would be more positive.
Reduced number of consumers	When the birth rates fall and the working-age population also declines, there are fewer consumers. This reduces the potential for growth for businesses. Fewer customers results in businesses not having the necessity or opportunity to expand their business, unless they consider diversifying in some way.
Older population	The life expectancy of many populations has increased. If this is also considered in association with lower birth rates, then the average age of the population also increases. This is why people are encouraged to work past the legal retirement age. If older people cannot work, they are not economically productive, and this will put a strain on the economy.
Reduction in wealthy marketing environments	Wealthier countries tend to have lower birth rates. This results in small segments of the population having a greater concentration of wealth as the business opportunities for growth become more focused. But this also means that poorer countries have a reduction in export opportunities as the growth in rich markets slows down.
Incentive for greater automation	If the labour market shrinks (fewer people available for work), then the incentive for implementing automation will increase. As population growth continues to slow down (due to lower birth rates), productivity needs to increase in order to maintain economic growth. Automation is an important consideration to address this issue.

▲ **Table 1.1** Challenges presented by change in the demographics of the world's population

implement change so that they can keep up with the needs of the market trends and remain viable.

Refer to section 1.2, p. 7 – social factors, market trends.

Refer to section 1.3, p. 11 – sales and marketing.

also known that people with a higher education level are more demanding. Businesses need to analyse their potential customer market and consider the changes needed to meet their demands (and budget).

- ▶ **Economic growth** – the higher the economic growth of an area or country, the greater access the population has to income.

Refer to section 1.2, p. 7 – social factors, socioeconomic aspects.

Socioeconomic aspects

Socioeconomic factors are characteristics that influence consumers. They are associated with the quality of life of individuals and families, and determine their behaviours, their preferences, attitudes, tastes and lifestyle.

These factors have an impact on businesses and the business environment. Consumers affect the growth of businesses. Therefore, businesses need to consider what these factors are in order to compete in a market that is forever changing.

- ▶ **Occupation and income capacity** – the amount of money people spend depends on what they earn. The amount they earn from employment can also depend on their occupation. The more money they earn, the more they have to spend on products and services. It is therefore important for businesses to consider changes that they may need to make so that they can meet the needs of a range of customers with varying incomes.

- ▶ **Level of education** – education can also influence the type of occupation that a person can have and therefore their income level. Education determines the occupational opportunities available to them and so influences how much they can afford to spend. It is

Remote working

While remote working is becoming more and more acceptable, it presents challenges to businesses. For it to work successfully with continued productivity and support for the customers, it is necessary for businesses to make changes to the way the business operates. Businesses should consider the following aspects of remote working and implement change to address any risks:

- ▶ **Communication** – regular communication between the management team and the workforce is important. Remote workers still need to feel part of the business environment and receive updated information, participate in business projects and ideas, and have the appropriate access to 'tools' to enable them to carry out their work activities.
- ▶ **Technology and security** – remote working can be very effective, but it comes with challenges, especially with respect to the security of data and information. For businesses working in a global market, the reliability of technology and the

technological infrastructure in different countries has to be considered. The remote working environment can also create privacy issues. There have been occasions when sensitive business information has been ‘leaked’ to the national press or social media through overheard conversations on trains and in cafes, or lost flash drives and laptops left behind on public transport. Businesses have to implement changes to mitigate against risks to enable remote working to function effectively, efficiently and safely.

Cultural expectations

Refer to section 1.2, p. 7 – social factors, cultural expectations.

Technological

Emerging technologies

Businesses must constantly look at opportunities to benefit from technology as well as anticipate any future changes. A business that does not consider emerging technologies is at risk of reducing its profits or potential for survival in the marketplace. It is also important for businesses to determine what changes should be made, and manage any cultural changes that are needed, to successfully implement any new technology.

Refer to section 1.2, p. 9 – technological factors.

Artificial intelligence

AI is the simulation of human intelligence in machines that are programmed to think like humans and imitate their actions. It also includes any machine that can learn and problem solve like the human mind.

Banks use AI for online banking where customers can now deposit their cheques into their account from home by taking a photograph of both sides of the cheque and uploading it into the bank’s online banking portal. The identification of credit card fraud is based on AI, where the system learns the spending habits of the customer and notifies the bank when abnormal spending appears to be taking place.

Innovation/efficiency

Innovation and efficiency are of paramount importance to a business. The business environment is highly competitive and customer expectations are becoming more demanding. Businesses need to demonstrate that they are forward thinking, with effective and efficient operations to meet the demands of their customers.

Technology plays a big part in driving change within the business environment. The changes do not have to be on a grand scale, but any changes must be effective. Innovation could be, for example, in relation to product

designs or a way to conduct business with customers. Businesses that are innovative and efficient will have a much higher chance of retaining their customers, attracting new customers and ultimately making money.

New payment methods

Payment methods have changed rapidly due to the increase in the use of smartphones and the increase in e-commerce. There are a number of reasons why changes have been made to the way people pay for goods and services:

- ▶ E-commerce and online shopping are fast and convenient. Customer expectations have therefore changed, and they expect payments to be processed quickly. Due to digital technology, customers expect a more rapid service.
- ▶ While customers adapt to new payment mechanisms, the payment industry recognises that customers still need a variety of options on how to pay. Customers may want to pay by cash, cards, bank transfers, digital wallet and so on.
- ▶ Emerging technologies and adaptations to existing technologies have provided customers with a variety of ways to pay. Smartphone technology in particular has provided customers with a range of services using ‘apps’. This can include mobile banking and apps for booking taxis and hotels.

Case study

A footwear retailer is planning to open an e-commerce business. They are in the process of planning for the change but need information about the different payment methods that are available to customers that purchase goods online.

You have been asked to research the different payment methods available to online customers and prepare a presentation to the retailer explaining:

- ▶ the different payment methods and how they function.
- ▶ the changes that the retailer would need to make to their operations and processes to support these payment methods.

- ▶ Regulation and legislation define how payment service providers and customers interact, exchange data and make payments. Regulations support innovation, encourage competition in the marketplace and protect customers.
- ▶ Payment service providers compete by providing new products and services to customers. The new payment services are a result of industry-driven collaborative initiatives, for example contactless technology on cards.

Legal/regulatory

Legislation, including new legislation and updates, and standards, are covered in Core element 8.

Legal factors are covered in section 1.2, p. 9.

Removal of European Union legislation

From 1 January 2021, the EU trade mark no longer protects **trade marks** within the UK. The Intellectual Property Office (IPO) in the UK created a UK trade mark that was comparable with the EU for all holders of an existing EU trade mark. This is referred to as the UKCA.

UK businesses that have an EU trade mark still receive protection in the EU Member State countries and UK businesses are still able to apply for the EU trade mark. Businesses are not charged for changing to the UK registered trade mark as a result of the UK leaving the EU (Brexit). Also, Community Designs (RCDs) and unregistered Community Designs (UCDs) are no longer valid in the UK. These were replaced by UK rights.

It is important that businesses consider the requirements for different legislation and regulation dependent on where they operate. If a business operates within the UK and on the global market, they must ensure that they comply with the regulation and legislation for each country.

Research

Research the meaning of RCDs and UCDs.

Prepare an information leaflet explaining what they are and their purpose.

Environmental

Sustainability

It is important for businesses to demonstrate that they are not having a negative impact on the environment in order to sustain growth. Businesses need to look at how they:

- ▶ operate their business
- ▶ transport their products
- ▶ travel
- ▶ operate in general.

All industries must meet targets to halve global greenhouse gas emissions.

Businesses can support environmental sustainability by implementing digital technologies.

Energy efficient technologies such as 5G, the Internet of Things and AI can provide new ways within the sectors of energy production, agriculture, land use, building, transportation, traffic management and services. Mobile broadband networks provide opportunities to improve social inclusion, economic growth and productivity on a global scale.

The importance of environmental sustainability has to be considered by all businesses and they have to consider the changes that they must make to their operations in order to comply with legislation and regulation.

Reduction in carbon footprint and use of green energy

There are many reasons why a business would be eager to make sustainability part of its business and therefore reduce its **carbon footprint** as part of its image. Consumers in particular are demanding that the businesses they use take action to reduce their impact on the planet and tackle climate change. Reducing their carbon footprint and using **green energy** also helps the business to cut costs. Below are some of the ways that a business can reduce its carbon footprint and use green energy.

- ▶ Reduce emissions by travelling less and using video conferencing software.
- ▶ Switch to green energy, for example solar powered energy, wind farms, efficient office lighting, for example LED bulbs, room sensors to turn lights on and off dependent on whether there is any movement in the room, or asking employees to turn lights off in rooms they are vacating.

Key terms

Trade mark: a word, name, symbol, design, or a combination of them, used in commerce to identify and distinguish the goods of one manufacturer and/or seller from those of another manufacturer/seller. It also indicates the source of the products.

Carbon footprint: the amount of carbon released into the atmosphere from the activities of individuals, organisations and communities.

Green energy: a type of energy that is generated using natural resources such as sunlight, wind or water. Green energy does not harm the environment by releasing greenhouse gases into the atmosphere.

- ▶ Reduce the amount of energy used in data centres and communications rooms by:
 - setting cooling systems for keeping the equipment cool to a higher temperature
 - setting up hot and cool sections within the room
 - using plastic curtains to prevent air of different temperatures mixing.
- ▶ Reduce, reuse, recycle – this includes water, paper, food and drink, packaging, laptops and smartphones. Businesses can purchase recycled paper and reconditioned IT and phone equipment.
- ▶ Reduce the use of single-use plastic, for example plastic cups for water.
- ▶ Reduce food waste, for example if a business has a canteen, kitchen staff should be encouraged to minimise food waste.
- ▶ Keep printing to a minimum.

Research

Research the different forms of green energy and consider how a manufacturing business could implement change to use green energy.

Produce a report of the results of your research.

Digital/tech waste

Often referred to as e-waste, this is any electrical or electronic equipment that has been discarded. It is very toxic due to the chemicals that leak from the metals the equipment contains. Digital devices are manufactured using rare materials. By minimising digital/waste, it helps to conserve resources and reduces the amount of material taken from the earth. Businesses are required to consider the amount of digital/tech waste that they create to sustain the environment (see the section on sustainability above). Businesses should:

- ▶ re-evaluate – whether they need the digital device/equipment
- ▶ extend the life of the equipment they have by careful maintenance
- ▶ purchase digital/tech devices that are environmentally friendly, for example LED light bulbs
- ▶ donate redundant equipment to social programmes to raise money to support people who are disadvantaged
- ▶ reuse digital/tech equipment where possible
- ▶ recycle digital/tech waste using professional recycling companies.

Digital/tech waste includes:

- ▶ cell phones/smartphones
- ▶ desktop computers
- ▶ laptops
- ▶ monitors
- ▶ circuit boards
- ▶ hard drives
- ▶ copiers/printers
- ▶ IT server racks
- ▶ IT servers
- ▶ cords and cables
- ▶ Wi-Fi dongles
- ▶ phone equipment
- ▶ audio/video equipment
- ▶ network hardware (e.g. servers, switches, hubs, etc.)
- ▶ power supplies.

Pandemic

Pandemics can be on a global scale or just within a few countries. This has a major impact in the way businesses function. Employees may have to work from home (isolate), and customers may not be able to visit the business premises and will decide to ‘purchase online’ instead.

In order to survive, businesses have to implement change very quickly. In recent years, there has been an increase in online shopping and therefore more and more businesses have had to move their operations online (e-commerce), restaurants have had to close and therefore have offered a ‘take away’ service for customers. For employees who are normally office-based, businesses have had to implement remote-working and provide employees with equipment they can use from home as well as access to the software, files and documents they would have had access to within the office.

It is important that businesses act quickly, but also plan carefully for such situations and take advantage of the digital technology that is available to maintain operations.

Competitors

New product/services

Businesses cannot assume that their products and services will maintain a high level of customers. New products/services are appearing in the marketplace all the time and customers can easily change what products/services they buy and from whom. Businesses need to be creative and ensure that the products/services that they sell are up to date, reliable, will attract new customers and most importantly retain current customers. Careful market research should be conducted to see what is

being offered by competitors and how the business has to implement change to compete with them.

Entering new markets

Businesses who have, for example, decided to use social media to advertise their products/services, must research carefully the companies that are also using social media to sell the same products/services. They should explore how these companies are making the most of the social media opportunities available. Businesses would therefore need to consider their marketing strategies, what products/services they want to promote to a larger audience and so on. If a business wants to expand into a different market from the one they normal work in, they need to consider:

- ▶ what products/services they could sell
- ▶ how they are going to sell them
- ▶ who the intended target audience is.

This takes careful planning and will require changes within the business's operations and functions.

Methods to respond to change

New or amended

- ▶ Whenever a business's plans change, whether it is a forced change through legislation or a business strategic decision for change, it has to consider the **policies** that are already in place and whether they need to be amended or if new policies are required. Health and safety policies in particular may need to be amended due to new health and safety legislation and regulation and/or because new equipment will be installed.
- ▶ Whenever digital technologies are planned for change, the **processes** already carried out by the businesses must be analysed and may require amending or a new process introduced, for example the process for running and using new digital technology.
- ▶ Any changes such as amendments to **products/services** or implementation of new products/services, will require businesses to consider how these changes will be implemented, the processes involved, any legislative requirements and changes in regulation. This is an important aspect of any implementation for change and drives the change within the business environment.

New/improved digital systems

Global trade is expanding rapidly, resulting in businesses implementing changes. Technology

provides the means to implement these changes allowing businesses to bring new products to the marketplace and meet customer demands for quality. In order to compete in the international marketplace, businesses must reduce costs and product development times. This requires the removal of time-consuming development and administrative processes and procedures. Quality global standards and business processes also continue to grow; this has increased the need for businesses to use technology to implement the changes required to meet them.

- ▶ **Operations** – technology can help businesses to manage the changes to their operations. Businesses can reduce costs by analysing the business processes and removing activities that customers do not believe are valuable. For example, time-consuming application processes, purchasing of products/services, purchasing of flight tickets and so on. Businesses face the challenge of transferring their focus on projects to develop new and innovative products/services and increase revenue.
- ▶ **Support** – by analysing how different departments within an organisation use internal support services, a business can identify functions that can be shared by multiple departments through the use of shared technology. By implementing automation, businesses can remove duplication and if appropriate outsource some of the administrative functions. It is important, however, that businesses consider the return they will have on any investment when implementing new or improved digital systems. It is important that any implementation benefits the business as a whole and not just a few staff members.
- ▶ **Centralising systems** – businesses can use new and improved digital systems to centralise, for example purchasing and logistics, and that in turn reduces costs. Communications technology allows businesses to integrate their digital systems with their customers and suppliers. The marketplace is fast-changing, and decisions can be made more quickly and efficiently to address these changes.

It is important, however, that businesses do not just consider any current and beneficial opportunities, but also anticipate what future changes may occur.

Training needs analysis

A training needs analysis (TNA) is a process that a business must go through to determine the training that must be completed over a set period of time

to allow the workforce to complete their roles and responsibilities efficiently and effectively. It also allows a business to progress and grow and is especially important when implementing change by using new and improved digital systems. There are three main steps that a business should follow:

- ▶ decide on the skills sets that are required
- ▶ evaluate the skills of the staff
- ▶ identify any skills gap.

The benefits of a business conducting a TNA are:

- ▶ It identifies any knowledge and/or skills gap before it becomes a problem. For example, it would not be good business practice to install a new digital production line if the workforce do not know how to use it.
- ▶ It is much easier for a business to schedule any training and decide on what order training should be conducted, when it should be available and so on.
- ▶ It can highlight training that a business may not have considered.
- ▶ It ensures that any training is focused on the correct areas of the business.
- ▶ It helps to identify the members of the workforce who need to attend the training.

Restructuring of priorities and resources

Whenever a business is planning to implement change, it is important to prioritise the changes and to analyse carefully the steps taken to implement the changes. For example, if the changes include new technology, how will this be incorporated into the current digital systems and what are the stages for this process? It is also important to consider the resources required, for example what resources are required, when they will be available and over what time period. Any change must not have a negative impact on the functioning of the business and therefore must be carefully planned for.

Test yourself

- 1 Describe how the removal of European Union legislation drives change for businesses.
- 2 Identify three internal factors that can drive change in the business environment.
- 3 Describe the term 'training needs analysis (TNA)'.
- 4 Discuss how social factors drive change in the business environment.
- 5 Explain how businesses can reduce their carbon footprint and how it drives change within the business environment.

1.8 The steps taken to respond to change

Change management for any organisation, large or small, requires careful planning, managing and reinforcement in order to succeed.

Planning for change

It is important for businesses to create a change management plan. This helps to manage the changes to processes, and helps to control budgets, schedules, scope, communication and resources. A change management plan can reduce the impact the change has on the business, employees, customers and other stakeholders.

Setting budgets and timescales

Invariably change costs time and money. In order for any change to be approved, it must be cost-effective and achieved in a reasonable timescale without causing any negative impact on the business and its customers (and suppliers).

Budgets must be created for the cost of resources such as equipment, materials and the cost of the time for people to support the implementation of the change.

Timescales must be identified to include when phases of the change will be implemented and when the complete change will have taken place. If timescales are not adhered to, this can have a negative impact on the budget and there could be a situation where there is no further money available to continue.

Careful analysis of the cost of the equipment to be purchased as part of the change must take place. When purchasing equipment, materials and so on, it needs to be considered that prices may increase prior to the purchases being made.

Communicating the change activity to all stakeholders

Once a business has identified how change can support the overall business goals, it has to convince the stakeholders. This is because change strategies change the way businesses function. There is an impact on people's jobs, how they work together and how they complete tasks. Engaging the stakeholders is not always an easy task for organisations. All staff from the boardroom to the 'shop floor' need to believe that they have a personal and professional interest in the changes being made. It is important that they can

understand the reason for the investment so that there is less resistance to new processes. This is extremely important when digital technology is being used to automate processes that would otherwise be carried out by people or when the investment in technology will deliver a profitable return.

Clarifying resources required

When implementing any form of change within an organisation, it is important that all resources required are identified and that associated costs are factored into the overall budget. The resources required will depend on the type of change taking place. Types of resources include:

- ▶ **hardware** – these could be digital devices, new robotic equipment, servers, laptops, desktops and so on.
- ▶ **software** – new technological equipment may require specialised software to run them. New devices such as laptops, computers, smartphones, will require applications (and in some instances operating systems) to be installed in order to function with the other systems already in place.
- ▶ **staffing** – change does not happen without the assistance of people. It is therefore important that the staff who are going to be involved in the implementation of the change are identified and their roles and responsibilities within the change process clearly defined.

Managing change implementation

Before the launch of any change the following checks should be confirmed as complete.

- ▶ Is there a digital statement that expresses the goals and methods to be used to achieve the goals?
- ▶ Have the stakeholders been contacted and are they on board with the planned changes?
- ▶ Has a centre of operations within the organisation been set up to lead the digital change process and monitor its progress?
- ▶ Are there records of any problems within the process including employee grievances, resistance to change and the abolition of or adaptation of traditional business methods?

Monitoring progress during implementation of change

The monitoring of change should be, where possible, an automated process as it is more convenient and

accurate. Change monitoring should include each of the following:

- ▶ **Real-time change reporting** – this will ensure that there are no negative changes inadvertently taking place, and should something occur, it can be acted upon quickly and rectified.
- ▶ **Centralised audits** – this would be a single storage location of changes made to critical files and configurations that identifies who made the change, the location and the time.
- ▶ **Understandable reporting** – any alerts and reports should be easy for the relevant member of staff or team to understand. This will reduce any margins of error.

It is important to monitor the progress of change to ensure that budgets have not been overspent, timescales are on track and that there have been no negative impacts to the business or their customers.

Maintaining quality of service during change

By maintaining quality products and/or services, businesses have the potential to retain their customers and meet customer expectations and satisfaction. Businesses can succeed or fail based on the customer perception of how they operate, and the products/services provided. During any form of change, businesses cannot allow the quality of service to be impacted in a negative way. Businesses have to ensure that the implementation of any new technology, equipment and/or processes, does not have a detrimental effect on their reputation.

Business acceptance and compliance with change

Change may be required for a number of reasons, but it is always important that any changes are accepted within the business and by external stakeholders, for example customers, suppliers, regulatory bodies and funding bodies, for example banks, shareholders and so on. Businesses must always ensure that they have the acceptance of all relevant internal and external stakeholders as well as ensuring that they are compliant with any regulations and/or legislation. If the change did not comply with regulation/legislation, not only would money be wasted, but it would damage the reputation of the business, and potentially levy heavy fines. Without the acceptance of the internal stakeholders, the implementation would not run smoothly and there could even be serious consequences such as staff resigning from the business. External stakeholders could withdraw their funding and support.

Team upskilling and development to facilitate the change

Change invariably requires the upskilling and development of the workforce, whether this is with respect to the use of new equipment/technology or on new/amended processes.

Refer to section 1.7, p. 42 – training needs analysis.

Communicating outcomes of change

There should always be regular update meetings for all relevant stakeholders during the implementation of change and once it has been completed. When identifying the changes, the risks involved are also considered. These must be communicated to all relevant stakeholders (internal and external to the organisation). The communications must be positive and timely.

It is important that the internal and external stakeholders, including end users are confident in the changes being made and that any changes will not create too much disruption to them. Communication can include online meetings, email, website and social media postings. Communication should continue during the implementation of the change and after it has been completed.

Post-project reviews

Post-project reviews (PRRs) are carried out when the change has been implemented. They are used to identify lessons learned from what went well and what did not go so well, as well as what could have been done better. A PRR is used to promote collaboration and agreement on what and why there were advantages, disadvantages, benefits and limitations of doing things in a certain way.

Reinforcing change

The purpose of reinforcing change is to sustain change, in other words to maintain the change even after it is completed. Without reinforcement, people such as employees may revert to the 'old ways' of doing things. This can occur because:

- ▶ people prefer what is comfortable, familiar and easy
- ▶ people who resisted the change may continue to resist it even after the change has been implemented.

If change is not reinforced, then all the effort of implementing the change may be wasted.

Reinforcement planning

► **Checking change is implemented** – when planning reinforcement of change, it is important to ensure that the actual desired change has been implemented. Once this is confirmed, then it is possible to identify what changes were required to processes, procedures, working practices and so on and whether these have also been implemented. It is then necessary to review whether these changes have also been adopted by the staff. If there are desired changes that have not been implemented, then questions should be asked as to why this is the case.

► **What steps to take if change isn't implemented quickly enough** – if it is identified that change has not been implemented in the appropriate timescales, then it is important to see what the reasons are and what impact this is having on other areas of the overall change. Once this is established, a plan can be created to reinforce the change. This may require the retraining of staff or a meeting with the person/people involved, with emphasis on the importance of what changes must be implemented and the set timescales. It is always important to make it very clear why these changes are important and why they must be carried out in a timely manner.

Collating and analysing outcomes of change data

Even though a change has been completed, it does not necessarily mean it has been successful. It is therefore important that the data relating to the outcome of the change is collated and analysed to establish:

- ▶ how effective the change has been
- ▶ whether it has achieved the desired outcomes
- ▶ whether there are any issues not previously identified that need addressing.

Data can be collated in a number of ways including statistical data available from the system, for example production, sales and finance figures. It can also be in relation to time management analysis, for example whether the savings have been achieved in relation to production time and time taken by employees to carry out their respective roles and responsibilities. Data can also be collected through discussions, interviews and questionnaires.

The analysis of the data collated can provide useful insights into the success (or even failure) of the implemented change.

Monitoring change

During the implementation stage, continuous monitoring should take place to ensure that everything runs smoothly, to budget and within desired timescales. This also helps to identify any potential issues that need to be addressed. During the reinforcing of change, monitoring still continues. Some reasons for continuing to monitor are:

- ▶ to ensure that the change continues to function as intended
- ▶ to ensure that updated/new policies and procedures are being followed in line with the requirements of the change
- ▶ to ensure that the workforce has received appropriate training and guidance and are now implementing the new skills and knowledge into their working practices
- ▶ to identify where revised working practices are not being adhered to and why this may be
- ▶ to ensure that customer satisfaction is being maintained.

Test yourself

- 1 Explain why it is important to set budgets and timescales when planning change within a business.
- 2 What is the purpose of a post-project review?
- 3 A business is implementing change by installing new technological equipment on a production line. Identify two potential skills and developments that the production team may require.
- 4 Explain the purpose of reinforcing change.
- 5 Explain the importance of clarifying the resources required when planning for change.

1.9 The measurable value of digital service to customers and end users

The first phase of any change management project starts with the development of the project's goal and overall measure of success (measurable value). The measurable value is the goal of the project and is used to define the value that the project will bring to the end users and customers. In order to provide real value to an organisation, the project must support the organisation's vision, mission and strategy.

Value to customers

Customer experience has become the forefront of how a business's products/services differ from those of its competitors. Businesses may develop the same types of products or provide the same services at the same price, but it is the customer experience that highlights the differences between the businesses.

Efficient digital support for products and services

The relationship that a business has with its customers can play a vital role in its success or failure. Strong relationships with customers build loyalty and encourage repeat business. Poor customer service has the adverse effect.

Digital technology has made it easier for customers and businesses to interact. Now businesses are able to communicate with their customers more quickly and efficiently, with some of the bigger businesses being available 24/7. Businesses such as Amazon allow their customers to search for products and buy online at times that are convenient to them. Online banking is available to customers to pay bills, check their bank balances and even pay in cheques. While not all businesses are available 24/7, customers can complete online contact forms or send emails, and post social media requests and will expect to receive a response when the business opens the following day.

Broadband companies provide online services that allow customers to check the status of broadband in their area, and receive updates when problems are being worked on by the engineers. This is all thanks to the use of efficient digital technology to support the customers.

Timely response to customer queries or needs

- ▶ **Communicating expected response time** – customers expect services to be available when they need them, whatever the time of day or day of the week. Digital technology such as chatbots and live chat enable businesses to provide immediate responses regardless of when the customer contacts them. Businesses that do not have such facilities can still send automated responses to customers informing them of when they can expect a response to their query. Instant answers may be available from frequently asked questions (FAQs) and quick resolutions to problems are therefore available without any person-to-person interaction.

- ▶ **Communicating any changes in response and why** – businesses can notify their customers of any response changes and the reasons for the changes by posting notices on their websites, so that customers can see them as soon as they access the site. Other forms of digital communication can be used such as social media, text messaging and emails. Prompt notification to customers makes them feel valued.

Financial savings

Digital services allow customers to ‘shop around’ from the comfort of their own home. Price comparison sites are available for all sorts of products and services and customers can input their requirements and let the system do the rest, by comparing their requirements to what is available. Customers are then provided with a list of options.

Comparison sites are widely advertised on television, for example the opera singer for ‘Go Compare’ and of course the delightful meerkats for ‘Compare the Market’. There are many sites that allow customers to find plumbers, electricians, builders and so on in their local area and ask for quotes for work that they want carrying out. All of this can save a customer time and money.

Access and engagement

Multi-platform multimodal format

Multi-platforms provide customers (and potential customers) with choices on how they want to communicate with businesses. Customers can access businesses in a variety of ways including email, websites, social media, live chats, phone calls and so on. The way that the customer contacts the business is referred to as a channel and it is important that businesses organise their channels and connect with them as this plays a major part of the customer journey.

Multimodal is a method of communicating with customers and refers to the customers using multiple channels simultaneously. For example, a customer could be having a live chat and browsing the web at the same time. They could be at an airport using the self-service booking-in system and responding to an email. Therefore, businesses must consider not what individual channel will suit a customer but the combination of channels that can be used to deliver good customer service experiences.

Time saving

Digital customer service fits in with people’s lifestyles. People with smartphones use them to text, post on

social media, shop online and chat with their friends and of course much more. Therefore, they use their smartphones for customer support as well. Customers like the convenience and speed offered by using the variety of digital channels available to them. For example, a person needs to urgently contact their bank but they are on a noisy train and it is not possible (or sensible) to phone them and provide verbally sensitive information. Instead, they use a chat session with their bank to resolve the problem. It is convenient and fast.

Social integration for user and support community

Social integration for customers means that the customers’ communications are all dealt with centrally by the business. When accessing the communication ('contact us') page of a business's website, the customer is given a choice of options on how to contact the business, for example email, phone, social media, online chat or using the support community. The customer selects their choice and the communication with the business begins. Because all of these methods of communicating are dealt with centrally, then all customer communications are given the same level of attention.

Value to end users

Efficient first line, second line and third line digital support to internal staff

Digital support is a form of customer communication used to support end users with help on how to get the most out of the digital technology they are using or to help solve problems with the technology itself. This is usually done through knowledge bases, live chat, email or telephone and aims to solve problems such as installation issues, log-in errors and so on, all of which can have a negative impact on the end user experience.

- ▶ **First line support** – the people providing first line support have a basic/general understanding of the product/service and do not always have the relevant competency to resolve more complex problems. Communication is usually via email or a chat box but if the situation is more complex, then a phone communication takes place.
- ▶ **Second line support** – this is used when the problems are more complex and time-consuming. Second line support staff have more specialist technical knowledge. They focus on problems that require in-depth knowledge about the products/services.

- **Third line support** – these are technically trained, experienced and knowledgeable technicians. Whatever the problem is for the end user, they will probably be able to fix it and, if necessary, conduct a site visit (visit the end user to resolve the problem).

Efficient resolution of end user needs

End users need to be able to use the digital technology to carry out their roles and responsibilities in an efficient and effective manner. Problems with technology can not only prevent the end user from carrying out their work activities, but also delay the work of others where the work of one person (or department) relies on the completion of work by another. As can be seen in the above section, the levels of support available are of paramount importance to businesses and in particular their end users. Therefore, the customer support available to them must be efficient and effective in order to resolve any technical issues which may delay operations.

Effective hardware or software deployments

End users need to carry out their workplace activities with the minimum of disruption, even when new hardware/software installations are taking place. Many organisations will pay other businesses to deploy their new hardware/software (this is known as outsourcing). This enables the in-house technical team to focus on resolving problems for the end users and to ensure that the current system functions efficiently. In addition, the deployment of any new system (hardware, software or both) should appear a seamless operation to the end user and should have been tested alongside any current system before release to the end user.

Test yourself

- 1 Describe how a business can ensure that it has efficient digital support for its products and services.
- 2 Explain the term ‘multimodal format’.
- 3 An end user has a serious digital system failure that has stopped the production of a new product. What line of support would deal with this problem?
- 4 Define the term ‘social integration’ for customers.
- 5 When considering providing support for its products to the customers, what communication channels should a business consider? Justify your response.

1.10 The considerations and value of meeting customer and end user needs within a business context

Considerations to meet customer and end user needs

It is important to consider the user needs (internal and external to the organisation) when implementing digital technology. It is part of the overall project planning. In addition, it is also important to consider how the digital technology will ensure and even enhance the quality of the service/product(s) offered by the organisation.

Customer or end user profile

Cultural awareness/diversity

The reception and use of technology in the workplace can be influenced by several factors, including **socioeconomic status**.

It is important to bear this in mind when implementing digital technology. This is because the availability of technology varies according to an individual's socioeconomic status, which is commonly referred to as the 'digital divide'. Whether someone is working for the organisation or is one of their customers, they can all be categorised as those that have technology (and to what extent) and those who have not. This can result in some people being less familiar with certain technologies and therefore reluctant or unable to use them. New technologies might therefore need to be sensitively implemented or accompanied by training.

Inclusivity

Inclusivity is ensuring the involvement of everyone.

Inclusivity includes:

- access to good quality hardware, software and internet connectivity
- access for people with disabilities
- computer literacy and skills
- education
- geographic location

Key term

Socioeconomic status: this is the social standing or class of an individual or groups of individuals. It can be classified based on a combination of factors such as education, income and occupation.

- ▶ culture
- ▶ age
- ▶ language
- ▶ economic situation.

Accessibility

Accessibility for customers and end users is an important consideration for businesses. Any system and/or process that has to be used by customers and end users must be simple and quick to use, while taking into account those people who may have a disability, for example impaired sight or hearing, or some other physical impairment.

Adhering to guidelines, policies and regulatory requirements

Businesses must consider any regulatory guidelines and requirements relating to customers and end users. These can include areas such as health and safety, minimum wage, employment law and so on. Additional guidelines were added by the UK government due to the pandemic situation in 2020/2021. Guidelines and regulatory requirements are developed into organisational policies for the business to comply with. The identification of these guidelines, policies and regulatory requirements enables businesses to conduct their operations while ensuring that the considerations of their customers and end users are taken into account.

Level of technical knowledge and skills

Technical knowledge can be linked to skills and education level. How much exposure a person has had to technology and how much they have used it will have an impact on their technical knowledge. For example, a person is confident using a smartphone to make and receive calls, use apps and social media, but if something goes wrong, they may not have the technical knowledge to solve the problem. The digital technology must enable end users of all skill levels to access and use the digital technology by assisting them to navigate and use the technology with minimal issues.

There can also be limitations of a person's technical knowledge with respect to the specific product and or service. For example, if a person accesses a website to try and resolve a problem with a specific product e.g. a television not displaying the output from a digital box for TV services, they may not be technically savvy as to how to set it up or the associated technical jargon. If it is difficult to trawl through a website to find an answer to the problem or even how to resolve the problem, because it has been written with a lot of technical jargon, this restricts access for the user. This is why a lot

of businesses include diagrams, graphics and even video clips to demonstrate how the problem can be solved or in this example how the devices should be connected.

Customer or end users

Problem type and pain points

For an organisation

There are several issues that can arise which cause pain to the organisation, its productivity and its employees. Below are examples of potential **pain points**.

- ▶ **Low budgets** – while organisations are under pressure to embrace digital technology, in some instances there is not sufficient funding to implement it. The costs can increase quickly, and organisations often try to cut costs in an attempt to save money.
- ▶ **Communication** – the lack of communication or miscommunication between the IT department and other departments in the organisation can be a barrier to adapting to, and entering, the digital technological era. All departments have the same goal – the success and growth of the business. But invariably these departments have different strategies to grow the business and increase its success. It is therefore important that all departments communicate effectively with each other to share their visions and collaboratively improve the business.
- ▶ **Lack of technical knowledge by end users** – IT professionals often spend precious time explaining basic IT functions to people because they lack the knowledge to do things for themselves. It can be very time-consuming during meetings to explain in detail how potential new and/or upgraded digital technology can improve the functions of the business. A wider knowledge of digital technology within an organisation can save time and resources.
- ▶ **Lack of training** – a lack of knowledge is an issue when implementing digital technology. End users who do not receive appropriate and adequate training will not be able to use the technology effectively, which in turn will have an impact on their ability to carry out the required functions. Good training for the end users will ensure the overall successful implementation of the digital technology, saving time and resources.

Key term

Pain points: issues that occur which people will work around. In some instances, they are not even aware they are happening.

Key term

Data virtualisation: connects all types of data sources regardless of the file types and location. The data is then combined, and users can access the combined data through reports, mobile apps, websites, dashboards and portals.

- **Security** – this is one of the biggest priorities of any IT department. **Data virtualisation** (although costly) has made organisations more vulnerable to security breaches. Data breaches can have an impact on an organisation through data loss as well as damaged customer confidence and trust. Budget cuts can lead to a reduction in the funding of security of systems.

For the customer

For customers, the pain points can be as follows:

- **Usability** – a customer's pain points can include usability issues. Usability requirements are the documented expectations and specifications that are created to ensure that products, services and processes (and even environments) are easy to use. There are five key components for usability:
- Learnability – how easy is it for an end user/customer to perform simple activities when they initially interact with the product/service?
 - Efficiency/effectiveness – how efficient is the product/service? Customers and end users do not like wasting time. The effectiveness means that it supports users in completing actions accurately.
 - Memorability – is the experience a good and memorable one? Is it easy to use the product/service again and remember what actions were taken?
 - Errors – there should be no errors. Errors create frustration in customers and end users (especially when it is not their fault). The products/services should support a wide range of user actions and only show errors in genuine and erroneous situations.
 - Satisfaction – does the product/service give the customers and end users satisfaction? If the above points are addressed, then satisfaction is usually easy to achieve.
- **Functionality** – customers and end users need the services/products of businesses to function in a way that solves their problems or meets their desires.

- **Training on new systems** – businesses need to consider new and innovative ways to train their customers on how to access and use their products/services. It is always important to consider the possible skills level of a wide range of customers (and end users), so that the methods used are clear, understandable (not too much technical jargon), accessible and memorable.

System or service response time

As stated in previous sections, customers do not like time wasting. They get frustrated and they take their custom elsewhere. They are expecting quick, efficient and accurate response times.

System or service availability

There will always be occasions when a system, website and so on has to be updated or maintained and therefore it becomes unavailable for use. These downtimes should be planned out carefully with respect to time schedules to ensure that it has the minimum of impact on the customers (and end users). Banks will usually notify their customers at least a day in advance informing them that online banking will be unavailable between the hours of X and Y for system maintenance and upgrade. They will plan the downtime for when there are only a small numbers of customers who would use the system at that time, for example overnight. If systems/services are unavailable for long periods of time, it is frustrating for the customers who may complain and take their custom elsewhere.

Value of meeting customer and end user needs

Happy and satisfied customers and end users will stay with a business over a long period of time. That should be the goal for any business. Ensuring that customer expectations are not only met, but exceeded, means that they will buy products and services from a business again and again.

Increased financial benefit

Happy customers are customers who will stay with a business. They will also promote the business by talking to friends, family and posting positive comments on social media. Retaining customers who repeat buy from a business means an increase in revenue. Gaining new customers through positive recommendations will also increase revenue.

User experience

As previously mentioned, it is important that customers and end users have a positive experience

when interacting with the business, their systems, products and services. If the customers and end users have a good experience, they will want to remain with the business. If, for example, a person wants to purchase a product online, but the website is difficult to navigate, or the system keeps crashing, then that will result in a negative experience, and they will look elsewhere to purchase.

Reputational

Reputations can be won and lost thanks to the perceptions of the business by customers and end users. If there is any negativity due to poor interaction between the business and end users, then custom will be lost, and negative comments will spread through word of mouth and of course social media.

Protection of brand reputation

It is hard for any brand to recover from a damaged reputation. Businesses cannot ignore this and can face a huge struggle to restore a damaged reputation, and will probably lose a lot of customers as well. It is therefore important that the needs of customers and end users are met as quickly and efficiently as possible. Here are some examples of how this can be achieved:

- ▶ **Mistakes** – these can happen in any business, such as failing to meet a delivery schedule, or a product is received damaged or goes missing during transportation. Mistakes should be admitted immediately by the business, an apology given to the customer and a commitment made to resolve the problem as soon as possible.
- ▶ **Ethics** – customers place their trust in a brand when they purchase the products and/or services. Employees must have a set of ethical principles to comply with every day to show that the business ‘means what it says’. Ethical principles include honesty, integrity, loyalty, respect and concern for others, commitment to excellence and law abiding.
- ▶ **Trust** – businesses have a responsibility to their workforce and customers. It is therefore important that they maintain a positive reputation with respect to moral and legal obligations. Consider businesses that have been the victims of cyber attacks where the attacker has had access to personal and sensitive information relating to the workforce and the customers. It is important that a business makes every effort to mitigate risks against such activities.
- ▶ **Politeness** – all businesses will come across an angry customer. They may vent their anger via the telephone, write a negative review online using

social media or the website, or even in a shop/store. It is important that every employee responds in a polite, professional and calm manner. This approach will help to retain customer loyalty (even from the angry customer) and also prove to other customers/potential customers that the business and its workforce are part of a helpful, caring and rational brand.

Brand awareness

The higher the level of brand awareness for products and services, the greater the potential for businesses to increase their revenue by generating more sales. Customers are faced with numerous choices, especially if purchasing through the internet. It is a well-known fact that they will favour a familiar brand as opposed to selecting an unfamiliar one.

Positive media exposure

This is a powerful marketing tool that places a business in a favourable position by showcasing the credibility, expertise and image that it conveys. By ensuring positive media coverage, it is possible to convert potential customers and end users to regular customers and end users.

Qualitative and quantitative market research

- ▶ **Qualitative** market research usually involves customer motivation and reaction through observation that may be face to face or in a small group of people. Qualitative market research provides a business with descriptive data that enables them to gather information on the experience of the customers and end users. It can be used to test new ideas and/or products/services and discover how customers and end users would react.
- ▶ **Quantitative** market research is the process of collecting large amounts of data using questionnaires, surveys and polls. While quantitative market research provides statistical data, for example how many people have purchased a specific product or service, it does not give an indication of their feelings and views about it.

Product development through product use analysis

By analysing the results of market research and sales statistics of existing products, businesses can identify the current level of market activity and interest in products that are similar to the new product being developed.

More sophisticated markets for personal and targeted advertisements

Targeted advertising ensures that businesses reach the right audience at the right time, in the right place. With the increasing use of the internet, users regularly share personal data online as well as web cookies tracking every click a person makes when online. This gives businesses an insight into customers and end users, and enables them to provide advertisements for products and services tailored to their individual needs.

Positive third-party reviews

These are reviews that are collected and presented on a third-party website, for example directory listing or social media profile. Positive reviews boost sales and attract customers; of course negative reviews would have the adverse effect.

- ▶ **Unboxing** – this is where a person will record a video where they open a product from a box, display it, review it, show its contents and even demonstrate how it works. There are a lot of unboxing third-party reviews on YouTube and many other social media channels.
- ▶ **Meta critic** – these are websites that collect the reviews of video games, films, TV shows, music and so on. Each product is given a numerical score from each review obtained and the total is summed to provide an overall score. Content from reviews (including a hyperlink to the source of the review) is also provided. This provides customers and end users with an insight into the popularity of the product/services.
- ▶ **User reviews** – these are reviews on products/services created by the customers and end users. Consider Amazon and the user reviews available for different products. These can have a major influence on the purchases made by customers and end users. They are more likely to believe a user review than the sales pitch provided by the business selling the product/service.

Test yourself

- 1 Identify three considerations that a business needs to take into account to meet customer and end user needs.
- 2 Describe the term ‘pain points’.
- 3 Explain why meeting customer and end user needs increases the financial benefit to a business.
- 4 Explain the term ‘unboxing’.
- 5 What is the difference between qualitative and quantitative market research?

1.11 Risks and implications within a business environment

All businesses have **risks**, many of which could have severe implications if they actually take place. It is therefore important that businesses constantly review these risks and implement strategies to mitigate against them occurring.

Privacy and security

Potential loss of control and compromise to confidentiality, integrity and availability of data

Businesses store a lot of data and information. These can be about their customers, suppliers, workforce and operations. It is therefore important that this data is stored safely and securely. The benefits to a business of using e-business strategies and internet-based technologies are vast, but so are the risks which can include:

- ▶ theft or manipulation of sensitive or private information, for example financial records
- ▶ computer fraud where cyber criminals send the user an email/message to trick them into providing valuable data and information, for example log-in details to a system that can be used to steal further data or money. The emails are designed to look as if they are from an official source, for example a bank
- ▶ computer viruses that can destroy data, damage hardware, render systems inoperable and disrupt business processes.

Some of the more damaging implications of data loss are:

- ▶ **Financial loss** – as well as a business potentially having its own money stolen, there are further costs that may have to be paid. This includes compensating customers and suppliers who have been affected, setting up incident responses, investigating the breach, investing in new/updated security measures, legal fees and regulatory penalties, for example non-compliance with the General Data Protection Regulation (GDPR).

Key term

Risk: in the context of business, risk refers to factors that could lead to the failure of the business or a drop in its profits.

- ▶ **Loss of reputation** – customers need to be able to trust the businesses that they deal with. Cyber attacks can damage a business's reputation and destroy their customers' trust. This can lead to loss of customers and sales, and a reduction in revenue. Loss of reputation can also damage the relationships a business has with its suppliers.
- ▶ **Operational downtime** – once a business has been victim of a cyber attack, the incident has to be investigated to see how it occurred and why it occurred. This involves taking down the system to ensure that there are no further attacks while it is being investigated and resolved. Operational downtime also means that the business cannot function as normal which, again, results in a loss of customers, sales, revenue and customer trust.
- ▶ **Legal action** – the data protection and privacy laws require businesses to manage the security of all personal data they store for staff and customers. If this data is accidentally or deliberately compromised and it is found that the business did not implement appropriate security measures, the business can be fined and face regulatory sanctions.

Loss of *sensitive* data can result in:

- ▶ loss of reputation and loss of customer loyalty
- ▶ financial loss through legal action being taken by customers
- ▶ disruption to operations
- ▶ business failure.

Non-compliance

Non-compliance is when a business or a person fails to or refuses to act in accordance with set policies, procedures and legislation. Core element 8 explains the regulations and legislation that businesses must adhere to, and the policies and procedures that must be understood by everyone in the business, and which are implemented and complied with.

Legislation and standards are covered in Core element 8.

Security measures are covered in Core element 10.

Audience exclusion

Audience exclusion is used mainly within marketing campaigns when a business only wants to target a particular customer group who they believe would be interested in their product and/or services. The benefits of audience exclusions are:

- ▶ reaching a more relevant audience
- ▶ avoiding 'ad fatigue' and overloading audiences for whom the product/service may not be relevant.

Businesses need to be cautious when implementing audience exclusion as they can be considered as biased towards a certain group or groups of people. This can damage the reputation of the business and their brand.

Insufficient business resilience

Business resilience is when a business anticipates, prepares for, responds to and adapts to staged changes and sudden disruptions. Ensuring that the business is resilient means that the business can continue its business operations, safeguarding people, assets and their brand. These businesses are therefore best placed to survive economic slowdown (fewer people spending) and continue to operate regardless of any uncertainty.

- ▶ **Inability to adapt to disruptions** – when disruptions occur, for example a pandemic, businesses need to react immediately to prepare and adapt for the challenges they face. While doing this, businesses must remain true to their business goals, and be supportive of customers and staff, while making frequent and rapid adaptations based on new information.
- ▶ **Inability to adapt to change** – businesses need to be flexible and must be able to adapt efficiently and effectively to change. Businesses that have are innovative and adapt quickly to changing circumstances also have the opportunity to take larger market shares in the process. Those that do not adapt to change will lose their share of the market and may even fail altogether. Businesses need to strengthen and constantly review their risks mitigation strategies to ensure that they are resilient to future changes.

Technical

Technology does not stand still. There are new technological devices and initiatives appearing all the time. Businesses need to constantly review the technology they have in place and consider how new technology and associated initiatives can ensure that they retain customers and have a viable operation.

System not fit for purpose

The technological infrastructure of a business uses about 50% of the allocated budget for technological spending. There are many businesses that therefore still have inefficient systems. It also hides the true cost and service levels for products and services and leaves them vulnerable to disruptions. It is important that the digital system is given the same level of importance as the products and/or services a business sells. Systems that are fit for purpose enable a business to view

priorities and collaborate more effectively to implement the business's overall strategy. Businesses have a more accurate understanding of the total costs of products and services across their entire business to include the workforce, products and/or services. In addition, businesses can prioritise their disaster mitigation and recovery plans; this reduces costs in relation to finance, reputation and regulation.

System does not meet user requirements

Businesses that do not have up-to-date and fit for purpose digital systems in place can lose money due to employees taking longer to complete tasks and in some instances with less accuracy. Businesses with many departments but no collaborative networking system create additional work for the employees through phoning or walking between departments to access information. Customers (as previously discussed), expect prompt responses from the businesses they deal with. If they cannot use technology to access the business, whether it is to purchase a product or service, or to have their problems resolved, they will not remain loyal. In addition, customers will complain about the business, and this can damage the reputation of the business and its brand.

Potential impact of risks

Wherever there is a risk, there is an impact. The severity of the impact depends on the severity of the risk. But all risks should be mitigated if possible.

► **Lawsuits/fines** – any breach in regulation and legislation can result in businesses being taken to court. (See the section on the privacy and security of personal and business information.) Businesses can face very high financial penalties if they fail to ensure that their systems are secure, and that data and information are protected. These heavy financial penalties can result in a business going out of business and/or severely damage its reputation and brand.

Refer to Core element 8, Legislation.

► **Dismissal/loss of job** – all businesses should have policies and procedures in place that not only comply with regulation and legislation but also explain clearly to the workforce (at all levels) their roles, responsibilities, permitted and non-permitted activities while at work, for example not using the IT system for personal use such as online shopping or answering personal email/social media posts. This is in place to help protect the business's digital system from being infected by a virus or malware,

and from being at risk from hackers. If during the investigation of a cyber attack it comes to light that an employee has 'broken the rules' and caused the problem (that may be catastrophic to the business), then they might be dismissed.

► **Reputational/brand damage** – through this section it has been highlighted how risks that occur within a business can have severe implications and this includes damage to the business's reputation and brand image.

► **Withdrawal of licence/rights to practise** – a business licence is a mandatory approval/permit issued by a government agency. It provides the business with authorisation to operate within a specific sector. Not all businesses require a licence; it depends on the nature of the business, the types of products/services it sells and any local government regulation that is in place. These licences hold businesses answerable for their actions and behaviours and are also used to protect the health and safety of the public.

A business's licence can be taken away if the company no longer meet the licensing criteria. This can happen if the business is convicted of committing a criminal offence. A licence can also be suspended if it is believed that the business is a risk to public safety, and it is in the public interest therefore to suspend the licence. Most licences are industry specific, for example

- healthcare
- insurance
- construction
- engineering
- retail sales
- charities
- security
- utility companies.

► **Loss of business/reduction in sales** – any risk that actually occurs and impacts on customers invariably results in a loss of sales. Depending on the severity of the issue, the loss of sales may be permanent as customers will lose confidence in the business and shop elsewhere. A loss of sales is a loss of business. A loss of business results in a loss of revenue. As you can see from the sections on the potential risks and subsequent implications, they can all result in a loss of business and a reduction in sales. This reduction in revenue can mean that some of the workforce may have to be made redundant or the business may even fail altogether.

Test yourself

- 1 Explain why insufficient business resilience is a risk to business survival.
- 2 A business has had a cyber attack and had customer data stolen. Discuss the implications to the business.
- 3 Describe one risk to a business of having a system that is not fit for purpose.
- 4 Explain the reason why a business licence can be withdrawn.
- 5 Explain why business risks can impact on a business's reputation and brand.

1.12 The purpose and applications of codes of conduct within a business

Purpose and application

Codes of conduct can be developed by an organisation or by industry bodies. Businesses that develop a code of conduct document a collection of rules, principles and values, setting out the expectations of employees' behaviour and relationships that the organisation considers to be important to its success.

Codes of conduct can set a business apart from other similar businesses and should reflect the culture that is present (or required to be present) within the organisation. Codes of conduct provide employees, customers and other relevant stakeholders with guidelines as to what the organisation believes is most valued, significant and desirable in relationships, interactions and the view of the world as a whole.

Some organisations refer to codes of conduct as a Code of Business Ethics, Code of Ethical Business Conduct or Code of Ethics and Standards. A code of conduct provides a framework for ethical decision making within an organisation and is a communication tool informing internal and external stakeholders about its values, employees and management.

Ensures individuals and organisations operate within policies, procedures and legislation

The codes of conduct of each of the professional bodies all include the commitments of the members to work in the public interest and to accept their professional duties.

The codes of conduct of each of the professional bodies also act as a benchmark when assessing the misconduct of their members. Each code of conduct includes statements of responsibility related to the relevant industry.

- ▶ **Industry standards** are criteria within a specific area of business that are the minimally accepted requirements followed by members of that industry sector. They provide a clear definition of what is and what is not acceptable practice. An industry standard is a mechanism used to simply and concisely communicate goals that have been developed both internally and externally to a business within a specific industry. It supports the improvement of customer and consumer experience external to the industry, for example creating performance specifications for the manufacturing of components, or creating minimum performance standards for those providing services.
- ▶ **Professional practice** refers to the conduct as well as the work of someone from a specific profession. Professions are defined as occupations that require extended periods of training.

Describes accepted practice for individuals and organisations

- ▶ **Confidentiality** – in many professions, for example healthcare, confidentiality is required to protect people and their personal information, to preserve their privacy, dignity and rights. Therefore, in these situations, organisations develop codes of conduct for confidentiality to ensure that data and information are kept safe and provide employees with guidelines about what they can and cannot do.
- ▶ **Ethical principles** – these are principles that are designed to guide employees and provide assurance to customers and colleagues about what to expect. Ethical principles include:
 - maintaining high standards of competence in the work carried out
 - maintaining integrity by being honest, fair minded and knowledgeable about their personal competences and limitations
 - upholding standards of ethical conduct that reflect the business and their profession/job role in a positive way
 - respect for people's rights and dignity.
- ▶ **Use of equipment and facilities** – this section of a code of conduct gives clear direction to all employees about what they can and cannot do when it comes to using equipment and facilities.

This can include confirming that employees cannot install their own software on the system, use the business equipment for personal use, for example for online shopping, going on social media or answering personal emails.

- ▶ **Standard working practice** – this section provides clear guidelines to all employees on the processes and procedures that they must follow when carrying out their work activities.
- ▶ **Access permissions to data and systems** – the code of conduct provides all employees with guidelines on the process of using usernames, passwords and so on to access systems and data. It will inform them about the requirement to keep passwords safe and not to share them with anyone else. It will also stipulate the job roles that can have access to certain systems and data.
- ▶ **Supports individual company values** – codes of conduct should support company values. These are the beliefs and principles that a company works toward. They impact on the employee experience as well as the relationship developed with customers, partners and shareholders.

A well-written code of conduct clarifies an organisation's values and principles, linking them with standards of professional conduct when it comes to the behaviour of the employees. As a result, codes of conduct set the benchmarks for companies to live up to.

Types of codes of conduct within a business

Organisational codes of conduct

As previously stated, these are codes of conduct that are developed by individual organisations that support the organisational values. Businesses such as Twitter, Google and COBC (Code of Business Conduct) all have their own codes of conduct and are available for members of the public to read.

Professional codes of conduct

These are industry standard codes of conduct that specify the minimum acceptable standards for people working in the industry. There are from organisations such as BCS (British Computing Society) who have defined codes of conduct for their members.

Governmental

These are codes of practice that are published by governments and are intended to help people understand how to comply with the requirements of

regulations and legislation. Examples of governmental codes of conduct include:

- ▶ **Technology Code of Practice** – a set of criteria to help government design, build and buy technology.
- ▶ **Data Ethics Framework** – a set of principles that have been developed by the government to provide guidance on the appropriate use of data in the public sector.

Research

- 1 Research the organisational codes of conduct for Twitter, Google and COBC and compare and contrast them. In your comparison, consider the similarities and differences between them.
- 2 Research the professional code of conduct for BCS and identify the key aspects of conduct expected from their members.
- 3 Research the Data Ethics Framework and identify the key principles that provide guidance on the appropriate use of data in the public sector.

Create a report to present the results of your research.

1.13 Types of hackers and the implications of hacking and non-compliance with a code of conduct

Types of hackers

White hat/ethical hacker

This is where the hacker is given permission to hack into digital systems, such as networks, to identify any holes or vulnerabilities. As this type of hacking is done with the permission of the business, it does not break any of the legislation that relates to hacking. A white hat/ethical hacker has permission to engage in social engineering within agreed parameters with the business.

Grey hat

Grey hat hacking is where the hacker hacks into computer systems for fun or to troll but does not have malicious intent towards the business and their digital systems. If a grey hat hacker finds a weakness, then they may offer to fix the vulnerability – but for a fee. Grey hat hackers can also manipulate the rankings of websites when a search is carried out on a search engine.

Black hat

Black hat hacking is where the hacker hacks into a computer system with malicious intent. This intent can include stealing, exploiting the data stolen or seen, and selling on the data. Black hat hackers can compromise and even shut down a business's security systems and networks. They can obtain unauthorised access to passwords, financial information and personal data. Black hat hackers carry out illegal hacking activities and can be prosecuted under UK legislation.

Black hat hackers include:

- ▶ **Hacktivist** – often work in groups to carry out united cyber attacks in support of political causes and personal beliefs, for example animal rights campaigners. They target entire industries or sometimes specific organisations who they believe do not align with their views, opinions or practices. They may target organisations based on the clients and partners they do business with.
- ▶ **Organised crime syndicate** – these are groups of hackers, programmers and other tech bandits who combine their skills and resources to commit major crimes that might not otherwise be possible. They are motivated by financial gain.
- ▶ **Nation state** – some people carrying out hacking are known as nation state actors. They carry out cyber attacks on behalf of one government (nation) on another government (nation) in order to obtain information, secrets and even cause chaos with a country's infrastructure. The motivation is purely political.

Implications of hacking and non-compliance

The implications of hacking and non-compliance can be internal and external.

Internal implications

Internal implications include:

- ▶ **Disciplinary action/loss of employment** – disciplinary action is a reprimand or corrective action in response to an employee's misconduct, violation of the codes of conduct, policies and procedures or poor performance. Depending on the severity of the case, the disciplinary action can be any of the following:
 - verbal or written warning
 - poor performance review/evaluation
 - performance improvement plan
 - reduction in pay or role status
 - dismissal (loss of employment).

▶ **Restriction of potential employability** – if an employee leaves one company and applies for a position with another company, they usually have to provide references. One of these references would be from their previous employer. If an employee was dismissed for gross misconduct, then the reference from the previous employer would not be favourable. This could restrict any potential employment opportunities.

▶ **Restricted privileges** – employers can restrict privileges that they allow other employees as a form of disciplinary action. What these restricted privileges are will depend on what privileges the business allows the employees and the seriousness of the misconduct of the employee. It could be restricted access to data and systems, or they may not be able to remain in the office on their own.

External implications

External implications include:

- ▶ **Loss of status with professional bodies** – some job roles require employees to be registered with a professional body, for example teachers, healthcare staff, accountants and so on. If the employee loses this professional registration, they lose their status or are suspended by the professional body, and they are not permitted to practice.
- ▶ **Prosecution** – if an employee is accused of hacking into their employer's computer system or some other form of non-compliance, they can be prosecuted under the Computer Misuse Act. There is other legislation, for example General Data Protection Regulation/Data Protection Act 2018 that can also be used within a prosecution case. The penalties can be high and can include:
 - fines
 - imprisonment.
- ▶ **Loss of reputation** – the impact on the reputation of the business if a member is discovered to be hacking into the system or not complying with the codes of conduct can be severe. The severity depends on the impact that the situation has had on the business's customers, suppliers and other stakeholders. The reputation to the employee will also suffer based on the penalties they are given.

Legislation and standards are covered in Core element 8.

Security measures are covered in Core element 10.

Test yourself

- 1 What are the implications to a person of losing their status with a professional body?
- 2 Describe the term 'nation state'.
- 3 Why would a business pay for the services of a white hat hacker?
- 4 Identify two internal implications to an employee of hacking or non-compliance within the business they work for.
- 5 Explain how an employee caught hacking or non-complying can be restricted from potential employability.

Project practice

A retail company selling pet food and other pet supplies is planning to implement an online e-commerce site and market its products using social media. They have a large warehouse and office space on one site. You have been asked to help them plan for the change and to provide them with advice and guidance on how they should proceed. Prepare a report for the business owner providing advice and guidance on the following.

- ▶ The measurable value of digitalisation to the business with respect to:
 - sales and marketing
 - operations
 - finance
 - KPIs.
- ▶ The influence and impact of digitalisation with respect to:
 - brand differentiation
 - digital innovations
 - wider access to customers
 - digital personalisation
 - platform interoperability
 - open standards.

- ▶ The role of technical change management with respect to:
 - preparation and planning
 - operations.
- ▶ The components of technical change management with respect to:
 - requests for change
 - setting SMARTER objectives
 - the risks and impacts involved
 - rollback planning
 - traceability
 - documentation.
- ▶ Factors that will drive the change with respect to:
 - technology
 - legal/regulatory requirements
 - access and engagement
 - social integration
 - value to end users.
- ▶ Considerations to meet customer and end user needs.
- ▶ The risks and implications within the business environment.
- ▶ The considerations for the implementation for codes of conduct.

Assessment practice

- 1 Compare and contrast public, private and voluntary/charity organisations.
- 2 Describe the term 'business to many (B2M)'.
- 3 Explain how political factors can influence the business environment.
- 4 Describe how business digitalisation can enhance operational communication channels.
- 5 Explain how virtualisation/cloud solutions enable scalability within a business context.
- 6 Why is it important to get 'buy in' from all areas of the business when preparing and planning for digital change?
- 7 Describe one reason why war can drive change in a business.
- 8 Why is it important to clarify the resources required when planning for change?
- 9 Discuss the measurable value of digital services to end users.
- 10 Describe the reputational value to a business of meeting customer needs.

Core element 2: Culture



Digital transformation is achieved through technology. But you must also remember that the human aspect is as important as the technology. Digital professionals must understand the ethical and moral issues within the digital sector for a variety of business contexts. It is important that you understand how technological developments impact on individuals, organisations and society on a global scale.

Learning outcomes

In this core element you will learn about:

- 2.1** How the increasing reliance on digital technology can cause ethical and moral impacts on business and society

2.2

- The impact of unsafe or inappropriate use of digital technology and mitigation techniques to reduce impact

2.1 The increasing reliance on digital technology and its ethical and moral impacts

Impacts on business

Impact on company culture

There are many challenges faced by organisations and individuals as the reliance on technology increases. While it is important that all organisations that intend to implement digital transformation embrace **ethics**, it is more difficult on an individual level. This is because it is individuals within an organisation that make decisions, not the organisation itself.

What is seen to be ethical can vary across:

- individuals
- groups
- religions
- cultures.

With a digital society that has expanded globally and is extremely fast moving, there is scope for a wide range of interpretation. Therefore, it is important that digital professionals at all levels determine:

- what is ethically correct (the right thing to do)
- the ethical training needs that may be required
- the ethical awareness within their organisation.

It is also important to consider the current legislation within the UK and other countries, and the impact and challenges this presents to an organisation when it increases its reliance on technology.

Changes to face-to-face communication

Digital technology has shaped the way societies and people behave, grow, evolve and develop, both within their own lives and in their relationships with others. In recent decades there has been an explosion in technology; this has caused crucial changes in how humans see the world and interact with others.

Key terms

Ethics: rules, actions and behaviours defining permissible actions/behaviours to address **moral** obligations.

Morals: the principles of what people believe is right or wrong.

Consider the internet and mobile phones, and how they have altered the way people interact with each other. One of the major impacts of technology is the optimisation of communication systems through telecommunications and networking.

Digital technology has changed human behaviours and interactions in positive and negative ways. Humans communicate with each other in the majority of cases using smart apps through the internet or Wi-Fi. The use of Voice over Internet Protocol (VoIP) and social media means that people can maintain contact with friends and family more easily. Organisations also use the advances in digital technology to interview potential employees or clients on a global scale. Learning behaviours have also changed. People can 'meet' people from other countries and learn about their culture.

Positive effects include:

- bridging the global gap
- access to a wide range of resources via the internet
- faster and easier communication.

Negative effects include:

- virtual distancing where people are physically together but detached from each other because they are immersed in the technology within their environment
- reduced physical interactions through face-to-face meetings and conversations.



▲ Figure 2.1 People using their phones

Remote working

Mobile and remote working is now more accessible to a wider range of people. Organisations with a larger remote workforce require less office space, and fewer materials and utilities, which in turn reduces costs. The

drawback of remote and mobile working is the work/life balance and employees' mental health. Remote workers can find it difficult to 'switch-off' at the end of the working day as everything is still accessible to them and they can be contacted. In addition, remote workers can be lonely, and therefore good communication through enhanced technology allows them to communicate effectively with their colleagues. In this way, their quality of work and productivity will not suffer.

Video conferencing

This is a low-cost solution that can be used if employees are based in different locations and cannot commit to attending face-to-face meetings because of work commitments and the travel involved. It improves communication between staff through sharing ideas and having discussions.

Increase in expected productivity and outputs

Although businesses benefit from digital technologies, employees benefit even more. Digital solutions and/or tools can help employees with their work activities, enabling them to obtain not only better but faster results. Decision-making and internal processes are more streamlined, and the employees' efficiency can be significantly increased. Digital solutions help to remove old and obsolete processes and/or technologies that do not support the growth of the business.

Mobile technologies clearly boost the efficiency and productivity because staff can complete work activities from any location. With the development of digital technologies, it is now possible to achieve full office functionality outside the physical working environment. Staff can respond to emails, read/edit important documents and so on without waiting until they get to the office.

Increase in reach and scale

Reach refers to the total number of people who have seen a business's advertisements or content. For example, if a total of 250 people have seen a business's advertisement, then the advertisement has reached 250 people. Reach can be categorised in the following ways:

- **Organic** – this is the number of people who have seen the business's content for free (organically), for example in a social media news feed.

- **Paid** – this is the number of people who saw a business's content through a paid advertisement. It can be affected by factors such as budgets and the audience being targeted.

- **Viral** – this is the number of people who saw a business's content because their friends interacted with it and shared it.

The scale of a business should not be confused with growth. The **growth** of a business is when the revenue is increased equally as fast with the cost of the additional resources purchased. For example, a business increases their revenue by £25,000 and hires a sales person for £25,000. The gains and losses are evened out. The **scale** of a business is where the increase in revenue is at a faster rate than the expenditure.

The increase in the availability of digital technologies has required businesses to change how they promote the business. Social media in particular is extremely popular and businesses have identified the need to use these platforms to:

- promote the business
- reach potential customers on a global scale
- maximise the potential for increasing revenue.

Increase of staff monitoring

It is legal for a business to monitor the use of its electronic and digital devices. This includes the use of phones and computers. But businesses must inform their employees if they are being monitored. The monitoring of employees can give a business an ethical dilemma: this is because of the personal information that may be seen or heard.

Employees can feel that their privacy is being invaded if their communications and work activities are being monitored without their knowledge. Confronting an employee with information obtained without their knowledge can destroy the trust between them and the business. This can reduce the morale of the workforce, which in turn reduces the overall productivity.

Employees with a low morale do not work as hard as those employees with high morale.

It is always important for an organisation to notify the workforce that they are going to be monitoring their use of the business's digital technologies.

Adaptive working practices

Mobile technologies provide businesses with benefits that can help to increase business growth. More and more people who work for organisations have flexible

working rights. Therefore, advances in mobile technology have contributed to the increase in employees working from home and other locations and not always having to go 'into the workplace'. The use of digital technologies can help businesses to develop a culture of happier employees. Their work/life balance is greatly improved.

A happy workforce is known to lead to:

- increased productivity
- reduced costs
- improved staff retention.

Autonomous operation

This is where a business optimises the operations of the workflow without human assistance. There are two main types of autonomous operations where business processes are automated:

- 1 **Industrial automation** – where physical activities that would normally be carried out by a human are carried out by robots.
- 2 **Software automation** – where computer-based tasks are carried out automatically, instead of manually by a human. **Intelligent software agents** also known as '**bots**' are designed so that they can identify and map business processes using **machine learning (ML)** algorithms to improve the flow of a process. The intended outcome is that the intelligent agent will determine the roles of people, technology and data for a specific business process and then identify how to optimise it.

As with all technology there are positive and negative impacts of autonomous operations. These also depend on the sector in which they have been implemented.

Key terms

Intelligent software agents: autonomous programs that can be aware of and interpret data that is sensed from the environment, reflect on events in the environment and take appropriate actions to achieve identified goals without permanent input from a user.

Bot: short for robot, this is an autonomous program that is on a network or the internet that has the ability to interact with systems or users.

Machine learning (ML): the process of getting computers to learn, think and act like humans. As with humans, computers that are implemented for machine learning will improve their learning over time due to the constant feeding of data and information from real-world situations.

Positives of autonomous operation

- **Cost-effective** – autonomous operations can function continuously as long as they are maintained correctly. There is no halting of a process through employee breaks, holidays or sickness and so on. Any initial cost outlay is soon recouped through lower production costs.
- **Enhanced quality assurance** – humans can get bored and lose concentration when they perform repetitive tasks. This can lead to errors that can be costly and even dangerous. These risks are eliminated by using autonomous operations. There is an increase in the production of products to a much higher standard.
- **Increased productivity** – there is an increase in productivity because (unless there is a system failure) the autonomous operation can be carried out continuously. This enables employees to learn new skills or adapt the skills they already have to other areas within the business.
- **Reduced risks to employees in hazardous conditions** – there are some activities in certain sectors that require employees to work with dangerous chemicals or in environments of extreme temperature. Where these tasks can be carried out just as effectively through autonomous operations, this provides a safer working environment for staff.

Negatives of autonomous operation

- **Dehumanisation of service:**
 - **Loss of jobs** – one of the biggest issues of autonomous operations is the potential impact on the workforce. If tasks can be carried out at a faster and more consistent rate by machines, then there is a concern that humans will not be required. While it is a concern, it is not necessarily a reality. Amazon has numerous autonomous operations implemented to function effectively and efficiently and yet they have increased their workforce rapidly and to significant levels.
 - **Loss of human empathy in decision making** – although the purpose of autonomous operations is to 'get machines to think like humans through machine learning', these machines do not have any emotions. Their actions are cold and calculated based on machine learning algorithms. If a decision is required, a machine will make the decision based on logic, with no emotional consideration. Humans will make decisions based on logic, but they will also look at the 'bigger picture' and consider things such as the impact on people and the environment and so on.

- ▶ **Hiring skilled staff** – businesses have found it difficult to hire necessary skilled staff. Even robots and other such autonomous operations require a certain level of skills to program, operate and maintain. The positive is that the current workforce could undergo specialised training to upskill and take over these new roles.
- ▶ **Initial investment expenditure** – this is always a challenge for any business which wants to implement autonomous operations. However, the returns on the investment can be vast and can even occur over a short period of time. A business's cash flow must be analysed carefully as it must remain sustainable, along with the stability of the business.



▲ Figure 2.2 A robotic arm used for manufacturing.

Shift in skills requirements and skills redeployment

As mentioned, when autonomous operations have been implemented, employees with a different skill set are needed. This can mean that the workforce will require training to enable them to take on new roles and responsibilities, including programming, operating and maintaining the equipment. In addition, employees can be deployed to different locations within the business. There are many people who do not like change and may even leave their job and work for another business.

Impacts on society

Loss of privacy

The value of data is increasing in the digital era, along with a loss of privacy. In exchange for our personal data, we can make our lives easier by permitting smart technology to carry out our wishes and take care of our needs. However, when giving up our personal

information, we must be able to trust the organisations that handle the data. We need to be confident that they will treat our data ethically, making sure it is safe from cyber criminals.

Digital footprint

This is the impression that someone creates when on the internet through their online activity. This can include browsing, interactions with others and the publication of content. It is a trail of a person's data when using the internet, whether it is intentional or unintentional. When a person visits a website, the website places a 'cookie' in their web browser, and this is part of a person's digital footprint. Our digital footprint is formed by posts on social media, email, records of websites visited, and records of online purchases.

There are two types of digital footprints: active and passive.

An **active** footprint is the intentional trail of data that a person leaves behind, for example:

- ▶ sending an email
- ▶ publishing a blog
- ▶ posting on social media
- ▶ completing online forms for subscription purposes or purchases.

A **passive** footprint is an unintentional trail that a person leaves behind, for example:

- ▶ records of browsing products and activities.
- ▶ Advertisers can use these to compile and analyse profiles so that they can send targeted advertisements
- ▶ using websites and apps that use geolocation to identify a user's location.

Surveillance

Cameras are everywhere in towns and cities. They are in shopping precincts, on the street, at tube and train stations, bus stations, airports and in buildings and so on. They are there to monitor the safety of the public. But not everyone agrees with this collection of data; some people believe it is against their civil liberties.

Employers use digital technology to monitor their workforce. This includes where and how employees use the digital technology that belongs to their employer, whether they are using the internet for personal reasons at work, and whether they are on social media platforms. Employers must inform employees if they are using technology to monitor their activities during the working day/night.

The ways in which society is monitored are endless, thanks to digital technology. Mobile phone companies can pinpoint a person's location based on when and where they have used their smartphone. Tracking apps can be installed on a smartphone that will allow someone to access social media posts, telephone calls and even turn on the person's camera to view the surrounding area.

There are many positive reasons for using digital technology for surveillance, but there are also a number of negative reasons. The availability of surveillance systems and monitoring software has an impact on a person's privacy.

Changing behaviours

These are the changes in people's beliefs, attitudes and behaviours as part of a social group, and as individuals, due to the increasing reliance on digital technology. Making positive changes is a challenge. Many people are reluctant to change because of a lack of knowledge and, in some cases, a fear that their jobs may be at risk.

Digital technology has transformed the way that people interact with each other and see the world. For example, the Internet, smart devices and recent advancements in networking have changed the way that we communicate with each other, especially through social media.

There are many positive sides to this transformation. The use of Voice over Internet Protocol (VoIP) and social media means that people can maintain contact with friends and family more easily. Organisations also use the advances in digital technology to interview potential employees or clients on a global scale.

Learning behaviours have also changed. People can 'meet' people from other countries and learn about their culture. Learning a language can now be accessed online instead of attending a classroom.

However, whilst digital technology has assisted in bridging the global gap, it has also created issues. People, for example, might spend lots of time communicating with others who are in a different location, and yet not communicate effectively with people within their own environment.

Social skills

As a society we now live in a technological world. We are always communicating but conversation has been sacrificed for the sake of connection. Instead of facing each other, we turn away and use our smartphones. Society's hunger and passion for technology has

resulted in less face-to-face conversation – and people are forgetting how important this is for our social skills. Face-to-face conversation is the most 'human' thing that we do. It teaches us to listen, to learn and to empathise with others.

Less face-to-face contact and real interaction has made society less tolerant and understanding of differences. Consider social media, where it has been proved that there has been an increase in divisions, with people living in social media bubbles. This means that we surround ourselves with like-minded people and ignore others.

The human race is a social species that benefits from human interaction by co-operating with each other and sharing discoveries and information. It is important that these social skills are not lost due to digital technology and that we consider ways to incorporate them into our everyday lives.

Scalable remote engagement, wider peer and professional networks

Before the increased use of digital technology, businesses would function with their workforce being on their premises or via the use of a telephone. Few people would work remotely from home as they would not be able to access the necessary resources such as files, software applications and so on. Thanks to the increased use of digital technology, people no longer need to travel to the workplace every day to access the resources they need in order to carry out their tasks. Meetings can be conducted online, along with project collaborations, and even customer interaction. The workforce can be increased or decreased, and the transition can be carried out effectively with little impact on the day-to-day operations of the business.

Digital technology provides the opportunity for people to extend their peer and professional networks. Before the increased use in digital technology, people would have to attend seminars, conferences and meetings in order to meet like-minded people or people that they needed to interact with in order to carry out their own specific roles and responsibilities. Now people can interact with a much wider range of people regardless of where they are in the world. Digital technology has provided the opportunity to meet with people online who may be based not only in other organisations, towns and cities, but also in other countries.

Key terms

Unique identifier: a series of letters and numbers that are unique to one person.

Shadow data: data that is automatically generated and recorded as we use the internet.

Creation and curation of a digital identity

A digital identity is information about a person or organisation that exists online. It is possible to detect people (and in some instances the devices they use) through **unique identifiers** and patterns. Website owners and marketeers use this information to identify and track users so that they can receive targeted advertisements and so on.

A digital identity is created from personal information that is on the web, as well as something called '**shadow data**' that is created by an individual when online. Examples of data that can be used to create a digital identity are:

- ▶ username and password
- ▶ date of birth
- ▶ online search activities including purchasing transactions.

User profiles often include parts of a person's actual identity. Therefore, there are always privacy risks associated with digital identities.

Curated self

When using the internet, a person projects an image that may not be their complete true image. This is known as a 'curated self'. They are used a lot by people who use social media. A curated self is the personality of an individual on the internet that is different to (totally or in part) their true self. This can cause problems for social media networks who try to understand who their users are. People will project the image of themselves that they prefer to be seen and do not necessarily have naturally. Originally, this started with people selecting the photo in which they looked their best; this then extended to activities, such as where people would like Facebook pages/Twitter posts so that they would appear in their profiles so that followers/friends could see them. Articles that are shared and 'check-ins' and/or videos are all ways that people are filtered according to their tastes (or alleged tastes). Social networks are a permanent display to the world of a person's curated self.



▲ **Figure 2.3** A person's posts help to create their 'curated self', which may or may not be true to who they are in real life

Communication access

Digital technology affects the way people communicate, learn and think. It has helped society and determined how people interact with each other on a regular basis. Digital technology has an important role in today's society but, like all things, there are positive and negative impacts on the world and people's daily lives.

Resistance to technological change

Communication is conducted through the use of technology within a working environment and within our personal lives. This can include video conferencing, email, online banking, purchasing products and services, as well as talking to friends and family using social media. People who resist technological change and do not adapt to these additional ways of communicating can reduce their potential for interacting with others. They can also isolate themselves from other people, as well as limit their access to products and services.

Potential isolation

Digital isolation happens when people cannot access the internet or digital media and devices in the same way as other people.

Research has proved that social isolation can damage people's health and well-being. It can lead to depression, loneliness and vulnerability. Older people are more likely to suffer from isolation than younger people for many reasons, including being relocated to different types of living arrangements and care communities.

Digital technology provides an opportunity for people to remain connected with their friends and loved ones through the use of social media and video calls. Depending on the age of the person, they may require

training on how to use the hardware and software, or need someone to set up the technology for them to use. Many care homes within the UK have set up video calls using social media apps such as WhatsApp so that loved ones and friends can see each other while talking. This usually involves a member of the care staff actually using the technology for the person concerned.

Transition to remote communication and services

Remote communication is a method for communicating with other people online. Meetings, information and training materials are all shared over the internet, as well as the purchasing of products and services. There are two types of remote communication, synchronous and asynchronous.

- ▶ **Synchronous communication** – occurs in real time, for example phone calls, video calls and virtual meetings.
- ▶ **Asynchronous communication** – does not require all intended parties of the communication to be present at the same time, for example project management apps, online training materials, file sharing platforms, for example OneDrive or DropBox, information/instructional videos, reference/user guides.

Most businesses now communicate with customers online and it has become necessary for people to adapt to various forms of remote communication and services. If people do not adapt to the use of digital technology to communicate and access services, they can feel isolated as they do not receive the same level or speed of response as those who use technology.

Businesses promote the sale of products and services, and price reductions, via their websites, social media posts, emails and text messages. Without access to these forms of communication, people will not always receive up-to-date or regular information.

Due to lack of digital skills or technology

In order to access digital technology and use it to their advantage, people need the technology itself and the skills to be able to use it effectively. This can cause issues as technology can be expensive and people may not have the means to buy it (or upgrade the older technology they have). In addition, people need to be trained in the use of the hardware and software they have.

A lack of technology and/or the necessary skills to use it can result in people being unable to access online products/services and/or communicate with businesses effectively. Consider how many businesses only operate via the internet. This can exclude those without the skills or technology to access them.

A lack of technology and/or skills can also result in people being isolated as it prevents them from communicating with family and friends who they are unable to visit or see in person.

Locations

Not all locations within the UK or even other countries in the world have reliable internet access. Although digital technology provides people with greater access to information, reduces costs in the employment sector and enhances connectivity between people, it does not happen equally on a global scale. This imbalance with respect to digital access is known as the digital divide. An example is that in Europe 87% of Europeans have access to the internet, whereas in Africa, only 39% do.

Causes of the digital divide can be the high costs of the technology, a lack of knowledge and skills to use the technology, and the lack of infrastructure used to access the internet. The lack of infrastructure in locations across the world, and even some areas within the UK, results in people being isolated or, at the very least, feeling isolated.

Improved access to information

- ▶ **Educational** – access to the internet provides students with a wealth of information that is available to them at any time of the day or night. Virtual lessons can be made available for students who are unable to attend school; virtual learning environments enable the students to access course notes and submit their assignments.
- ▶ **Employment searches** – many businesses will advertise their employment opportunities through social media sites such as LinkedIn. People can sign up to be notified of potential vacancies that match their profile. There is also the opportunity to apply by accessing links to online application forms and upload curriculum vitae (CVs).
- ▶ **Access to 24/7 advice** – many businesses provide online ‘chat assistants’ for people to ask questions and obtain support. This can be for issues such as upgrading broadband, mobile phone packages, or reporting problems with equipment. The National Health Service (NHS) provides advice, not only through their 111 service, but also by accessing online advisors who will answer questions and provide advice via their internet platform. In addition, they provide up-to-date information relating to ailments and provide advice on when it is advisable to visit the doctor or a hospital.

Research

In small groups, carry out research into the use of digital technology by businesses and society. Identify countries where access to modern digital technology and access to the internet is limited (or not available). Prepare a report on the impact this has on the people and businesses in these countries. For businesses consider:

- ▶ accessing potential markets for their products/services
- ▶ communicating with their customers and potential customers
- ▶ expanding the business to a global platform instead of just in their own country.

For society consider:

- ▶ communicating with businesses
- ▶ communicating with each other
- ▶ accessing products/services
- ▶ additional training needs.

Test yourself

- 1 Define the term 'autonomous operation'.
- 2 Explain how the increased reliance on digital technology can result in a loss of privacy for society.
- 3 Describe two positive and one negative effect due to changes in communication brought about by the implementation of digital technology.
- 4 Explain the term 'scale of a business'.
- 5 Explain the difference between an active and a passive digital footprint.

2.2 The impact of unsafe or inappropriate use of digital technology and mitigation techniques to reduce impact

Impacts

Psychological impacts

Using digital technology in an unsafe or inappropriate way can lead to psychological harm.

Cyber bullying

This is bullying that happens online through the use of digital devices such as smartphones, computers and/or tablets. It can occur through text, SMS, apps, social

media, forums and gaming where people are able to view, participate in and/or share content. Cyber bullies send, post and/or share negative, false or harmful content about another person. This can include the sharing of private and/or personal information about someone that causes them embarrassment and humiliation. Some forms of cyber bullying are seen as criminal behaviour.

Cyber bullying occurs on:

- ▶ social media, for example WhatsApp, Facebook, Instagram, Tik Tok and so on.
- ▶ text messaging and other forms of messaging apps
- ▶ instant messaging, direct messaging and online chats
- ▶ online forums, chat rooms and message boards
- ▶ email
- ▶ online gaming communities.

Cyber bullying can harm the online reputation of people and the major concerns are that it is:

- ▶ **permanent** – it can be permanent and publicly available if it is not reported and removed. A negative online reputation can have an impact on a person's employment prospects, admission to colleges and universities and many other aspects of their lives
- ▶ **hard to notice** – it is difficult to recognise because people such as parents, teachers, or other relevant family members may not overhear or see the bullying taking place
- ▶ **persistent** – digital devices are available 24 hours a day, every day and therefore the communication is available immediately and continuously. This means that the person being bullied has difficulty finding any relief from the barrage of abuse.

Below are some examples of cyber bullying:

- ▶ sending emails, texts or instant messages to people with hurtful content
- ▶ sending neutral messages which tell the recipient something that is unpleasant or unusual
- ▶ bombarding someone to the point that they are being harassed
- ▶ posting hurtful comments about people on social media
- ▶ spreading rumours/gossip about someone online
- ▶ making fun of someone during an online chat that includes other people
- ▶ constantly and deliberately attacking/killing an avatar or character during an online game
- ▶ pretending to be someone else by creating a fake online profile

- ▶ taking an embarrassing photo or video of someone and posting it online to share with others without the victim's consent
- ▶ threatening someone online or in a text message.



▲ Figure 2.4

Emotional impacts of cyber bullying

- ▶ **Humiliation** – because the negative posts can be seen by vast numbers of people (many of them unknown to the victim), a person can feel exposed and embarrassed.
- ▶ **Isolation** – victims of cyber bullying can often be excluded by others, and therefore they often feel alone and isolated.
- ▶ **Anger** – many victims get angry about what is happening to them and in some cases even plot revenge on the cyber bully and retaliate.
- ▶ **Powerlessness** – victims of cyber bullying often feel unsafe and vulnerable. They feel powerless to prevent it from happening or even escape from the bullying taking place. If victims do not know who the bully is, it can make them feel even more insecure and powerless.

Mental health impacts of cyber bullying

- ▶ **Anxiety and depression** – victims can become severely stressed as they are constantly trying to handle issues surrounding the cyber bullying. This can stop them feeling happy and contented as well as increase their feelings of isolation. It can destroy a person's self-confidence.
- ▶ **Low self-esteem** – cyber bullies will look for things that make a person feel vulnerable, for example it could be the way they look or speak. When the victim's vulnerabilities are targeted, their self-esteem diminishes even more.
- ▶ **Employment/academic issues** – victims of cyber bullying will often lose interest in their work and/or academic studies. This can result in a higher level

of absenteeism than normal. This may be caused by the victims wanting to avoid the cyber bullies or because they are too embarrassed by what has been posted online. They find it hard to concentrate and therefore their work/studies suffer as well.

- ▶ **Suicidal thoughts and self-harming** – in extreme circumstances where victims have not received help and support, they will respond by self-harming as a mechanism to 'fight back', or even commit suicide as a means of escaping the incessant bullying. They are desperate and cannot see any other means to solve the problem.

Behavioural impacts of cyber bullying

- ▶ **Use of drugs and/or alcohol** – victims of cyber bullying may engage in some form of substance abuse. They can lose themselves in a world away from the cyber bullies.
- ▶ **Absenteeism** – this was discussed in the previous section.
- ▶ **Carrying weapons** – because victims can feel unsafe and threatened, they may carry a weapon to 'protect themselves'.

Physical impacts of cyber bullying

- ▶ **Eating disorders** – victims of cyber bullying may change their eating habits by skipping meals or binge eating. They feel that their life is out of control and therefore will use their eating patterns as something that they can control. If the victim has been bullied in relation to their physical appearance (being targeted and told that they are too fat or too thin), this can lead to eating disorders such as anorexia.
- ▶ **Stomach and gastro issues** – the stress and anxiety cause by cyber bullying can cause the victim to have an upset stomach that may lead to ulcers, abdominal pain, sickness and diarrhoea.
- ▶ **Sleeping disorders** – victims can have trouble sleeping, sleep too much or even have nightmares.

Mental health

Mental health issues do not just apply to cyber bullying but to any unsafe and inappropriate use of digital technology. Under the section above on cyber bullying, the impact on mental health due to cyber bullying was discussed. If people have a positive interaction with the use of digital technology, then they are less likely to suffer mental health issues such as anxiety and depression. People who have a negative interaction using digital technology can suffer with mental health problems to varying degrees.

While digital technology has potential benefits, it can also have potential dangers that can cause mental health issues. These can be caused by:

- ▶ cyber bullying (as discussed earlier)
- ▶ accessing inappropriate content
- ▶ contact with strangers
- ▶ being the victim of cyber criminals, for example the victim of scamming.

Addiction

An addiction to aspects of digital technology can be a major problem for some people, including addictions to gambling and gaming, and even social media.

Gambling

Online gambling websites have made gambling more accessible to people. Gambling is now available anytime and anywhere. One of the main issues with online gambling is that it can be kept secret. Smartphones have numerous gambling apps available to users and bank accounts are easily accessible. This can encourage gamblers to bet on impulse and continue to gamble to recoup their losses.

As the vast majority of gambling sites offer a 'free to play' version of their games, people try out the games and are not required to play with real money. These 'free' versions are programmed to play favourably for the gamblers, giving them a false sense of security and that they could win 'big' money. Unfortunately, once a person starts playing with real money, the programs are designed to play in favour of the gambling site. This results in people not winning the 'big' money as they had hoped. People are also encouraged to set up an online account with their bank details and continued play will result in large losses of money.

Gaming

Gaming addiction is diagnosed as the compulsive playing of online games that can cause physical and/or mental issues. Some people are unable to stop playing online games for long periods and this can have a detrimental effect on their health. There have also been some cases of fatalities associated with long periods of online gaming. Some people are able to stop and carry out their work or academic studies, but they are still obsessed with online gaming, and it dominates their lives. This can have an impact on their relationships with others, other activities that they could be carrying out and even their life ambitions.

Online gaming can cause changes to the chemistry of the brain and in particular to something known as the brain's 'reward centre'. This encourages the

compulsive need to continue to play the games, regardless of any negative impact. It is well known from research that addiction can have an impact on a person's relationships, social life, view of the world, life ambitions and prospects, and general well-being.

Social media

Research has confirmed that there is a link between social media use and negative mental health issues. While social media platforms can have benefits, excessive use can make people increasingly unhappy and isolated. This can be due to social pressure for sharing things with others, as well as comparing one's own lifestyle and material possessions to other people's posts and the advertisements from businesses trying to increase their customer base.

Many social media platforms promote **curated content** to users. These are advertisements and posts designed to appeal to a person based on their interests. These can have a positive or a negative impact on people depending on the content. A person can be made jealous or even depressed when they compare their lifestyle with that of someone else, based on what they have seen on social media.

Social media creates an environment where people can compare their real 'offline' self to the filtered and edited online version that they promote to others. This can cause issues with mental well-being and a person's perception of themselves. Excessive use of social media can cause anxiety and depression because people are constantly comparing themselves to others, making them self-conscious, and with a need for perfection and order. This creates social anxiety disorder.

Social anxiety can also be triggered when people have a fear of 'missing out'. This is a fear of not being included or missing out on a social event. They become anxious that they have not been missed by anyone because they were not there or that people have forgotten about them. This can have an impact on a person's self-esteem and result in them constantly checking their social media accounts to ensure that they are not 'missing out' on anything. This behaviour can have an impact on a person's personal relationships, work life or education.

Stress

The unsafe and inappropriate use of digital technology leading to stress has been covered in the sections above. There are various ways that a person can

identify that they are stressed through using digital technology:

- ▶ They try to juggle too many different things even though they are comfortable using digital technology.
- ▶ Their sleep is disturbed by having digital technology in the bedroom.
- ▶ They spend too much time using social media.
- ▶ They are constantly on their digital device.
- ▶ They are too busy to eat at regular meal times.
- ▶ There is no time for themselves, just to relax.

Physical impacts

Using digital technology can cause physical harm.

Posture

Back pain in particular is due to poor posture when using digital technology. Smartphones and computers are used consistently every day and it is easy to put unnecessary strain on the muscles and ligaments of the spine and neck. People who use smartphones and similar digital technology tend to hunch their shoulders as they stare down at the device. This creates bad posture. It can lead to problems such as nerve pain, headaches and arthritis. In addition, by leaning over at relatively high angles, for example 30 degrees, 40 degrees or more, there is a risk of the neck and spine being pulled out of alignment.

People now sit down for longer using digital technology, sometimes for up to eight hours a day. This lack of movement can cause neck and spine problems.



▲ Figure 2.5 Posture when sitting.

Eye strain

People do not realise the impact that prolonged use of digital technology can have on their eyesight.

Computer vision syndrome (CVS) is the term used for people such as office workers who spend

long periods of time in front of the computer. CVS includes:

- ▶ headaches
- ▶ difficulty with focusing
- ▶ itchy, burning, watery eyes
- ▶ dry eye
- ▶ double and/or blurred vision
- ▶ sensitivity to light (photophobia).

These symptoms can occur because a person:

- ▶ blinks less often
- ▶ looks at text directly in front of them instead of looking down (this allows more air to get into the eye, therefore drying it out)
- ▶ looks at the screen more closely than normal, for example holding a smartphone closer to the eyes to read it.

Repetitive strain injury

Repetitive strain injury (RSI) is pain felt in the muscles, nerves and tendons caused by repetitive movement and overuse. It affects the following parts of the body:

- ▶ forearms and elbows
- ▶ wrists and hands
- ▶ neck and shoulders.

The symptoms can be mild or severe, and develop gradually over time. Symptoms include:

- ▶ stiffness
- ▶ throbbing
- ▶ tingling/numbness
- ▶ pain, aching or tenderness
- ▶ weakness
- ▶ cramp.

Reduction of physical activity

Using digital technology such as computers, laptops, gaming consoles, smartphones and so on has resulted in people taking up fewer physical activities, for example walking, playing sport and so on. People will spend hours at a time on their digital devices, usually sitting down. This can lead to health issues such as obesity and weakness in the muscles, tendons and ligaments within the body.

Disturbed sleep patterns

We know that the overuse of digital technology can disrupt sleep patterns. Most people will take their smartphone with them when they go to bed or have smart devices within the bedroom. Digital technology emits blue light that can interrupt sleep patterns. In addition, having electronic devices in the bedroom can result in people being tempted to continue using the

device, for example to check social media posts and messages. This makes it more difficult for people to fall asleep.

Mitigation techniques

As with all things, there are ways that we can reduce, and in some cases even prevent, the risks associated with using technology.

Regulate use of digital technology

As we live in a technological age, it is not possible to totally avoid all the risks associated with technology, but we can do things to reduce them. Here are some examples of how to regulate the use of digital technology.

- ▶ Choose to do more outdoor activities that do not require the use of technology. These can be physical activities such as riding a bike, going for a walk or going swimming. These can be done alone, with friends or with family members.
- ▶ Limit the amount of time spent on social media. Avoid browsing aimlessly and only use it for a defined purpose such as researching local events, holidays and/or concerts. Once the research is completed, log off, shut down the social media and leave it for a few hours.
- ▶ Set yourself a goal to read 10 to 30 pages of an interesting book, complete a task, or have a phone call with someone before checking your digital device.
- ▶ Set yourself projects. This could be learning a new skill such as drawing/painting or learning a language. Decorate a room such as your bedroom – anything that is creative, useful and does not require technology.
- ▶ Most importantly, turn off all digital devices in the bedroom before sleeping. In the case of mobile digital devices, do not take them into the bedroom at all when you are going to bed.

Report misuse to relevant authority

People who have been a victim of a cyber crime, such as a scam or cyber bullying, often feel reluctant to inform anyone and ask for help. There are many ways that crimes can be reported, and the authorities are supportive and can help you as well as preventing it happening to others.

- ▶ **Report it to the police** – they have specially trained officers to deal with all forms of harmful activities such as cyber bullying and internet fraud.
- ▶ **Notify the social media hosts** – you can report offensive posts using the report button and the posts are removed immediately. The social media

hosts will investigate the post and if necessary, remove the person's account who has posted it.

- ▶ **Identify the relevant authorities** – simple searches online can find the authorities who can deal with all types of cyber issues that cause harm to others.
- ▶ **Speak to family and/or friends** – so that they can support you and give you advice.
- ▶ **Report it to a teacher, manager and/or human resources department** – talk to a teacher if the activities are occurring within the school/college or your manager or HR department if it is in the workplace.

Display screen equipment and workstation assessment

The incorrect use of display screen equipment (DSE) and poorly designed workstations can lead to neck pain as well as pain in the shoulders, back, arms, wrists and hands. In addition, this can cause eye strain and fatigue. It is not just about the use of the digital equipment but also other factors such as the chair, having insufficient workspace, not taking regular breaks and a lack of training.

Employers have to comply with regulations and carry out regular workstation and DSE assessments to ensure that employees are not put at risk. The legislation covers:

- ▶ fixed workstations
- ▶ mobile/home/remote workers
- ▶ hot-desking, where employees frequently change desks and do not have any fixed work area allocated to them. Employees should carry out risk assessments if they regularly change desks.

Employers must by law:

- ▶ carry out DSE workstation assessments
- ▶ reduce risks by ensuring that DSE users take regular breaks or do a different type of work for a period of time as a form of a break from DSE
- ▶ reimburse the costs of DSE user eye tests
- ▶ provide employees with training and information.

The following link from the UK Government's Health and Safety Executive (HSE) website will provide you with a suggested checklist for carrying out such risk assessments.

www.hse.gov.uk/pubns/ck1.htm

Self-exclusion

Self-exclusion is when a user tries to remove themselves from accessing activities such as online gambling and the overuse of apps, websites and social media. A user can

ask a gambling provider to exclude them from gambling/using their site for a set period of time. This is usually for a period of between 6 and 12 months but in some instances can last for a number of years. This prevents the user from gambling during the set time period. It is a legal requirement that online gambling providers within the UK offer this service. There are even apps that can be downloaded onto smartphones, laptops, tablets and computers that will actually prevent the user from accessing any gambling and/or gaming sites.

Social media providers do not currently provide a self-exclusion option, so it is up to the user to make some decisions to help themselves. This can include removing social media apps from their digital devices. Many people believe that social media providers should offer the same service as the online gambling and gaming sectors.

Test yourself

- 1 Discuss how social media has had a negative effect on mental health.
- 2 Explain how cyber bullying can harm the online reputation of people.
- 3 Identify four examples of cyber bullying.
- 4 Explain how a person can regulate their use of digital technology.
- 5 Describe the term ‘computer vision syndrome (CVS)’.

Project practice

This can be carried out as an individual or in small groups.

A local school is concerned with the increase in children becoming addicted to social media and online gaming. They have asked you to prepare a presentation to deliver to the schoolchildren to include:

- ▶ the impacts of the unsafe and inappropriate use of digital technology
- ▶ the steps that can be taken to mitigate the risks.

You have been asked to research real-life examples of the impacts and include these in the presentation.

Deliver your presentation to the rest of your group.

Assessment practice

- 1 Discuss the psychological impact of cyber bullying on individuals.
- 2 Explain how the unsafe or inappropriate use of digital technology can cause a reduction in physical activity.
- 3 Describe how digital technology in the bedroom can disrupt sleep patterns.
- 4 Explain how digital technology can impact on society through changing behaviours.
- 5 Describe how someone addicted to online gambling can use self-exclusion.
- 6 A person is a victim of cyber bullying via social media. Describe the steps that they should take to help themselves.
- 7 Identify two ways that a person can regulate the use of digital technology to mitigate against personal risks.
- 8 Describe the impact of unsafe and inappropriate use of digital technology on mental health.
- 9 Discuss the impact on company culture of the increasing reliance on digital technology.
- 10 Explain how the increasing reliance on digital technology can create a dehumanisation of service.

Core element 3: Data

DASHBOARD

Last Updated:
3 min ago

92%

Data Availability

More info ➔

Evolution

Metric

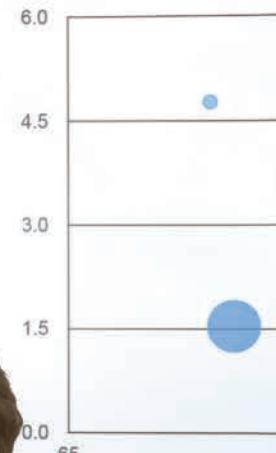
Actual vs Target

You are going to learn about data and how it can be used to support organisational needs, as well as the range of ways in which data can be sourced and stored.
You will learn about the different types of data and how organisations can use them when sourcing data. All data needs to be managed, and the method used will depend on how the data is collected and entered into the digital system. There are a range of methods that can be used to ensure the validity of the data to ensure that it is fit for purpose on data entry, and how it can be maintained to ensure its ongoing usefulness. You will also learn about the resource implications of entering and maintaining the data.
Data can be stored in a range of different formats and structures to ensure that the stored data is organised and accessible for the end users. Data can be presented and visualised using a range of different methods. You will learn about these different methods and their suitability to meet the needs of the target audience.
Data can be used by organisations in different ways and you will learn about some of these common uses of data. Data is a very valuable asset to any organisation and access to it has to be controlled and managed. You will learn about the different data access management tools and controls that can be implemented by an organisation to increase the security of the stored data.

Actual Target

\$3.4M	82.0%
\$1.2M	108.7%
\$850.3	71.0%
96.0%	96.0%
15432	145.0%
98.3%	105
46.9%	8

Products positioning



Top 10 products

430

Learning outcomes

In this core element you will learn about:

- 3.1** The fundamental characteristics of data
- 3.2** The fundamental functions of information systems and the application of data
- 3.3** The concepts and tools of data modelling
- 3.4** The concepts involved in data entry and maintenance
- 3.5** Characteristics of data formats and importance for analysis

- 3.6** Methods of presenting and visualising data and their suitability for application
- 3.7** Applications of data within an organisation
- 3.8** Types of data access management across platforms within a digital environment
- 3.9** Types and application of access control methods

3.1 The fundamental characteristics of data

There are many different types of data that can be collected, stored and used. Which type of data is collected, stored and used will depend on what the data is needed for.

Data types

The most common data types are outlined here.

- ▶ **Numeric data** – represented using a range of different number types. These can be exact types such as integer, decimal and currency or approximate types such as floating point.
- ▶ **Text data** – represented using characters, words and paragraphs. This book is an example of the use of text data.
- ▶ **Media data** – represented either visually or in an audio format. This type of data is all around us and includes images, sounds and videos. Websites use media data to increase usability and understanding of the message they are providing. It can sometimes be easier to understand facts and figures if they are presented using the media data type.
- ▶ **Geospatial data** – represents elements and components that are found on the Earth's surface – a location. These components can be man-made or natural. Examples of geospatial data include Google Maps, satnav maps and weather maps. One use of geospatial data was during the Covid-19 pandemic when governments and health organisations used geospatial data to monitor the locations of coronavirus cases.
- ▶ **Temporal data** – represents a moment in time and is usually shown with a date or timestamp and a duration. For example, the data collected during the 2021 UK census represents the temporal data on 21 March 2021. Temporal data can be used to analyse patterns, for example rainfall, on a specified date

Industry tip

Every organisation, whatever its size, will source, generate, store, process and analyse data to help it flourish. What that data is will depend on the organisation sector.

Irrelevant data is worse than having no data so all data sourced, generated, stored and processed, and how it is analysed, must be relevant to the organisation, its function, needs and requirements.

over the years. By using temporal data it is possible to identify trends and patterns which can then be used to make predictions.

- ▶ **Logical data** – has two states or choices. This type of data is also known as Boolean data. This means the data can be true or false, on or off, or 1 or 0.

Sources of data for organisations

Organisations can gather data from a range of sources. These sources can be classified as internal or external. Internal data comes from within an organisation, with external data being sourced from outside the organisation.

Internal data

The type of data that is sourced internally will depend on the function of the organisation.

Sales data

As an example, a retail organisation will have internal data related to sales. Sales data shows the sales of goods over a time period. This type of data can be used to predict future sales to ensure that enough goods are available to meet demand.

Marketing data

Marketing data is sourced from advertising campaigns. The advertising can be in digital form, such as emails, social media, TV commercials and websites. Advertising can also be in print format, for example leaflets, or in newspapers. The data sourced will show how successful the campaign was, based on the increased number of sales. The marketing will include **engagement data**. This is the response by customers through, for example, online surveys, clicking links in emails or social media, or by using a specific offer code on a print format.

Financial data

All organisations will generate internal financial data. This type of data will show the financial health of the organisation. The data will include income and outgoings and the total profit or loss of the business. Financial data is an ongoing source of data as financial income and outgoings will change from month to month.

Employee data

Every organisation has employees. The HR department will collect and store employee data. This data will be collected directly from the employees, but some of it may have to be verified by external sources. Data stored about employees will include personal details, contact and emergency contact details, salary, employment history and qualifications.

Customer data

Customer data is likely to be stored in a customer relationship management (CRM) system. This data will include contact details, order history and any interactions with the organisation, such as complaints.

There is more information about confidential company, customer and employee (colleague) information and data in section 10.1, p. 237.

Usage data

Most organisations have an online presence. This usually includes a website and social media accounts. How much the online presence is used by customers and clients is important. Each time an online platform is accessed, this can turn into a new customer or client, or be an interaction in the form of, for example, an order for goods. Traffic to a website can be measured and the organisation can use this data to, for example, increase accessibility of the website or streamline the process of interacting with the organisation.

Website traffic is the number of people who visit the website. The greater the traffic, the more opportunities there are to increase the customer and client base. Website traffic monitoring software will provide an organisation with data and information. This information can be used to make informed decisions about any remedial action needed to increase the performance of the website or to enhance the design.

Monitoring users on a website can take many forms. These can include:

- ▶ checking how long a user spends on the website
- ▶ if the user is a registered user then how long they are logged in for
- ▶ how many clicks the user takes to carry out the purpose of their visit.

This data can be used to improve the user experience: if the website is intuitive and easy-to-use then it is likely that users will visit the website and be able to carry out the purpose of their task. Data may be analysed about specific products bought on a website by a customer which can lead to an organisation targeting marketing about 'similar but different' products.

For example, if a customer regularly purchases dog food from an organisation, then the data would show that there was a high probability that the customer owned a dog. The organisation could then send this customer targeted marketing about other dog-related products. The targeted marketing could be, for example, an email, or recommendations next time a customer visited a website.

External sources

No organisation can function without external data.

Public

There are vast amounts of data stored which can be accessed by anyone – this is **public data**. One example of this is **open data**. Open data is data that everyone can access and use without legislative restrictions. An example of open data is Google Open Data.

Data repositories are where data is stored. A data repository is somewhere that:

- ▶ holds data
- ▶ makes data available to use
- ▶ organises data in a logical manner.

A data repository can be:

- ▶ public where anyone can access data or
- ▶ private where a user needs to, for example, register, pay a subscription or one-off fee, or request the data under a Freedom of Information request.

Types of repositories can include a data warehouse or a data lake.

The Freedom of Information Act is covered in section 8.1, p. 193.

Data warehouse

Data is key to organisational decision-making. But this is often complicated by the fact that data is held in many places and in a variety of formats across the business.

The solution to this problem is a data warehouse: a central collection of key data, integrated into a pre-defined format. This allows the data to be used across the business to make business-critical and evidence-based decisions.

Data warehouses are sometimes known by other names such as management information systems, executive information systems or decision support systems.

Data in a data warehouse will be taken from a range of internal and external sources.

This data will therefore likely be in a range of formats and will therefore need to be subjected to **data cleaning**. This process converts the data into the standardised and pre-defined format of the data warehouse.

Key term

Data cleaning: the process of going through data looking for errors and correcting them, or excluding data where errors have been located.

A data warehouse can be used to process and analyse data on previous data rather than data that is being currently used and updated by an organisation. Data warehouses are used by specific business users to analyse and extract a particular meaning from the data that was defined when the data warehouse was set up. Analysing data held in a data warehouse usually focuses on changes in data in any given time period, for example analysing data on sales in the previous year.

Data stored in a warehouse must be secure, reliable, easy to retrieve and easy to manage to enable analysis to be carried out. The data warehouse can be stored on physical storage devices or in a secure area in the cloud.

Data lake

Data lakes are data stores that hold data in an unstructured way. Unlike data warehouses there is no defined format to the way the data is structured; the data is stored in a raw state as it may not have been processed.

Unlike a data warehouse where the sources and format of the data are defined, a data lake takes data from all sources in any data type. The data is only converted into a predefined format when it is ready to be used and analysed.

It is possible that some of the data stored in a data lake will never be used. This may be because the data lake contains all data collected over time in a raw and unprocessed state.

One benefit of a data lake is that, because there is so much data held there, a range of analysis and processing can be carried out on the stored data.

Data stored in a data warehouse or data lake can be referred to as **big data**.

Government

Governments of all countries collect and store data. Most of this data is open data and can be accessed by anyone. The data stored on the UK Government's website provides open data on a range of topics. It

Key term

Big data: very large data sets that can be analysed to produce information such as trends and patterns. Big data cannot be analysed using traditional data analysis tools.

is also possible to access data through the Office of National Statistics website.

Research

Access the website for the Office of National Statistics. Investigate the available statistics for your area relating to the population demographics.

Suppliers

Most organisations have suppliers. The suppliers will provide goods if the organisation is in the retail sector, or materials if they are in manufacturing. The external data supplied is likely to include their selling price to the organisation and recommendations about the selling price. Organisations will also have to purchase items to enable them to function. These items will range from stationary to furniture. Other items bought from suppliers will include hardware, software and cloud services.

Competitors

All organisations have competitors. These are other organisations who provide the same goods and services. An organisation will need to keep up to date with their competitors to ensure that their customers do not move to their competitors. The data that is sourced from competitors is likely to be prices, discounts and delivery costs.

Sector/industry

Many sectors and industries have associated professional bodies. These bodies are directly linked to the sector and can provide a range of data. This data can range from changes in legislative requirements to providing certification for employees. There are many organisations that aim to provide standards and guidelines specific to any given defined sector. Data can also be provided by other organisations or businesses within the same sector.

Industry standards related to the digital industry are covered in section 8.3, p. 207.

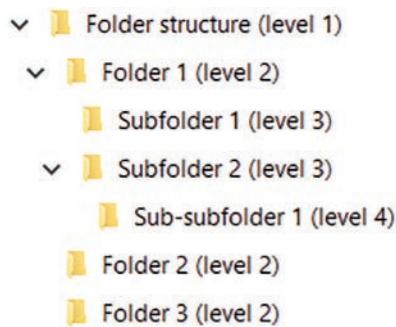
Research

Investigate the four different types of market data – engagement, financial, employee and customer.

Create a digital communication detailing each of these, including the purpose and the types of data that could be gathered. The digital communication should be aimed at 16–18 year olds.

Test yourself

- 1 What is meant by temporal data?
- 2 Which department will collect and store employee data?
- 3 What is website traffic?
- 4 What is the difference between a data lake and a data warehouse?
- 5 What is open data?



▲ Figure 3.1 A folder structure

Data storage

Data needs to be stored so it can be processed and used. Data can also be used to assist in analysis.

Data can be stored on premises or in the cloud.

Methods of storing data on premises

Internal databases

Data can be stored in an internal database. This means the database is usually stored on a database server which is on the premises of the organisation. A database is an organised collection of data, containing tables, records and fields. Most databases used in organisations are **relational databases** which are designed using entity relationship diagrams (ERDs).

ERDs are covered in section 3.3, p. 82.

Relational databases are covered in section 3.5, p. 88.

File structures and formats

Data is stored in files which can then be stored in folders. This leads to a hierarchical directory structure, and opening a folder will show all the files and subfolders which it contains.

A directory structure can make it easier for the end user to locate files as long as the folder structure is logical. What is important is that folders and files are named with meaningful names. For example, a folder named 'PT3FB' is an example of an unmeaningful name. However, a folder named 'Unit3ClassNotes' provides details about the files that could be saved to and retrieved from it.

Key term

Relational database: a database that has relationships between the tables to reduce data duplication.

Activity

Create a digital communication providing rules and guidance to be used when saving and naming files, and creating and naming folders. A range of data types should be included in your communication.

The help sheet should be aimed at 16 year olds starting a course at your centre.

It is also important that files are saved in the correct **format**. Most software packages will have a default format that their data will be saved as. This is shown in the file name extension. For example, Microsoft Word, by default, save files with the file extension .docx.

Most software packages will provide a list of options that can be used to save the files. These are useful when data has to be shared as there are common file extensions that will allow files to be opened on a range of different applications. One common data file format is CSV. This is used by organisations to move data between software that may be incompatible. Many data handling software packages support the saving, importing and processing of CSV files.

For example, a user may need to transfer information from a database that stores data in a proprietary format, to a spreadsheet that uses a completely different format. The database program will be able to save the file in the CSV format which will then enable the spreadsheet package to import, save and process the data. The file extension for CSV files is .csv.

Research

Investigate the software applications that are used in your centre.

- ▶ What are the default extensions for each application?
- ▶ What options are available for saving in different formats?

Hard drives

Data can be stored on hard drives. There are two main types of hard drive – hard disk drive (HDD) and solid state drive (SSD).

- ▶ **HDDs** – spinning disk, mechanical hard drives. They are usually used where the requirement for speed and performance is not as important as the cost. As HDDs have physical limitations and are mechanical by nature with numerous high-speed moving parts, they have a high failure rate compared to SSDs.
- ▶ **SSDs** – used where speed and performance have a greater priority than cost. SSDs do not have any moving parts and can read and write data at a much faster rate than HDDs.

The risk of failure is not as great with an SSD as it is with an HDD.

Research

Research the differences between HDDs and SSDs and complete the table below.

	HDDs	SSD
Cost		
Speed		
Storage capacity		

Portable storage devices

Portable storage devices are devices that usually connect to a USB port of a digital device and are used to store and retrieve data. They are also known as external storage devices as they are external to any digital system. The most common examples of portable storage devices include:

- ▶ USB sticks/thumb/flash drives
- ▶ external hard drives.

File servers

File servers are dedicated to storing data held in files. A file server will:

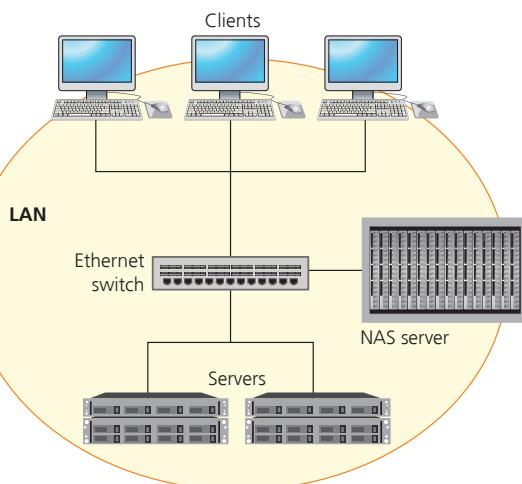
- ▶ store data in files
- ▶ index the files
- ▶ identify the location of a file when it needs to be retrieved
- ▶ take responsibility for the security of the files
- ▶ facilitate access to files from the network and can allow internal and external access.

By using a file server, limited storage needs to be made available on workstations across the network.

Network Attached Storage (NAS)

This is a storage device that is connected to a network and acts as a central point for the storage, management and access of files. As the NAS is connected directly to the network, it can only be accessed by authorised networked devices and users. NAS is configured with data transfer protocols (DRPs) for example, NFS (Network File System) allowing the transmission of data between devices.

One of the main benefits of a NAS is the fact that additional storage can be added to it easily. To increase the storage capacity, there is just the requirement to add additional disk drives. Data recovery and backup is easier with a NAS, but it should never be the only backup option used as accidental deletion, failure and/or virus infections cannot be overcome as there is no inbuilt option to recover deleted files. Security is always a major



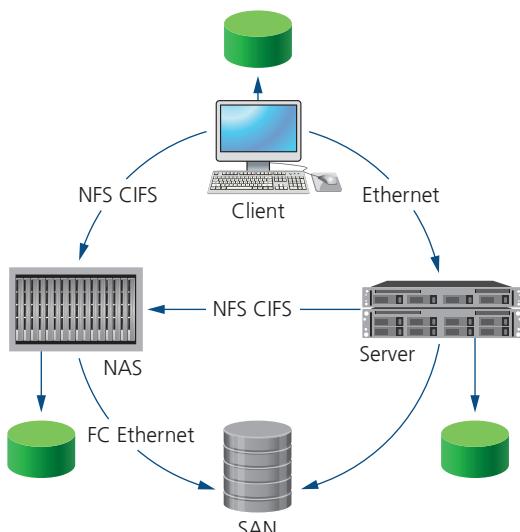
▲ Figure 3.2 Example of a NAS configuration

concern where data is involved and like any other system/device that is used, it is always important that they are regularly maintained and updated and that any system connected to the same network, along are carefully monitored and controlled.

Storage area networks

A SAN is a network of interconnected storage devices accessible by computers and servers. Its purpose is to store, manage and protect data. SANs use block storage where data is broken down into 'blocks' and are stored separately. Each block is allocated a unique identifier and a software program reassembles the requested blocks. Once a request is made, the software identifies the relevant blocks based on their unique identifier and reassembles them into one file that is then accessible for the user. The block storage system means that data can be accessed more quickly than a standard file storage system and can be accessed using different types of operating systems.

A SAN network is usually connected using fibre optic cabling which is faster than other forms of cabling and uses a protocol known as a fibre channel, providing better performance. SANs are expensive in relation to the technology required and it is also complex to set up, configure and maintain. Invariably, this means that there is the additional cost for a skilled network manager to monitor and maintain the SAN. SANs, however, are more easily scalable by adding additional hard disks and switches.



▲ Figure 3.3 Example of a SAN configuration

Cloud storage

Data can be stored in the cloud. Data that is stored in the cloud is usually referred to as **data as a service (DaaS)**. This is a deployment model and/or data management strategy that focuses on public or private clouds to deliver data-related services such as storage, processing and analytics. Organisations are able to use cloud-based software applications delivered through the network rather than use dedicated hardware servers for specific tasks for specific data.

DaaS is about sharing a common infrastructure as well as sharing data among teams, therefore supporting greater collaboration and knowledge transfer within the organisation. Organisations control most of the storage, processing and analytic requirements in the cloud which reduces **data sprawl** and **data silos**. It provides a secure platform for data and supports demand access for business units, departments and customers, irrespective of their location.

There are three main ways that data can be stored using DaaS.

File storage

This is a method of storing data in the cloud that provides access to data through shared file systems. Compatibility makes cloud file storage ideal for organisations that rely on shared file systems. A file system in the cloud is a hierarchical storage system that provides shared access to file data.

Users can create, delete, modify, read and write files. The files can be logically structured using meaningful file names to speed up access. A path is used to provide access to the data which can make accessing the data relatively slow as the whole path has to be travelled.

Object storage

This is a flat structure in which files are broken into pieces and spread out among the storage devices.

Key terms

Data sprawl: the vast amounts and variety of data produced by organisations on a daily basis.

Data silo: a group of raw data accessible by one department but not available to the other departments within the organisation.

Each piece of data is classified as an object. The data is kept in a storehouse rather than as a file. The data is stored with its metadata and a unique identifier is allocated.

Object storage requires an **application programming interface (API)** to access the data.

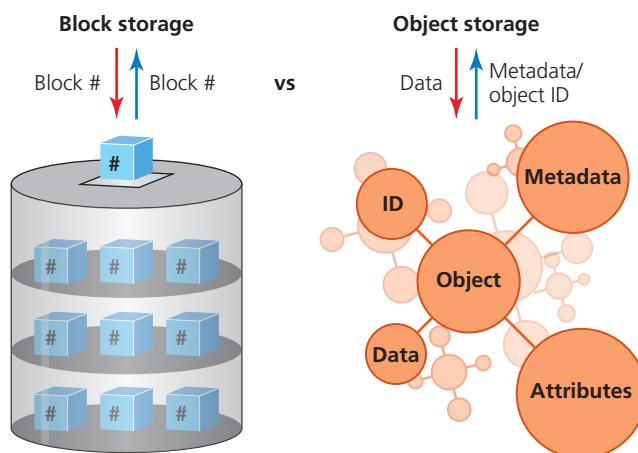
APIs are covered in section 3.8, p. 96.

Block storage

This splits a file into blocks of data and stores these blocks as separate pieces. Each block of data is given a unique identifier, as in object storage. This means that the data can be stored anywhere.

Block storage in the cloud is usually linked with a SAN and so must be linked to a server. When the data is needed by a user, the blocks of data are reassembled and sent to the requesting device. The data can be quickly accessed by the user as block storage does not need a path, unlike file storage, to be travelled. Block storage is usually used when large amounts of data needs to be stored, edited and accessed quickly.

Elastic cloud/scalable storage is covered in section 5.5, p. 145.



▲ Figure 3.4 The differences between block storage and object storage

Cloud-based database services

A cloud-based database is a database built and accessed through a cloud platform. The database provides most of the same functions as a relational database stored on premises but has the flexibility of utilising a cloud computing platform. The database is accessed through a web interface or an API.

Where the database is cloud-based it can be referred to as **database as a service (DBaaS)**. This means that usually the database service provider takes responsibility for installing, building and maintaining the database. The database owners are charged according to their usage of the service. This is a type of **software as a service (SaaS)**.

Cloud computing and software as a service (SaaS) are covered in section 5.5, p. 144.

Test yourself

- 1 What are the differences between an SSD and an HDD?
- 2 What is a data silo?
- 3 What are the three ways data can be stored in DaaS?
- 4 What is it called when a database is cloud-based?

3.2 The fundamental functions of information systems and the application of data

All organisations use data and information systems to be able to store, process and analyse data. Some of this data will be generated internally within the organisation while other data will be taken from other sources.

There are different functions of information systems which enable organisations to productively process and use data. All information systems have the same basic functions. How an organisation uses these functions will depend on the data being processed and analysed, and how the results are to be used.

The core functions of data systems are input, saving/storage, processing, output and feedback loop, as outlined here.

Input

Input is the collection of raw data. The data is inputted into the system ready for processing.

Saving/storage

Data that has been input into the data system can be saved or stored so it can be used again. The data

will have to be in an appropriate format based on what processing will take place. The data may be stored in, for example, a spreadsheet or database format. The data will need to be restructured and sorted into an order to meet the organisation's requirements. Saved data can be used in the future to be searched, processed and analysed. The saved data can also be edited and resaved. Data may also have to be saved/stored to meet legislative requirements.

Legislation is covered in section 8.1, p. 188 and the implications of the legislation are covered in section 8.4, p. 213.

Processing

Processing is used to convert the data into output that is meaningful and meets the specified requirements and needs. There are four main tasks that can be performed during processing:

- ▶ **Analyse** – searches and queries can be carried out on the data to meet the specified needs and requirements of the organisation. Data that has been saved in the data system can be searched many times using different search criteria.
- ▶ **Update** – over the life of data it will need to be updated to ensure that all records are up to date because if the data held is out-dated then it is of limited use. This may be as a result of routine maintenance but is also a legislative requirement.
- ▶ **Remove** – as with the task of updating, data should be removed when it is no longer relevant. This task can also apply to the removal of any duplicated data entries to maintain the integrity of the data. This is also known as data cleansing.
- ▶ **Integrate** – different data sets, types and formats can be combined into a single location – a data warehouse. The aim of data integration is to generate valuable and usable information to help solve problems, and to produce full and complete outputs that meet specified needs and requirements.

Data warehouses are covered in section 3.1, p. 75.

Output

Output is when the processed and analysed data, the output, are sent to the relevant people or

places. The output can be used to identify and locate required specific information and data to meet a specified purpose. It is at this stage that the output can be used to provide an insight to support decision making.

Feedback loop

Feedback is output that is returned to, usually, senior management. They can use it to help evaluate the process to, for example, correct the tasks carried out at the input stage.

Test yourself

- 1 Where can input data be sourced from?
- 2 Identify one format that data can be saved in.
- 3 What is processing?
- 4 Identify one task that can take place during processing.
- 5 What is meant by the term 'output'?

3.3 The concepts and tools of data modelling

One definition of a data model is:

'The logical interrelationships and data flow between different data elements involved in the information world that also documents the way data is stored and retrieved.'

A data model will help when a database is being designed and will ensure that the final database is fit for purpose and has no omissions. The final database will be efficient meaning that all database relational tables, primary and foreign keys are fully and completely defined which will lead to little chance of any omission or errors in the structure.

This will ensure that all the data needed by the database, based on the requirements of the end-user, will be correctly and fully represented with no missing or redundant data.

Type	conceptual data model	logical data model	physical data model	hierarchical database model	relational model.
Definition	defines what the system contains.	defines how the system should be implemented, regardless of the database management system (DBMS).	describes how the system will be implemented using a specific DBMS.	shows the database structure on a hierarchical (tree) structure.	shows a database as a collection of relationships.
How used to organise data	to scope, organise and define rules, and to identify the data used.	To develop the rules and data structures. This model expands on the conceptual modelling.	The actual implementation of the database.	to show the relationships between the tables, records and fields.	to show the relationships between the tables, records and fields using primary and foreign keys.
Techniques	ERD	ERD Data Dictionary	ERD	ERD	ERD Data dictionary

▲ Table 3.1 Types of data model and their uses

Data dictionary

Data dictionaries contain information about the data that will be included in a database. It contains metadata. A data dictionary is usually created as part of physical data modelling and will include details about each entity (table) and its attributes. The contents of the data dictionary will vary dependent on the software package that is to be used to implement the output of the logical data modelling.

Entity relationship diagrams

An entity relationship diagram (ERD) can be used during the creation of data models and to design relational databases. There are three main parts to an ERD including:

- ▶ entities which will become the tables
- ▶ columns which describe the tables and are also called attributes which will become fields in a database

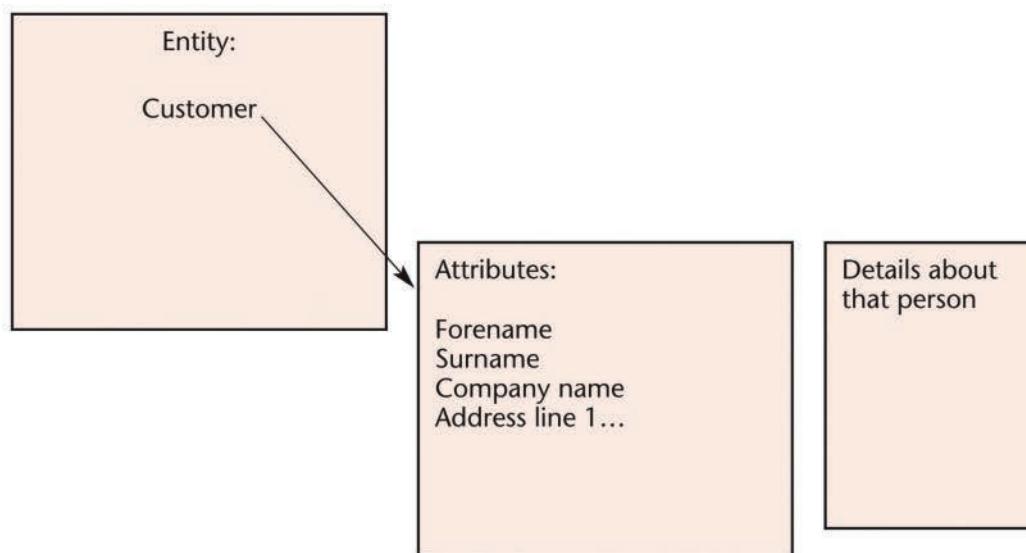
- ▶ relationships which are how the entities (tables) are linked. Relationships can be one-to-one (1:1), one-to-many (1:M, M:1), or many-to-many (M:M). These show the cardinality.

Research

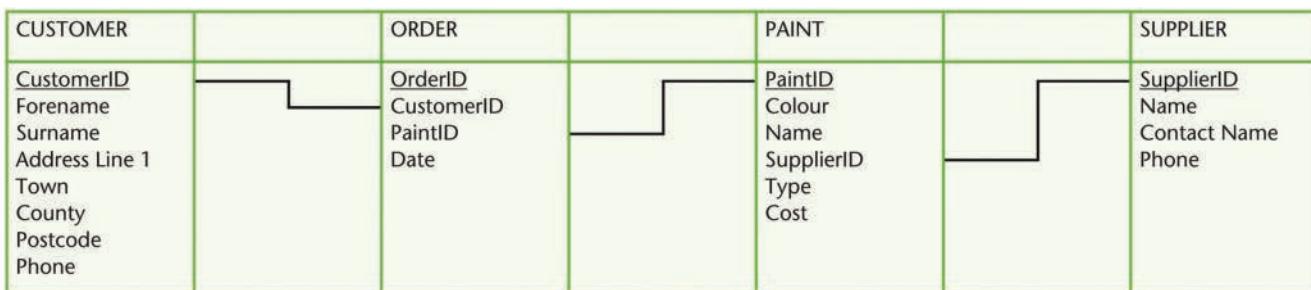
There are many different notations that can be used when creating an ERD. Investigate these and select a set that you will use for this course.

Create a list of the notations and their meanings.

A completed ERD should not include any M:M relationships. If a M:M relationship does exist, then a link entity needs to be included.



▲ Figure 3.5 First ERD for paint shop



▲ Figure 3.6 Resolving M:M relationships for paint shop

For example, a shop sells paint to its customers. The shop has a number of suppliers, each of which supplies many products. Many customers can buy many products. The ERD would look like Figure 3.6.

The M:M relationships need to be resolved. This is done by a link entity. In this case the link entity is a list of products from the product entity that a specific supplier can provide. It can be seen that the link entity contains the many relationships, but these are broken down into a 1:M relationship.

This stage of the ERD modelling would be part of the conceptual data modelling process.

When the ERD is undergoing physical data modelling, the ERD will be used to create the database. Primary and foreign keys will be used so that the links in the ERD can be created and to remove any data duplication. The ERD can also be known as relational database modelling.

As part of the logical data modelling stage, more detail is added to the ERD to show how the **DBMS** is going to be implemented. The ERD is developed to show the entity (table) name, attributes, **primary** and **foreign keys** and relationships defined.

Activity

Create an ERD showing the relationships between teaching staff, students and courses at your centre.

Key terms

DBMS: database management system.

Primary key: a field in a table that allows each record to be uniquely identified. For example, every person 16 years or older in the UK has a National Insurance number. This uniquely identifies a person.

Foreign key: these are used to link tables together. A foreign key is a field in one table that is linked to a primary key in a different table.

Data flow diagrams

Data flow diagrams (DFDs) model how data and information flow through a digital system. In this course you will learn about L0 and L1 DFDs. The DFD shows:

- ▶ where the data and information come from
- ▶ what is input
- ▶ what happens to the data
- ▶ how it is output
- ▶ where the data is stored.

An L0 DFD is sometimes called a context diagram. This level of DFD shows the data system in brief detail. However, the diagram enables a user to get an idea of how data moves through the system.

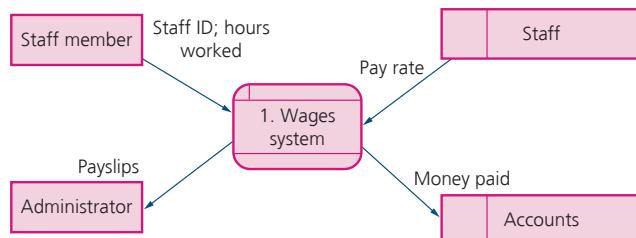
There are four elements in a DFD. There are many different sets of symbols that can be used to create a DFD but the most commonly used set are shown in Table 3.2.

Element	Symbol
External entity	
Process	
Data store	
Flow	

▲ Table 3.2 The symbols commonly used to create a DFD

An **external entity** is a source of data that is input into the system and where the data to be output from the system is sent to. These entities are external to the digital system being shown in the DFD, for example a customer. A **process** is the action that is performed on the data, that is what happens to it. A **data store** is where the data is stored, for example a database table, a CSV file. The data **flows** are just that: they show where and how the data flows around the system.

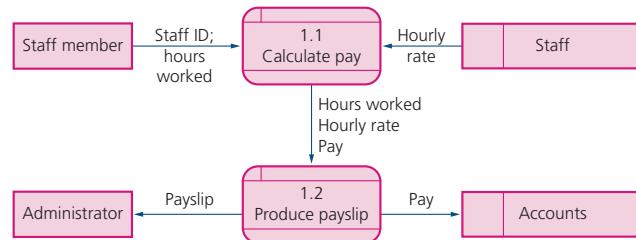
An L1 DFD focuses on a system and provides more detail than the L0 DFD. For example, an L0 DFD for a wages system is shown below.



▲ Figure 3.7 Level 0 DFD

The wages system is shown in the centre of the L0 DFD as a single process. Data stores are shown with the external entities of staff and administrators. Each data flow shows what is being sent through the system at each point.

An L1 DFD can then be created from this L0 DFD. This is shown in the diagram below.



▲ Figure 3.8 Level 1 DFD

Creating DFDs can become complicated so there are some rules that should be followed:

- ▶ There is at least one input or output for each external entity.
- ▶ Data only flows in one direction.
- ▶ Every data flow is labelled.
- ▶ Every data flow connects to at least one process.
- ▶ There is at least one input/output flow for each process.

Activity

Create an L0 and L1 DFD to show the process of selecting and enrolling on a course at your centre.

Test yourself

- 1 How does the hierarchical database model represent a database?
- 2 Identify one relationship shown in an ERD.
- 3 What is an L0 DFD also known as?
- 4 What is the symbol for a data store?
- 5 Identify one rule for creating a DFD.

3.4 The concepts involved in data entry and maintenance

Data entry

Assign common data types to screen input boxes

Data needs to be entered into a digital system. The data entered will probably be through a digital system screen input form. The form will include input boxes which will enable the user to input the data in the correct data type and allow validation to take place.

By assigning data types to input boxes, the chance of invalid data being entered is lowered. This means that the entered data will be in a data type that can be useful to the organisation receiving the data and will allow meaningful processing to take place.

If **numeric** data is to be entered, then the input box can be set to accept data as:

- ▶ integer – whole numbers, positive or negative
- ▶ real/float – any number, with or without decimal places, positive or negative, with up to 6–7 decimal digits
- ▶ double – any number, with or without decimal places, positive or negative, with up to 15 decimal digits.

If **text** data is to be entered, then the input box can be set to accept data as:

- ▶ character – a single character which can be a letter, number or symbol
- ▶ string – a group of characters stored together.

If **Boolean** data is to be entered, then the input box can be set to accept data as:

- ▶ true/false
- ▶ yes/no
- ▶ check box – checked or not checked.
- ▶ Radio button – selected or not selected.

Activity

Create a table to show the different data types that would be used on a data entry screen for a library. For each data type give an example, explaining why the data type has been used.

Discuss your findings with the rest of your teaching group.

Test yourself

- 1 Why should a data type be assigned to an input box?
- 2 Identify one type of integer.
- 3 What is the maximum number of decimal digits in the double numeric data type?
- 4 What is a string?
- 5 Identify one type of Boolean data.

- ▶ sensible
- ▶ in the correct format
- ▶ reasonable
- ▶ within predefined boundaries
- ▶ complete.

The most common input validation techniques are:

- ▶ **Check digit** – a check digit is calculated using a set of numbers and then added to the end of them. When a code is created, the check digit is created and added to the code. Before the code is processed the check digit is recalculated and compared to the one at the end of the code. If they are the same then processing can continue, if not then an error has occurred and the code needs to be rechecked. Check digits are commonly used when data is being transmitted. Corruption can occur during transmission and a check digit can be used to check the data received is the same as that sent. A check digit can identify errors caused by transposition errors: if two numbers were transposed then the check digit check would produce an error. An **International Book Standard Number (ISBN)** number has a check digit at the end, the 11th digit, which is used to check the rest of the ISBN, the other ten digits, is correct.
- ▶ **Format check** – this can also be known as an input mask. Some data to be entered into a digital system might be a combination of letters and numbers. This means that a validation rule can be set to ensure that the data entered meets the required format. This means that the letters and numbers will be in the same place each time data is entered. For example, most postcodes follow the format of LLNN NLL where L is a letter and N is a number. A rule could make sure that the postcode entered has to follow the LLNN NLL format.
- ▶ **Length check** – any data entered into a digital system has a length. For example, 'Hello' has a length of five while a single character has a length

Reducing risk of data entry errors

Data has to be input into a digital system. Sometimes this is done by combining data stores, but data is usually input by a person initially. Every person is capable of making errors during data entry. There are, however, features that can be introduced to reduce the risk and number of data entry errors. Using **verification** and **validation** techniques can reduce data entry errors.

Verification

Verification can be performed when entering data. There are a range of verification methods.

- ▶ **Entering the data twice** – it is very common that data has to be entered twice to check that the second entry matches the first. For example, when choosing a new password, it is usual to enter it twice. This double entry process lets the digital system check that both data entries are identical. It verifies that the first version is correct by matching it against the second version.
- ▶ **Cross-checking** – this is usually carried out manually. The process is a form of proof reading. This means checking the source document against the data that has been entered. This process is not very reliable as it can be very difficult to keep track of the source and destination of the data.

Research

Investigate other verification techniques.

How can each technique you have found decrease the risk of errors on data entry?

Validation

Validation is a check that is run by the digital system as the data is being entered. Validation attempts to prevent the entry of any data that does not meet the predefined rules. The rules will not stop incorrect data being entered but ensure that the data being entered is:

Key terms

Verification: a check to see whether the data being entered into a digital system is identical to the source document or initial data entry.

Validation: checks that the data being entered into a digital system is sensible and reasonable. Checks the data against pre-set rules.

International Book Standard Number (ISBN): a number that uniquely identifies a book. It usually has ten digits with an 11th digit being a check digit.

of one. A length check ensures that the length of the entered data is no longer than a predefined length.

- **Lookup table** – this technique is where the entered data is cross-checked against a list to make sure the data is valid and acceptable. In some cases the cross-referencing may give extra information for the user. For example, a postcode can be checked against a list and if there is more than one property in the postcode then a choice of property addresses is provided. This is a conformation of acceptable data entry. It should be remembered that this type of validation is not a search, it is a comparison against known data.

Validation techniques can be used on an online data entry screen to limit the risk of data entry errors. If an error is made, then a useful message should be provided to the users. The message should provide details about the error and how it can be corrected. It is also common to use colours to help the users. For example, the use of green when everything has been entered correctly and red if an error has been made.

Data entry errors can result in incorrect data being held. This is an example of **GIGO**. This means that as incorrect data is entered, the data stored will also be incorrect. When any processing of this data occurs, the results of the processing will be correct in terms of the data that was processed but will be incorrect in terms of accuracy and usefulness.

Activity

Find a website that includes a data entry screen, for example a retail website. Investigate the validation techniques that have been used and the error messages that are shown when a data entry error has been made.

Discuss with your group how using validation techniques and error message will decrease the impact of data entry errors on the owner of the website.

Most data in industry will be entered through a data entry screen. When a data entry screen is being designed and created it is important that the developer takes the time to clearly understand the needs and requirements. For example, where data needs to be

Key term

GIGO: Garbage In, Garbage Out

in a specified format this must be included in the validation rules set on the data entry screen. By doing this, the time taken to enter the data will decrease as validation techniques, such as presence and type checks, will help users enter the data and also increase the probability that the correct data will be entered first time. When data has been entered and during the life of the data in terms of its usefulness, it will need to be maintained. Data can be maintained at several levels in an organisation. Data can be maintained in other ways. For example, by carrying out searches to remove redundant or expired data. Legislation also requires those storing data to delete data when requested to do so by the data owner.

Research

Research and make notes about situations when data should be maintained and the risks of not maintaining the data. Discuss your findings with the rest of your group.

Test yourself

- 1 What is cross-checking?
- 2 What does validation check the data against?
- 3 What is a check digit?
- 4 What does the presence check do?
- 5 How is most data entered?

Privacy

When data has been entered into a digital system it should be kept private. Data access management and control methods can be used to increase the security and privacy of the data. Keeping data secure and private is also required to comply with standards and legislation related to data.

Data access management is covered in section 3.8, p. 96.

Access control methods are covered in section 3.9, p. 97.

Legislation and standards are covered in Core element 8, Legislation.

Data maintenance

Over the life of the data it will probably need to be edited and maintained. This is to keep the data up to date and to comply with legislation and standards.

There are two main groups that can maintain data – a user and the system administrator.

User

A user will be able to make changes (edits) to data but the data that can be changed will depend on their job role. A data entry screen will be used to carry out any edits required. It is also possible that a user will be able to change their own data if, for example, they are a registered user. At the most basic level, the data that could be edited is:

- ▶ address detail
- ▶ contact numbers
- ▶ communication preferences.

The data entry screen will have permissions (privileges) attached to the fields so only the data where the permissions are granted can be edited and saved.

The digital system administrator

The digital system administrator will control who is able to edit data, including direct edits. The privileges to directly edit data will include:

- ▶ **user level** – specific users can be granted privileges. These are likely to be senior positions within an organisation.
- ▶ **user group level** – groups of users can be granted privileges. For example, all of the HR department will be able to make changes to employees' records.
- ▶ **file level** – specific users or user groups will be able to make edits to a specified file.

Business resource considerations for data entry and maintenance

It is very important that data is entered correctly and maintained over its life. Data that is incorrect is useless to an organisation and can have legal implications.

However, entering and maintaining data takes time and money; these are the operational impacts of entering and maintaining data. Entering and maintaining data will take time, especially if data entry errors are to be reduced, but employees (staff) will be needed to carry out these tasks.

There are also **financial considerations**. For example, digital systems may have to be purchased, installed and maintained. If the data is to be stored in the cloud, then cloud storage space may need to be expanded. In addition, the data entry employees will need to be paid. The data entry and maintenance will need to be included in the budget which is given

to any department in an organisation. The budget is normally set for a tax year. The tax year goes from the beginning of April to the end of March each year. The budget will be set on the previous year's expenditure, estimates of costs (which will be a forecast of how much time will be needed for data entry and maintenance), the cost of employees, possible increased storage space and extra digital devices.

When data is being collected, entered, stored and maintained there may be **technical resource considerations**. This may be, as already discussed, the purchasing of new digital systems, including installing and maintenance. Hardware might also have to be purchased to increase storage capacity if the data is stored on premises or to update the hardware as it becomes obsolete. New versions of software may also have to be purchased and installed. This may be because the software has become legacy, or when new software, which better meets the needs of the organisation, is released by software vendors.

As the amount of data entered and stored by an organisation increases, it is possible that storage capacity has to be increased. This could result in, as already discussed, increased hardware capacity or, if the data is being stored in the cloud, increased cloud storage capacity.

Test yourself

- 1 Why should data be kept secure and private?
- 2 Identify one group that can maintain data.
- 3 What does the digital system administrator control?
- 4 Identify one financial consideration of data storage.
- 5 Why would new software have to be purchased?

3.5 Characteristics of data formats and importance for analysis

Data formats

When data has been entered, it can be stored in different types of formats. The three main format structures are:

- ▶ file-based
- ▶ directory-based
- ▶ relational database systems.

File-based structure

A file-based structure is one where the data is held in one file. This type of structure can be used to maintain and organise single or many data files and can help with basic data management and analysis. A file-based structure facilitates a range of application software packages to carry out functions for end users of the digital system. Each package defines and manages its own data. This means that within each file there is a consistent set of items including attributes, data types and validation with data referenced within the file. This can, however, put limits on how the data can be used or transmitted.

It is important that the system permits concurrent access by different processes. Data stored in a file-based system should be consistently structured and stored so it is accessible.

Directory-based structure

A directory-based structure is one where the data is held across many files, for example a presentation can show data from a spreadsheet or database. This means that the data held in the files has different attributes, data types and validation, but generally each file will have its own attributes, data types and validation. Each file will have its own context, and this is usually the same context as the structure.

A directory-based structure can make it easier for the end user(s) to locate files, as long as the folder structure is logical. In addition, the data can have a relationship across many files. The data required can be extracted from a range of files and across a range of different file types.

The data in a directory-based structure will be stored hierarchically. For example, an HR department may store records of all employees. Each employee will work in a department. Each department could have its own folder, with subfolders for each employee. Within the employee's subfolder will be stored all files relevant to that employee.

The files in a directory structure are usually created by different data owners and may come from different sources.

Relational database systems

A relational database system is one which has been designed using the ERD data modelling tool. The

data is connected by relationships. The relationships reduce duplicate, or redundant, data being stored. Normalisation, primary and foreign keys are used to reduce **data redundancy**.

The ERD data modelling tool is covered in section 3.3, p. 82.

A relational database can be stored on a server and it is possible that a dedicated server may be utilised. The server hosts, delivers and manages the database. As end users (clients) request access to the database, the server facilitates these requests. Searches can be carried out on a relational database. These searches can be carried out using a structured query language (SQL), which is one example of a data processing language. The queries can be hard-coded searches that are frequently needed, or carried out when needed by the end users (clients).

Importance for analysis

By using a specified format, analysis of the data held can become more efficient. This is because data that is in specified formats means queries can become easier to formulate so producing the results required by the end users.

Data can also be updated and shared between end users more efficiently. Files can be saved in the relevant and logical place, for example in a specified directory, folder and file. This helps end users to locate the data they require using, for example, the correct directory and file format. As data can be located efficiently using searches or locating the required file, this can help when drawing conclusions from the data. By using specified formats, end users can be assured that they have located all data relevant to the analysis.

Test yourself

- 1 Identify two consistent items in a file-based structure.
- 2 What is a directory-based structure?
- 3 What data modelling tool is used when creating a relational database?
- 4 Identify two features that can be used to reduce data redundancy.
- 5 What does SQL stand for?

3.6 Methods of presenting and visualising data and their suitability for application

Presenting data

When data has been input, processed and analysed it has to be output, that is presented in a format that is useful to the end users. The main ways data can be presented are explored here.

Reports

Data can be presented in data reports. There are many different types of data reports but in industry most reports will be formal and will present an overview. The data being presented and visualised must be the most relevant, with no errors. Errors could include selection of the incorrect data or incorrect formatting. When creating the data report, essential information should be extracted from the data so that the data report conveys all the information needed to fulfil the specified requirements and needs of the end user. The data presented in the report must be arranged and displayed in an easy-to-read format to enable the end users to easily visualise and understand the data report.

Research

There are many different types of reports that can be used in the digital industry.

Research the different types, and find out when and why each type would be used.

Digital slides

Data can be presented using digital slides. Digital slides are commonly used in presentations to convey a message. The slides can be used on, for example, a website, a video conference or in a face-to-face situation. The slides can be created using a template or predefined organisation house style and can include a range of different components, for example text, images, graphs and links to other resources.

Webinars

Data can be presented using a webinar which can also be referred to as a video conference. A webinar is an online meeting that is hosted by an organisation with the participants viewing the webinar on digital devices over the internet. A webinar allows a host to share presentations, videos, audio, web pages or other multimedia content with the audience. The participants

can interact with the host in real time through, for example, email or instant messaging.

Extended reality

Data can be presented using extended reality (XR). XR is the overarching term used for all types of the immersive presentation of data. This includes virtual reality (VR), augmented reality (AR) and Mixed Reality (MR).

► **VR** – where the user is totally immersed in the virtual world with no sight of the real world. This is facilitated using special VR headsets/glasses that will also block out any sight of the real world. Unlike AR where the user interacts with the augmented real world, with VR the user can only interact with the virtual world.

VR is a popular training tool for the airline industry (training pilots to fly certain types of aircraft) and firefighters (to navigate their way through buildings full of smoke and fire without putting their lives in danger).

► **AR** – a view of the real world with computer-generated input (for example graphics, audio visual or text) superimposed onto it. In essence the AR content augments (enhances or adds to) the real-world scene that is viewed by the user. AR is an immersive visual experience and is commonly used to provide the user with information or guidance, allowing them to visualise things that they may not have access to or be able to imagine under normal circumstances. IKEA, for example, provides an immersive AR experience through their app where a customer can select items such as furniture and ‘place’ them in their home. This is a digital version of “try before you buy”; a customer is able to see the visual impact of the item within their own home surroundings.

AR has also been used in oil and gas exploration to help the engineers to navigate their way through complex equipment to carry out repairs, upgrades and/or solve faults. They can view the piece of equipment through an AR headset and they are provided with instructions and images that they can interact with and work through in order to identify a problem, dismantle the equipment to fit a new part or replace the item altogether.

Because the AR experience is immersive, the user feels part of the activity that is taking place. Firefighters are trained using AR for tackling incidents in dangerous situations, for example on oil refineries.

Video and sound

Data can be presented using video and sound. A video is a set of moving images and can present data in a

visual way. It is often easier to understand if the data is presented visually. Videos can be uploaded to a range of video sharing platforms or embedded into a website. Sound can also be used to provide a commentary on a video presentation by, for example, explaining the data presented in the video. Sound can also be used as an independent element to present data.

Animation

Animation can take the form of effects on digital slides and animated images. Data can be presented in animated form to create models. Animation can be used to create 3D, realistic models that allow diagrams and so on to show accurate representations of an object, for example a new product or a graph.

Visualising data

When the data is being presented to the end users, there are different visualisation methods that can be used. Which method will be used will depend on the type of data and the end user's knowledge. The main visualisation methods are explored here.

Graphs and charts

Graphs and charts are generally used to visualise numerical data. Charts allow data to be visualised in the form of graphs, diagrams or tables. Graphs show the mathematical relationship between sets of data. Graphs are one type of chart; all graphs are charts, but not all charts are graphs. Charts are a large group of methods for visualising information.

A graph/chart will enable the end user to visualise and understand the data more easily than being presented with just numbers. Titles and labels can be used to put the data being shown into context. It is easier to identify trends and patterns using a graph or chart.

There are some disadvantages to using graphs and charts. If the graph or chart being used to present the numbers is poorly presented, the end users can misinterpret the data being shown. It is possible to use incorrect data when creating a graph or chart. By doing this, the data being presented will become useless to the end user.

There are many different types of graphs and charts. Each type has a different purpose and this should be considered when selecting the type of graph or chart to use to present the data.

The most commonly used types of graphs and charts used to visualise data are:

Charts	Graphs
<ul style="list-style-type: none">PieAreaFunnel	<ul style="list-style-type: none">Line graphBar graph/histogram

Research

Research a range of charts and graphs, including the type of data that each can be used for.

Create a communication to present your findings for an audience aged 16 to 19 years old.

Dashboard

A dashboard is a type of graphical user interface (GUI) providing simple visualisation of data related to performance indicators. Dashboards are commonly accessible by a web browser and can show real-time data updates.

Dashboards can be customised to meet the needs of the end users. A dashboard connects to files, emails and application programming interfaces. All the data is shown on the dashboard using, for example, tables, text, graphs and charts. A data dashboard is an efficient method of tracking multiple data sources to provide a single source to monitor the data in real time.

Data tables

Data tables can be useful when the data being presented belongs to the same category, or when a single category of data varies when measured at different points or time. For example, the percentage increase in the use of the train network for different regions of the UK.

To successfully use a data table, the data being presented and visualised must be relatively small. It is very difficult for an end user to interpret or visualise large amounts of data with a table; the table becomes too complex or large. However, unlike graphs and charts, it is possible to use data tables to present very precise data values. It can be difficult to represent precise data on a graph or chart, but a data table can allow the clear presentation of numbers to two, or more, decimal places.

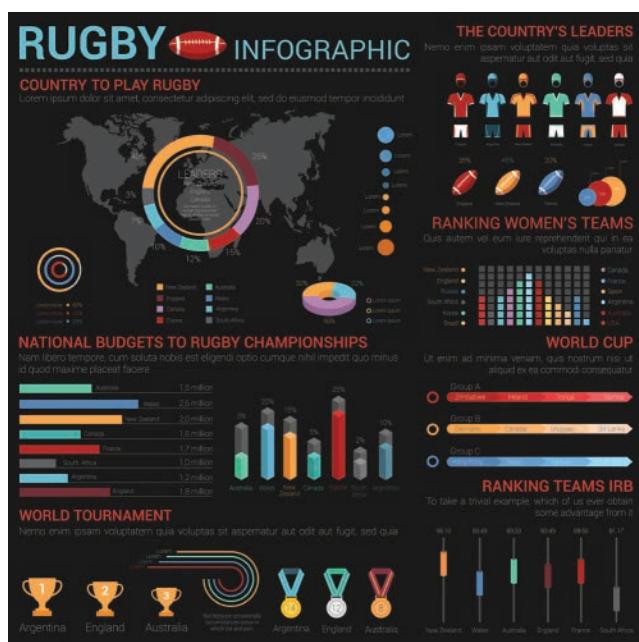
Data tables can be used to visualise data in a clear and easy to read and understand format. They can be used to summarise data. However, the data tables must be clearly labelled, with headings used to indicate what the table is showing. Column headings must also be clear to enable an end user to fully understand the data being presented and visualised.

Infographics

Infographics are, according to the *Oxford English Dictionary*:

'a visual representation of information or data'

An infographic is a collection of images, charts/graphs, with minimal text to provide an easy-to-visualise overview of a topic.



▲ Figure 3.9 An infographic

Where data is to be presented using an infographic, then charts or graphs are most appropriate. Looking at non-visual data can become difficult for the end user to interpret the message of the data. By displaying data in a visual way, the end user can interpret and increase their understanding of the data so increasing effectiveness.

Research

Research data visualisation infographics, finding examples.

Discuss the effectiveness of each example with your teaching group.

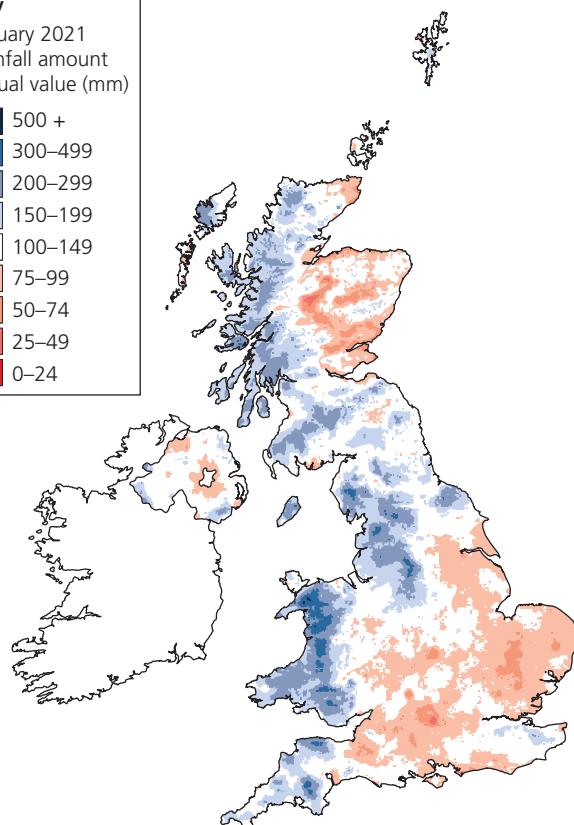
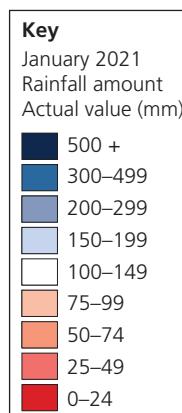
Activity

Create an infographic to show the different methods that can be used to visualise data.

Maps and heat maps

Map visualisation of data is used to display geographical-related data and present this in the form of a map. One type of map is a heat map. A heat map is a graphical representation of data where values are depicted by colour. Heatmaps make it easy to visualise and understand complex data. Heatmaps can be used to show user interaction with a website, for example, where the greatest and least user clicks were.

The most common example of a heat map can be found in weather. A heatmap can be used to show, for example, the amount of rainfall over a given time period. It is usual to use one colour with the greatest number as the darkest shade and the lowest as the lightest shade.



▲ Figure 3.10 Heat map for the amount of rainfall in the UK in January 2021. Contains public sector information licensed under the Open Government Licence v3.0.

During the Covid-19 pandemic of 2020, heat maps were used to show the greatest and lowest number of cases.

Suitability for application

When data has to be presented and visualised by the end users, the audience, there are some factors that should be considered when selecting the presentation and visualisation methods.

Formal or informal?

It is important to consider whether the data is to be presented, visualised and communicated formally or informally.

- **Formal communication** – follows set procedures and is usually part of a job role. The formal communication will be used at meetings, reporting to line managers or as part of a formal feedback process. The language used is also likely to be formal. This means that slang or shortened versions of words should not be used. Any written communication should have correct sentence construction, with correct use of punctuation. The correct technical terminology should also be used. Reports are considered to be a formal method of presenting data.
- **Informal communication** – can occur anywhere. Informal communication is likely to be used at a meeting of peers or for an informal department discussion about a specific topic. It is likely that abbreviations can be used. Written communication should also have correct sentence construction, but minor errors are more acceptable than when communicating formally. Infographics are considered to be an informal method of visualising data.

Meeting requirements

The methods used to present and visualise data should meet any specified requirements provided. These requirements are usually provided in a **brief**. The brief will provide details about the message that needs to be conveyed by the data, for example an analysis of sales over a given time period.

The audience will need to be considered in terms of their **level of technical knowledge and skill**, location (face to face or remote) and the understanding of the data. You should adjust technical language to meet the knowledge and skill set of the audience. If the audience has limited technical knowledge, then you should limit the use of technical terms and abbreviations. You should use simple terminology that conveys the meaning but does not go into too much detail. For example, use the term 'hard drive' for storage location rather than using read/write speed, capacity and type.

The data should be visualised using a method that considers the audience. For example, where data analysis skills are limited then it may be more helpful to use an infographic than data tables. However, you should also consider the data being visualised, and the message to be conveyed, when selecting the method of presentation and visualisation.

Test yourself

- 1 What does a graph represent?
- 2 What is AR?
- 3 What size of data should be considered for data tables?
- 4 How is data represented on a heat map?
- 5 Identify one presentation method that could be used in a formal situation.

3.7 Applications of data within an organisation

Data is an organisation's most valuable asset. It is said that an organisation that does not understand the importance of data is unlikely to succeed.

All organisations need data and information to be able to make informed and correct decisions. Without data and information, decisions cannot be made. An organisation will need to make decisions about a range of areas related to the function of the organisation.

Data is the raw facts and figures, including statistics, that an organisation will collect while carrying out its business function. This data needs to be processed and analysed to enable it to be put into a form which can be informatively used. Data can be **qualitative** or **quantitative**.

Analysis

Organisations use data and information to enable them to complete a range of activities including to carry out analysis and marketing and to assist in operational management.

Key terms

Qualitative data: data that is non-numerical.

Quantitative data: data that is numerical.

Identifying trends and patterns

The analysis of trends and patterns can be carried out using data mining. One of these is market analysis which is defined as:

'a quantitative and qualitative assessment of a market for an organisation'

Data mining is covered in section 12.1, p. 291.

Market trends can vary between sectors. For example, the holiday sector traditionally has an increased market trend in January and February. This is because, historically, people book summer holidays during these months.

The retail sector has an increased market share during October to December when gifts are bought for the various religious festivals such as Hannukkah, Divali and Christmas.

The fashion sector needs to predict trends and patterns in the clothes people will buy in advance. This is because clothes need to be made, shipped into distribution centres and delivered to the shops or put onto websites if the clothes retailer has an online presence.

Some trends can happen very quickly and can be influenced by social media.

An organisation that uses data and information to make decisions about market trends and patterns will be able to respond to these very quickly. This will help the organisation stay competitive and profitable.

Monitoring performance

Data can be used to monitor performance, including:

- ▶ the performance of staff
- ▶ product/service usage.

Workplace monitoring enables an employer to track staff activities and then monitor staff engagement with work-related tasks, including product and service usage. A business using employee monitoring on a digital device can measure productivity, track attendance, ensure security and collect proof of hours worked.

There are several ways in which employees can be monitored and the most common use of monitoring relates to electronic communication. This involves the monitoring of products and services including:

- ▶ computer screens
- ▶ email

- ▶ internet and app use
- ▶ phone use.

The Telecommunications Regulations 2000 allow employers to monitor employees without the employee having given their consent first. Employers must clearly explain the amount of monitoring in the staff handbook or contract. These details may be also included in the Acceptable Use Policy (AUP):

- ▶ if/how they are being monitored
- ▶ if personal emails and calls are not allowed
- ▶ the acceptable number of personal emails and phone calls.

Research

Research the acceptable purposes for monitoring employees as detailed in the Telecommunications Regulations 2000.

There are several reasons an employer may want to monitor staff electronic communications. These include to:

- ▶ detect any criminal activity
- ▶ ensure that staff are following the correct procedures and working to appropriate standards
- ▶ investigate any allegations of misconduct, for example if a member of staff has raised a grievance that they are being harassed
- ▶ see if there has been any mishandling of confidential information
- ▶ see if they are abusing work systems.

Most employers have internet access which employees use as part of their job role. It can be helpful for an employer to monitor the websites accessed during working hours. Internet monitors can be installed to detail which websites are being accessed. For example, if the internet monitor audit log shows details of shopping websites being accessed, it can be assumed that the employees are not focusing on their job roles.

However, there are some job roles which require access to websites such as social media. A business may have a social media manager who, as part of their job role, uses social media such as Facebook, Instagram and Twitter. Accessing and posting to these websites are the main parts of the job role. However, while the monitoring audit logs will show these websites are being accessed, are they being accessed as part of the job role or for personal use?

Websites can also be blocked. Many employers will restrict their employees from visiting websites with inappropriate content, while others may allow websites, like Twitter or YouTube, but only for a limited period of time.

Phone calls can be monitored. When a contact number for a business is dialled, it is quite common to hear an automated message stating:

'This call may be recorded for training, quality assurance and monitoring purposes.'

This message means that the employer is recording all phone calls. This can cause a moral dilemma. If employees are allowed to make and receive personal calls then these too will be recorded.

Recording calls can help with training. If an employee gets constant positive feedback from customers then their calls can be listened to. By doing this, the calls can be used to see why customers provide positive feedback. The calls can also be used to train those employees who are either new or who do not receive as much positive feedback.

Those businesses that are only concerned about the misuse of phones can simply record the numbers dialled and how much time is spent on the calls.

Advantages and disadvantages of monitoring, and monitoring software

There are advantages and disadvantages to the use of monitoring, and monitoring software, in a workplace.

The **advantages** include:

- ▶ Employees can work flexible hours as monitoring can ensure all employees complete their required tasks.
- ▶ The most productive employees can be identified and rewarded by, for example, a promotion or a pay rise.
- ▶ Delivery drivers can be tracked to ensure their safety and that of delivery vehicles and contents.

The **disadvantages** include:

- ▶ Employees can feel that they are not trusted and that the monitoring is an invasion of privacy.
- ▶ Employee morale may reduce due to continual monitoring and lack of trust.
- ▶ Employee stress levels may increase which could lead to an increase in the number of employees off sick.

Reduced digital system performance

Data and information are usually stored on a digital system. It is highly probable that many of employees will use a digital system to help them carry out their

job roles. In addition, an organisation is likely to use a network to enable collaboration and sharing of data and information.

Over time the performance of a system can reduce. This may be as a result of, for example, an increased use of storage devices, conflict between software applications, or software updates.

Other reasons that system performance can reduce include outdated system components or an increased number of users.

Systems can be analysed using a range of software tools which can show where any reduction in performance is happening. Some tools can show hardware system metrics, including:

- ▶ computer processing unit (CPU) and memory utilisation
- ▶ memory and socket interconnect bandwidth
- ▶ cycles per instruction
- ▶ cache miss rates
- ▶ type of instructions executed
- ▶ storage device access.

Other tools can show the software system **metrics** including:

- ▶ response times
- ▶ rate of completion of user requests
- ▶ identification of any bottlenecks.

The results from the analysis of system performance can be shown on a dashboard in graphs and charts. Using graphs and charts will enable trends and patterns in performance to be identified which can then lead to informed decisions relating to the possible upgrade of a digital system.

Research

Investigate the software tools that can be used to provide metrics about hardware and software performance.

Invite a system support technician to provide details about the tools used to monitor system performance in your centre or workplace.

Discuss your findings with the technician and your teaching group.

Key term

Metrics: a set of numbers that gives information about a particular process or activity.

Forecasting

A business can use data to carry out **forecasting**, for example **predictive analysis**. Predictive analysis is a process that facilitates the prediction of what is likely to happen in the future. This can be done by looking for patterns in the data and information already stored. Predictive analysis is part of the wider context of **data analytics** and uses techniques including:

- ▶ machine learning
- ▶ statistics
- ▶ data mining
- ▶ AI.

These techniques are used to create predictive models which can be used to interrogate data to identify patterns, which are then used to predict possible outcomes. Predictive analysis allows a business to use their stored data to **inform decision making** and improve their business.

Marketing

Targeting customers and customer profiles

Having data and information about their customers will enable an organisation to carry out **targeted customer marketing**. These data and information can come from a range of sources. Data may be analysed about specific products bought on a website by a customer, which can lead to an organisation targeting marketing about 'similar but different' products.

For example, if a customer regularly purchases baby food from an organisation then the data would show that there was a high probability that the customer had a baby. The organisation could then send this customer targeted marketing about other baby products. The targeted marketing could be, for example, an email, or recommendations the next time the customer visited a website.

As explored earlier, each time a customer uses a loyalty card, data can be gathered, processed and analysed about them. By collecting this data, **customer profiles** can be created, and the data can be processed and analysed to provide targeted marketing.

Direct marketing promotion

This includes:

- ▶ emails
- ▶ online adverts on websites
- ▶ promotional letters
- ▶ catalogues and flyers
- ▶ newspaper and magazine adverts
- ▶ text messaging
- ▶ phone calls.

The direct marketing must conform to legislative requirements. The results of the direct marketing can be analysed to, for example, define the most successful method in terms of response to it and the sales that have resulted from the direct marketing.

Legislation is covered in Core element 8.

Operational management

Operational management relates to the monitoring and control of the operations that are carried out by an organisation. This includes the setting and monitoring of **key performance indicators (KPIs)**.

Any KPI that is set must be achievable and deliverable. When setting KPIs, the data currently stored by the business should be considered. This will help to follow the steps involved in setting and monitoring KPIs.

- ▶ Review the objectives of the business.
- ▶ Analyse the current performance of the business.
- ▶ Set short- and long-term KPI targets.
- ▶ Review targets.
- ▶ Monitor progress and, where appropriate, revisit the KPIs.

By setting KPIs and reviewing the stored data, an organisation should be able to **improve the service** they provide to customers and stakeholders.

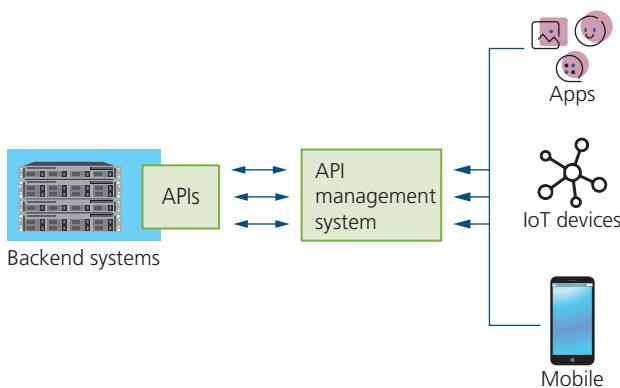
Key terms

Data analytics: the science of analysing raw information to answer specific business questions.

Key performance indicator (KPI): a quantifiable measure used to evaluate the success of an organisation in meeting predefined performance objectives.

Test yourself

- 1 What is qualitative data?
- 2 Identify two reasons an employer may want to monitor staff electronic communications.
- 3 Identify two techniques used in predictive analysis.
- 4 Identify three different direct marketing methods.
- 5 Identify two steps in the process of setting KPIs.



3.8 Types of data access management

Data is a very valuable asset to organisations and individuals but also cyber attackers. It is, therefore, very important to manage access to data very carefully.

User access controls

User access controls should be implemented to attempt to reduce the risk to data. The controls that can be implemented include:

- ▶ physical access
- ▶ remote access
- ▶ permissions
- ▶ authentication.

User access controls and restrictions are covered in section 10.6, p. 254.

Application programming interface

An **application programming interface (API)** is the interface that enables two or more different software applications to communicate. Each time a user sends a request or accesses a web page or app, a remote API is used. Remote APIs can interact through a communications network with the resources, for example a web page is outside the computer making the request.

An API allows applications to access data and interact with other applications or systems, by sending and receiving requests. To send and receive the requests the API uses **JSON**.

Key term

JSON: JavaScript Object Notation.

▲ Figure 3.11 APIs

The majority of APIs are designed using web standards. Remember: not all remote APIs are web APIs, but all web APIs are remote.

An API will ensure that authorised users can access and manage data but, to maintain the integrity of the data, the API must be maintained to ensure the highest level of security. It is also important that the certification of the API is appropriate. The certification should be set to the level which is appropriate to the data being accessed. This means that most API certification should be set to partner or private certification and not public.

- ▶ The **private** certification means that the API is only used internally within the business or organisation. This is the most secure certification as the assets can only be accessed within the internal network.
- ▶ The **partner** certification means that the API is only available to trusted partners of the business or organisation. This certification is secure as long as the partners can be trusted and have a high level of security on their own systems.
- ▶ The **public** certification is the least secure. The public certification means that the API is available to everyone. For example, third parties can develop apps that can interact with the API. This means that security risks on the app could, through the interaction, have access to the assets.

Activity

Apply the three different API certifications to the data and information held in your centre. Consider the data and information held about the staff, students, course information and the website.

Create a digital communication describing your findings and suggest any possible improvements. Discuss your findings with the rest of your group.

Uses of APIs

An API enables users to manage, access and use data across a range of platforms. The main advantage of using an API is that users do not have to create accounts for multiple websites. Accessing a website through an API means that only an account for the API needs to be created. This means that users can access a range of websites, and data, using their log-in credentials for the API. An API sends a user's action (request) to a digital system. The digital system sends a response back to the user.

For example, a user adds a product to their shopping basket. The API will tell the website that a product has been added to the basket and the website puts the product into the user's virtual basket. The basket is then updated.

Another example is a user checking the motorway network for delays on their journey. The API enables the user's digital device to send a request to the remote server that stores the web page. This server then links to the server the data is stored on. When the data is received it is processed by the original server and returned to the user.

An advantage of using an API to enable authorised users to access data, is to allow the organisation to make changes to the backend systems, usually a DBMS. This will have no impact on the authorised users as long as the basic structure and behaviour of the API does not change.

APIs are most commonly used in the financial services sector, **CRM** and online retailers.

APIs and vulnerability

Over time, APIs can become insecure. This can lead to vulnerability that can be exploited by risks and threats. Most data is interconnected as websites, apps and software programs interact. If one API is insecure this vulnerability can lead to a higher risk of threat to everything that this API interacts with.

Test yourself

- 1 Describe one advantage of using an API.
- 2 What does an API use to send and receive requests?
- 3 Identify three ways an API can be accessed.
- 4 Which API certification should not be used to maximise the security of data?
- 5 Identify two sectors that use APIs.

Key term

CRM: customer relationship management.

3.9 Types and application of access control methods

Data and information are very valuable assets to an organisation. The method that is used to control access to data should be carefully considered. There are four main types of access control methods.

Role-based access control

Role-based access control (RBAC) is a type of access control that restricts or permits access to resources, including software and data, based on the role of a user. This method can be used to form relationships between a user's needs and their roles and responsibilities. The needs of the users are grouped into roles which are based on common responsibilities. A user can then have one or more roles based on their needs and responsibilities. The permissions are then based on the role(s). This means that a user does not have to be allocated access individually but based on their role. Access to resources can be easily changed if an employee leaves, starts or changes job role. The role is the only thing that needs to be changed as this will automatically change the permissions.

For example, the data managed by the HR department will have access based on the roles. The Head of HR will have a role, and associated permissions, to access and edit all employee records. A junior member of the HR department may only have permission to access and edit data in employee records that relates to the updating of personal contact details. All employees will have access rights to view their own employee record but not make any edits.

Attribute-based access control

Attribute-based access control (ABAC) is a type of access control that restricts or permits access to resources, software and data, based on attributes or characteristics. ABAC builds on the roles as defined with RBAC. There are four types of attributes that

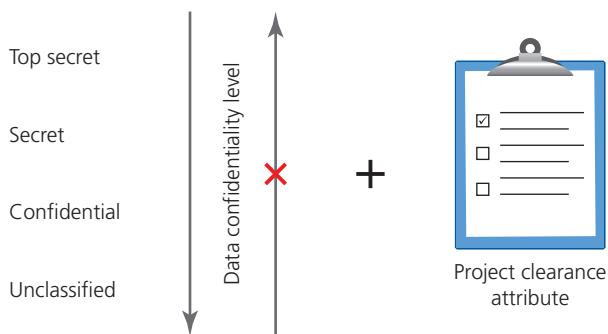
can be considered when creating an ABAC system. These are:

- ▶ **User attributes** – describe the person trying to access the resources, software and data. Examples of user attributes include system username, ID number, job title/role and department they work in.
- ▶ **Resource/object attributes** – describe the resources, software and data being accessed.
- ▶ **Action attributes** – describe what the user will do with the resource, software and data. Examples of action attributes include view, read, transfer, delete and edit.
- ▶ **Environmental attributes** – describe the context of the access attempt. Examples of environmental attributes include day, time, location and device.

For example, the HR manager will always have access to all employee records. This could be unrestricted access based on defined user, resource and environmental attributes, with all possible action attributes permissible.

Mandatory access control

Mandatory access control (MAC) is a type of access control that restricts or permits access based on a hierarchy of security levels. This means that all resources, software and data are given a security category. MAC is perceived to be the most secure of the access control methods. For example, the lowest security level could be ‘unclassified’ with the highest level ‘top secret’. Each resource, software and file is allocated a level of security category. The users and devices are also given a security category. When a user attempts to access a resource, software or file, their security category is checked. If their security category is equal to or above the security category of the resource, software or file, then access is granted.

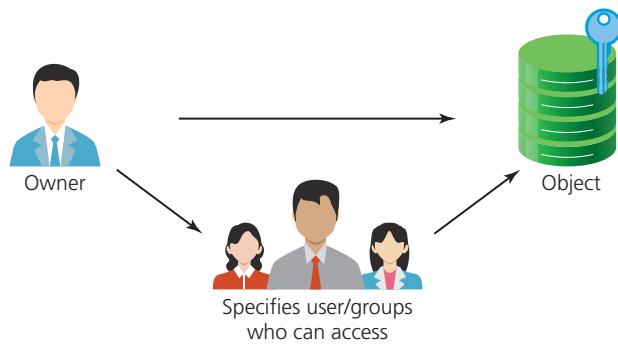


▲ Figure 3.12 MAC

For example, the resources, software and files for the HR department will be allocated a security category. The HR manager will have the highest user security category and will be able to access all employee records. A junior member of the HR department will have a lower security category and so it is unlikely they will be able to access everything the HR manager is permitted to access.

Discretionary access control

Discretionary access control (DAC) is a type of access control that restricts or permits access on permissions granted by the owner of the resource or data. DAC is easy to implement and maintain as the owners have control over the resources, software and data. The owner can grant or define access permissions to the resource or data for a specific user or a group of users. The permissions are stored in an access control log (ACL) which is either automatically created when access permissions are granted, or manually created by the system administrator. The ACL contains the details of the specific user or groups of users and the associated access levels.



▲ Figure 3.13 DAC

For example, the HR manager will determine access control to the resources, software and files for the HR department.

Research

Research each access control method.

Create a digital communication providing details of each access control method, including an explanation, the advantages, disadvantages and examples of use.

The communication will be used by a non-technical director of a medium-sized organisation. You should use a range of data types in your communication.

Test yourself

- 1 What does RBAC stand for?
- 2 Identify one attribute used in the ABAC method.
- 3 What does MAC use to determine access to resources, software and files?
- 4 Which is the most secure access control method?
- 5 Where are permissions stored in the DAC method?

Project practice

A retailer with a physical presence is considering moving to an online presence. The retailer sells sports clothing and equipment. They are hoping that by moving to an online presence they will increase their customer base to worldwide. The retailer is considering carrying out analysis of pre-existing data sets to evaluate the feasibility of the move.

At the moment stock records are kept on a spreadsheet on a stand-alone digital device. The stock records are manually updated twice a week, with stock orders being completed once a week.

The retailer has been informed that to have a successful online presence, stock levels need to be updated automatically to ensure that customers are advised if an item they want to buy is out of stock. Customers should also be advised of when items will be back in stock. The retailer has also been recommended to require customers to register to use

the online presence, providing their name, contact details and any default settings such as a 'leave in a safe place'.

You have been asked to:

- ▶ Create a logical modelling entity relationship diagram for the stock levels and reordering process.
- ▶ Create an online form for the customers to use when registering, showing the data types applied to each field and validation routines.
- ▶ Select and justify the on-premises methods of storing the customer registration data.
- ▶ Explain how charts and graphs could be used by the retailer.
- ▶ Explain to the retailer how targeted marketing can be carried out using customer registration details.
- ▶ Select and justify two different user access controls that could be used to maintain the security of the customer and supplier data.

Assessment practice

- 1 Identify and describe two different data types.
- 2 Discuss the benefits of using NAS to store data and information.
- 3 Compare object and block cloud storage.
- 4 Identify two types of validation, explaining how each can reduce data entry errors.
- 5 Identify and describe two elements of an L1 DFD.
- 6 Discuss the business resource considerations for data entry and maintenance.
- 7 Explain the term 'augmented reality'.
- 8 Explain two advantages of presenting data in an infographic.
- 9 Explain how an API can be used to access data across a range of applications.
- 10 Compare role-based access control and attribute-based access control.

Core element 4: Digital analysis



Digital analysis and problem solving are used to analyse and solve problems. This will lead to solutions which can then be developed into code for digital systems. Computational thinking, which you are going to explore in this core element, provides a framework for the ways in which a problem can be solved.

You will learn about the different characteristics of algorithms and how these should be considered when creating an algorithm to solve a problem.

There are different tools that can be used to create algorithms including decomposition diagrams, flowcharts and pseudocode. You will learn how each tool can be used to create algorithms. You will also learn about the different representations of each algorithmic method and how to use them to create an algorithm that accurately represents a problem.

It is very important that algorithms are correct, solve the problem and produce the correct, and expected, output. You will learn how a visual check and trace tables can be used to ensure that the created algorithm is fit for purpose, providing a clear and robust design to inform the coding of the solution to the problem.

Learning outcomes

In this core element you will learn about:

- 4.1** The characteristics and applications of algorithms in digital analysis

- 4.2** The process of computational thinking and tools applied in problem solving and algorithm design

4.1 The characteristics and applications of algorithms in digital analysis

Algorithms

An algorithm is defined as **a plan, or a well-defined set of step-by-step instructions, to solve a problem.**

Algorithms are the basis on which all software is created. An algorithm is language independent. This means that step-by-step instructions can be implemented with the expected output being the same.

The purpose of an algorithm is to:

- ▶ automate calculations
- ▶ process computational actions
- ▶ support problem solving.

An algorithm must:

- ▶ be clear, with clearly defined steps
- ▶ have clearly defined inputs and outputs
- ▶ be simple, generic and practical
- ▶ be language independent.

The **advantages** of algorithms:

- ▶ They are easy to understand by anyone.
- ▶ They are a step-by-step representation of a solution to a given problem.
- ▶ The initial problem is broken down into steps, which means it is easier to convert into code.

The **disadvantages** of algorithms:

- ▶ Creating a complete algorithm can be time-consuming.
- ▶ Some constructs can be difficult to represent.

An algorithm can be represented as a decomposition diagram, flowchart or pseudocode. These are covered in section 4.2, p. 109.

Characteristics of algorithms

Algorithms have a range of characteristics. These should be considered when an algorithm is being created for any given problem. The characteristics of algorithms are outlined here.

Finiteness

The algorithm should solve the problem in a given number of steps. It is not possible for an algorithm to have an infinite number of steps as this means the algorithm will never solve the problem. The algorithm should also end after a finite number of steps.

Unambiguous

The steps shown in the algorithm must be clear and precise, with the steps clearly defined. The input(s) and output(s) connected with each step should also be clear and only have one meaning. Each user of the algorithm should view and understand the algorithm in the same way.

Inputs and outputs

The inputs used and outputs produced by an algorithm should be clearly defined. Each algorithm should have 0 or more inputs and at least 1 output. The input(s) should be well defined and clear, with the output(s) meeting the defined purpose of the algorithm.

Logical sequencing of steps

The steps in the algorithm should follow a logical sequence to solve the problem. This means that the steps should flow on step by step with no 'jumping' back. The algorithm should solve the problem logically.

Iteration

The algorithm should use discrete steps. That means that each step is carried out based on the previous step. These steps should be repeated (iteration) until the required output is produced. However, the iteration must have a finite number of steps.

Selection

Any input into the algorithm should lead to a specified step(s). The input could be used in a range of steps if decisions have to be made. Each input should relate to a choice of step(s).

Independent

An algorithm should have step-by-step directions, which should be independent of any programming code. This means that the algorithm should be able to be implemented in any programming code.

Feasibility

The algorithm should be able to be implemented with the specified and defined resources. This means that the algorithm should provide a feasible solution to the problem.

Structured English

Algorithms can be written in structured English. Structured English allows users with no programming knowledge to understand the algorithm. Structured English lies between the English language and a

programming language. There are many different examples of structured English but most, if not all, include indentation and programming keywords.

Research

Investigate the different types of structured English.
What are the differences and similarities between them?

Activity

Using one of the structured English types you have found, create an algorithm to output the average of five numbers to be input by a user.

Applications of algorithms for digital analysis

Algorithms can be used in many different situations for digital analysis. What is important is that the algorithm conforms to the characteristics and solves the problem.

The most common applications of algorithms in digital analysis are to:

- ▶ automate calculations to improve efficiency of a process
- ▶ design a step-by-step solution to solve a problem
- ▶ support machine learning for data analysis.

Activity

Select one emerging technology, for example self-driving cars. Investigate how algorithms can be used to support machine learning in the emerging technology.

Create a digital communication to explain your findings to 16–19 year olds.

Test yourself

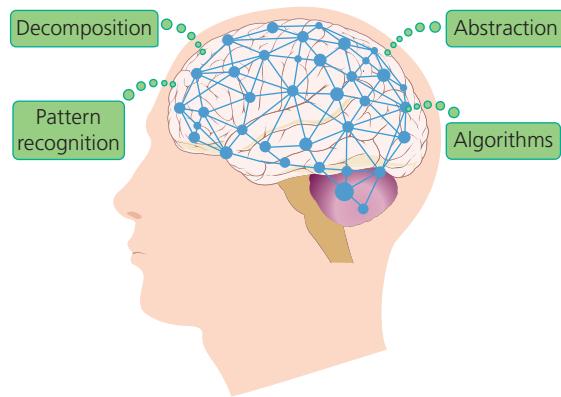
- 1 What is an algorithm?
- 2 Identify one advantage and one disadvantage of using an algorithm.
- 3 Identify two ways algorithms can be represented.
- 4 What is meant by language independent?
- 5 Identify one application of algorithms.

4.2 The process of computational thinking and tools applied in problem solving and algorithm design

Process of computational thinking

There are four techniques, also known as pillars, that can be utilised as part of computational thinking. These are:

- ▶ decomposition
- ▶ pattern recognition
- ▶ abstraction
- ▶ algorithms.



▲ Figure 4.1 The four techniques, or pillars, of computational thinking

Decomposition

Decomposition is one of the techniques involved in the process of computational thinking.

Decomposing a problem is the technique of breaking a complex problem or system into smaller, more manageable, separate parts or stages. These can also be called modules when the solution is being created. Decomposition helps to clarify the stages required to complete a task. It also provides information on how the parts link to and are dependent on another.

Once a problem has been broken down, the separate parts can be understood separately. This also means that the parts can then be solved and developed separately to solve the initial problem. Each part can also be evaluated, or tested, when a program has

Key term

Decomposition: breaking a complex problem into smaller sub-problems.

been developed. Using decomposition makes complex problems easier to solve, and large digital systems easier to design and create.

Solving a complex problem as a whole may seem very difficult. However, the solution to each decomposed part may be much simpler. When all the parts are solved, these solutions can be put together. This will provide a solution to the initial problem.

Decomposing problems is a skill that is needed in many different job roles including project management and software design. When a project is being planned, the initial project is broken down into many different sub-tasks which have to be completed to complete the project.

Activity

You have been asked to plan a trip to Bletchley Park for your teaching group. Split into smaller groups of three or four. Plan the trip and create a digital communication to show all the tasks and sub-tasks which would be needed.

Each group should present their plan.

For each plan, think about:

- ▶ was everything included to make the trip a success?
- ▶ any tasks or sub-tasks that were forgotten, considering the impact these omissions would have on the trip.

The top-down approach to problem solving uses decomposition. This is because the initial problem is broken down until no more decomposition can be carried out. When decomposition is complete, each sub-problem should be at the same level of detail and able to be solved on its own. The sub-problems, or modules, are then combined to solve the initial problem.

Top-down approach

The top-down approach is a technique used to solve problems where the problem is broken down into smaller and smaller problems, modules, until an easily solved problem is defined.

This means that the top-down approach divides a complex problem into multiple smaller parts which can then be used to code the associated modules when creating code. Each module is decomposed until the final module(s) cannot be further decomposed. This approach uses a stepwise process to break a large problem into simpler and smaller problems, modules, to organise and code the software program in an

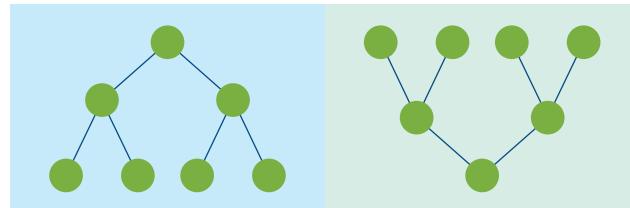
effective and efficient way. The flow of control in this approach is always in the downward direction.

The top-down approach is usually represented as a tree structure, as shown in Figure 4.2.

Each level in the top-down approach shows a different level of detail (**abstraction**) with the top level, level 1, showing the greatest level of abstraction. Using the top-down approach, it is possible to break a problem into detailed sub-problems. The top-down approach begins with the abstract problem and refines the problem by decomposition until no more decomposition can be carried out.

Key term

Abstraction: The filtering out of details that are not needed to complete a task.



▲ Figure 4.2 A top-down approach (left) and a bottom-up approach (right)

Bottom-up approach

The bottom-up approach is the opposite of the top-down one (Figure 4.2). The process starts with the smallest part, module, of the problem. These are then combined to move up a level and this then carries on until the complete problem is solved. The combination of the modules is called integration.

Table 4.1 shows the main differences between the top-down and bottom-up approaches.

Modularisation approach

The modularisation approach aims to break a problem into different components, or modules. One definition of modularisation is:

'The degree to which a system's components may be separated and recombined.'

Most problems are not one big problem but are a collection of different tasks, modules, which can be separated and independent. A big problem can seem daunting but by breaking it into smaller tasks, modules, the problem can become more manageable and solvable.

	Top-down	Bottom-up
Concept	Splitting (Breaks the massive problem into smaller subproblems)	Merging (Solves the fundamental low-level problems and integrates them into a larger one)
Redundancy	Contains redundant information	Redundancy can be eliminated
Programming languages	Structure/procedural oriented programming languages (e.g. C)	Object-oriented programming languages (e.g. Python, Java)
Main use	Module documentation, test case creation, code implementation and debugging	Testing

▲ **Table 4.1** Features of top-down and bottom-up approaches to problem solving

All these modules work together in some way to provide a solution to the initial problem. A module can be seen as a subprogram where the main program ‘calls’ each module. This is a strategy often utilised in an object-orientated programming language.

Activity

Split into three groups. Each group should choose a different problem-solving approach:

- ▶ top-down
- ▶ bottom-up
- ▶ modularisation.

You want to make a cooked dessert as a treat for your family. Using your group’s approach, produce a document showing the steps that should be taken.

Each group should then present their solution.

- ▶ maintenance of the final software solution can be completed at modular level.

The **disadvantages** of using decomposition to analyse, plan and create a digital solution include:

- ▶ the sub-problems, modules, may not combine to solve the initial problem
- ▶ if the initial problem is not fully understood, then it can be difficult to decompose.

The four steps of decomposition

When decomposing a problem ready for coding there are four steps that should be carried out:

- 1 **Identify and describe the problems and processes** – the problems should be identified and described. It is important that at this stage the technical terms used should match the sector the problem relates to. For example, if the problem relates to the retail sector then terms related to the retail sector should be used.
- 2 **Break down the problems into separate tasks** – this stage begins to decompose the problem. It is usual to use the top-down approach as the problem is known. There is no limit on the number of tasks and sub-tasks that should be used. What is important is that the problem is decomposed until it can be decomposed no further. It is also important that the final decomposition should only include tasks and sub-tasks that fully relate to the initial problem.
- 3 **Describe the tasks and sub-tasks** – this stage requires documentation to be created that relates to the decomposition. The documentation produced should be clear and concise to enable a third party to implement the solution to the problem.
- 4 **Communicate** – most software solutions are coded by a team of people. When a problem has been decomposed it is possible that each person will take responsibility for coding a specified task or sub-tasks, modules. When the modules have been

Test yourself

- 1 What is computational thinking?
- 2 How is the top-down approach usually represented?
- 3 What does the top-down approach begin with?
- 4 What type of programming languages use the bottom-up approach?
- 5 What is the combination of modules called?
- 6 What is the aim of the modularisation approach?

Advantages and disadvantages of decomposition

The **advantages** of using decomposition to analyse, plan and create a digital solution include:

- ▶ different people can work on the different sub-tasks, modules, which can then be integrated to make the final solution

coded then they can be bolted together to provide a solution to the given problem.

Test yourself

- 1 What is decomposition?
- 2 What are modules?
- 3 How does the top-down approach use decomposition?
- 4 Identify one advantage and one disadvantage of decomposition.

Pattern recognition

When a problem has been decomposed into the smallest sub-problems, it is often possible to identify patterns. Patterns can be found everywhere. For example, every school and college has a timetable showing lessons, teachers, rooms, days and times. This is an example of a pattern. This is because the timetable runs for an academic year and does not change over the year.

Research

Investigate the artist M.C. Escher.

How does the artist use patterns in their work?

The identification and recognition of patterns – things that are common between problems or programs – is one of the pillars of computational thinking. Patterns can help to solve complex problems more efficiently.

There are patterns that are used in many situations. For example, Morse Code was used during World War 2 for communication between ships.

Activity

Binary uses a pattern of 1's and 0's to represent each letter of the alphabet. Find the patterns that are used in binary to represent each letter. Write a phrase in binary. Share your phrase with your group to decipher it.

During World War 2 work was done by Polish codebreakers, which was then shared with and continued in the UK. Code breakers at Bletchley Park, including Alan Turing, deciphered German coded messages which had been ciphered by the Enigma

Machine. The Enigma Machine used different ciphers to convert each message into code. Each cipher used had a pattern and it was the recognition of these patterns that provided the initial breakthrough when identifying the cipher used for each message.

Activity

Research the Enigma Machine and how the cipher was cracked by Alan Turing and the team at Bletchley Park.

Create a digital communication to present the results of your research.

Key term

Facial recognition software: software that can identify or confirm someone's identity using their face in a photo, video or in real time.

Pattern recognition can also be used in a range of emerging technology applications. For example, **facial recognition software**, voice recognition software and automated transport. These applications use predefined and pre-learned patterns to process the inputs and produce outputs.

Research

Select an emerging technology application. Investigate how the application uses patterns and the advantages and disadvantages.

Discuss your findings with the rest of your teaching group.

By identifying and recognising patterns, it is possible when coding to locate a pre-existing module of code.

There are five main steps to identifying and recognising patterns.

- 1 **Identifying and interpreting common elements in problems or systems** – when a common pattern has been identified, there is more than likely going to be an existing solution to the problem. For example, a search can be carried out for a specific customer in a customer database. The process of searching a database varies slightly depending on the type of database, the number of records or the purpose of the database.

- 2 Identifying and interpreting common differences in problems or systems** – using the customer database example, all customer databases store records of customers. What information is held about the customers and how the information is recorded may be different, but the purpose of the databases is the same – to store information about customers.
- 3 Identifying individual elements in the patterns** – the elements can be input, processed or output. For example, the customer database may record the number of times a customer has placed an order. These orders may be recorded as a number or by recording the date each order was placed. The inputs are different but the process of calculating the number of times is the same.
- 4 Describing patterns that have been identified** – when a pattern has been identified, then it needs to be described. The pattern may be one that occurs several times or a new one.
- 5 Making predictions based on identified patterns** – when a pattern has been identified then a decision can be made about using it multiple times in code or reusing it in a different program.

When the patterns have been identified, it is usually only the specific details that need to be changed within any module of code.

Test yourself

- 1 What is pattern recognition?
- 2 How does Morse Code use pattern recognition?
- 3 What would be the result of not identifying patterns when starting to code?
- 4 How do emerging technology applications use pattern recognition?
- 5 Identify and describe one step used in identifying and recognising patterns.

Abstraction

Abstraction is the process of removing or filtering characteristics that are not needed to be able to focus on essential characteristics.

A well-known example of abstraction is the London Underground map.

By looking at the map, it is possible to plan a journey, know how many stations will be visited and if changes of line need to be made and where. It is not necessary



▲ **Figure 4.3** The London Underground map is an iconic visual representation used by millions of people to plan their journeys

to know how many miles the journey will take or where each station is in relation to the next – these have been filtered out of the map during the process of abstraction.

By carrying out abstraction it enables a general idea of what a problem is and how it can be solved. The process removes specific detail and patterns that do not help you to solve the problem. If abstraction is not carried out, then it is possible that an incorrect solution to the problem may be provided.

Abstraction provides a general idea of the problem rather than focusing on specific details. This general idea is known as a model. By carrying out abstraction the complexity can be reduced while the efficiency can be increased.

Table 4.2 shows the difference between specific and general detail, using the example of making a casserole.

General	Specific for the program
A casserole needs ingredients.	It is not required to know what ingredients.
Each ingredient has a required quantity.	It is not required to know the quantity of each ingredient.
A casserole needs to be cooked for a long time.	It is not required to know the time required.

▲ **Table 4.2** General versus specific

Activity

Complete a table showing specific and general details for driving a car. Compare your results with the rest of your teaching group.

Creating layers of abstraction

Each layer of abstraction hides the complexity of the layer below. This means that the top abstraction layer hides all the complexity of the problem. There are two main steps involved in abstraction.

- 1 The information needed to solve a given problem needs to be identified.** Without this, the solution may not solve the problem. It is also important to know and understand why this information is needed. The required format of the information should also be considered.
- 2 Carry out abstraction to filter out the unrequired information.** This means that only the information required will be considered. Anything else will be a distraction to the process. It is also important to know and understand why information is required and not required.

Each layer of abstraction needs to be complete. This means that each layer should show:

- ▶ **the inputs** – what the user will input into the digital system at that level. This could include validation, and the format of the input, for example currency shown to two decimal places
- ▶ **the outputs** – how and in what format the output will be given. For example, a printed document showing specified data and information or on-screen output. This is usually specified by the client
- ▶ **variables** – these are values that will change. Variables usually change as a result of an input by an end user or of a calculation being carried out
- ▶ **constants** – these are values that do not change. A constant could be, for example, a fixed delivery price
- ▶ **key processes** – these are the actions/processes that the layer must carry out
- ▶ **repeated processes** – these are processes that are carried out several times in a digital system.

Activity

Create the lowest abstraction level for a digital system that can be used to calculate the costs of a school prom, including inputs, outputs, variables and constants. The output of the system should be the cost of a ticket to the prom and how much profit would be made.

Test yourself

- 1 Why is abstraction important?
- 2 What is the aim of abstraction?
- 3 What happens to efficiency when abstraction is carried out?
- 4 Identify one step carried out in the process of abstraction.

Algorithms and actions

The final pillar of computational thinking is algorithms. It is very important that algorithms are correct, solve the problem and produce the correct, and expected, output. You will learn how a visual check and trace table can be used to ensure that the created algorithm is fit for purpose and, when combined with the other pillars of computational thinking, provides a clear and robust design to inform the coding of the solution to the problem.

The actions that can be taken in algorithms include:

Sequence

The order of the processes (tasks) in the algorithm is very important. During the process of decomposition tasks are broken down into small manageable tasks that link together in order – the **sequence**. If the sequence of the algorithm is wrong, then the output may not be that required.

For example, if the algorithm is to find the average of five numbers input by a user, the sequence would be to input and add each number and when five have been input, the total of the five numbers is divided by 5. A sequence different to this would not elicit the average of the five numbers.

Activity

Create an algorithm to draw a rectangle, 15 cm by 10 cm.

Selection

Many algorithms need to take different actions based on the answer to a question or a decision. The question or decision will have two or more options – routes through the algorithm. The route to be taken will depend on the answer to the question or decision. The route will only be followed when the answer to the question or decision dictates. The route will have a set of steps with those not on the route ignored. By using

selection more than one route through an algorithm, and eventually the program, will be possible. If selection and the associated routes are not included in an algorithm, then the algorithm is unlikely to meet the specified needs and outputs.

For example, if the weather is raining, then an umbrella is needed, else take a jacket.

Iteration

Many algorithms carry out tasks until a condition is met or the steps have been repeated a specified number of times. This is **iteration**. There are two types of iteration: count-controlled and condition-controlled.

Key terms

Sequence: the specific order in which instructions are performed in an algorithm.

Selection: a decision or question.

Iteration: repeating steps, or instructions, over and over again until a condition is met.

For example, calculating the average of five user input numbers has iteration until five numbers have been input. This is count-controlled iteration. Adding the user input numbers until the total is over 150 is condition-controlled iteration.

Complex algorithms may have hundreds, if not thousands, of steps. It is critical to make sure all steps in the algorithm are in the correct sequence before programming begins. Once programmed, trying to find an error can be extremely difficult.

Each algorithm will have a purpose – the problem to be solved. There are a number of methods that can be used to ascertain the purpose of an algorithm. If the algorithm is simple, then it can be straightforward to determine if the purpose has been achieved. But if the algorithm is more complicated, then a **trace table** can be used. A trace table is a tool that can be used to dry run the algorithm.

Dry running an algorithm means to use values for the **variables** used in an algorithm and to trace, or run, the processing before beginning to code.

A trace table can allow the values assigned to the variables to be recorded.

The simple pseudocode algorithm shown below shows the multiplication of a user input up to its seventh value. NUM represents the user input to be multiplied up to the seventh value.

NUM = User Input

For number = 1 TO 7

Output NUM * number

END FOR

Key terms

Trace table: a tool used to test or dry run algorithms to make sure no logical errors occur while calculations are being processed. Each column represents a variable and the rows represent the numerical input and the output of the variable.

Variable: a value that will change usually as a result of an input or of a calculation being carried out.

The user inputs a value of 8 for NUM. The trace table shows the values that would be output by the algorithm.

NUM	number	Output
8	1	8
	2	16
	3	24
	4	32
	5	40
	6	48
	7	56

By using a trace table, it can be confirmed that the logic and processing in the algorithm is correct.

A visual check can also be used to determine the purpose of the algorithm. Looking at the simple pseudocode above it is clear that this solves a maths problem, and that multiplication is involved. This is shown by the use of the * operator and the loop that shows how many numbers should be output before the code stops.

Test yourself

- 1 What is the purpose of an algorithm?
- 2 Define the term 'sequence'.
- 3 What are the two types of iteration?
- 4 What is the purpose of a trace table?
- 5 What is a variable?

Tools for problem solving and algorithm design

There are different tools that can be used to create algorithms. Here you will learn about how decomposition diagrams, flowcharts and pseudocode can be used to create algorithms.

Each algorithmic method has a different representation method. There are, for example, a set of symbols that are used when creating a flowchart.

Decomposition diagram

A decomposition diagram shows the tasks in the simplest form and how they link together. This type of diagram is created as a result of the decomposition pillar of computation thinking. The structure of the decomposition diagram will depend on whether top-down or bottom-up decomposition has been used.

Decomposition diagrams were covered in section 4.2, p. 109.

Activity

Create a decomposition diagram to check for a fault on a digital system screen.

Compare your diagram with diagrams created by the rest of your group.

Pseudocode

There are many different ways to write **pseudocode**. Pseudocode is an informal programming description showing the flow through the process. Pseudocode is written in a format that is similar to the structure of a high-level programming language. The purpose of pseudocode is to enable the logic, including the sequence, selection and iteration of the pseudocode, to be the main focus. Pseudocode provides an outline of what the resulting program should achieve.

Pseudocode has its own syntax, some of which is very similar to many actual programming languages. Pseudocode algorithms will not run unless they are converted into an actual programming language.

The **advantages** of using pseudocode include:

- ▶ the pseudocode can be converted into programming code with minor changes to the syntax of the programming language
- ▶ it can be easy to follow and understand even if errors are present in the pseudocode

- ▶ unlike using a flowchart, changes can be implemented quickly
- ▶ it can act as a link between the algorithm and the final program
- ▶ the pseudocode explains the purpose of each line of code, so if the pseudocode is fully complete and detailed, the creation of the final code should be uneventful and meet the needs of the client.

The **disadvantages** of using pseudocode include:

- ▶ it can be as time-consuming to write clear and well-structured pseudocode as it is to write the final programming code
- ▶ it can be difficult to see the logical flow of the program.

There are keywords, which are normally shown in capital letters, that can be used in pseudocode.

- ▶ To show the beginning and end – START/BEGIN and STOP/END
- ▶ For user input – INPUT, READ, GET
- ▶ To display a message or results – PRINT, DISPLAY, or WRITE

Activity

Create pseudocode to meet the following requirements.

A retailer is having a sale. Items are discounted based on the original selling price. The table shows the original price and the discount.

Lowest selling price £	Highest selling price £	Discount %
1.00	4.99	5
5.00	9.99	10
10.00	19.99	15
20.00	200.00	20

Dry run your pseudocode, using a trace table to check the logic. Correct any errors that are found and dry run the pseudocode again.

Flowchart

A **flowchart** makes use of a standardised set of symbols which are connected by lines showing the flow of the algorithm. The purpose of flowcharts is to communicate how a process works or should work without any confusing technical jargon.

The **advantages** of flowcharts include:

- ▶ the flow of the program can be seen clearly

- ▶ flowcharts are created using a standardised set of symbols so can be interpreted and understood by many people.

The **disadvantages** of flowcharts include:

- ▶ with a large, complicated program the flowchart can become very large and difficult to follow

- ▶ changes to the design may result in the flowchart being amended or redrawn.

There are many sets of flowcharts symbols. One set that could be used is shown below in Table 4.3.

Symbol	Meaning
	The start and end of the algorithm
	A process that has to be carried out
	A sub-process
	A decision; this must have 2 outputs – true/false, yes/no
	An input or output
	A connection – used to link parts of a flowchart that cannot be easily connected, for example when the flowchart goes onto a different page
	The flow of the algorithm – arrows are used to show the direction of the flow

▲ **Table 4.3** Symbols used in flowcharts and their meanings

Activity

Create a flowchart to validate a password. The password should be ten or more characters and include at least one number. If the password does not meet these requirements, then an error message should be displayed, and the user asked to edit the password.

Using the flowchart you have created, write some pseudocode to validate the password.

Share your pseudocode with the rest of your teaching group. What are the similarities and differences?

Test yourself

- 1 What is the purpose of a decomposition diagram?
- 2 What is pseudocode?
- 3 Identify one disadvantage of pseudocode.
- 4 What is the flowchart symbol for a decision?
- 5 Identify one advantage and one disadvantage of using a flowchart.

Project practice

An online retailer applies delivery costs to each order. The delivery cost is calculated on the total cost of the items bought. The minimum order is £10. The table shows how the delivery costs are calculated.

Cost of items	Delivery cost
£10.00 – £24.99	£2.50
£25.00 – £39.99	£5.00
£40.00 – £59.99	£7.50
£60.00 – £74.99	£10.00
£75.00 or above	Free

The retailer stores the customer delivery addresses, the items they have purchased, the total cost of the items and delivery costs.

You have been asked to:

- ▶ Create a top-down diagram to show the decomposition of the problem.
- ▶ Create a flowchart to show how the delivery costs will be calculated.
- ▶ Create pseudocode, based on the flowchart, including the use of comments.
- ▶ Explain how the retailer could use pattern recognition.
- ▶ Explain how algorithms could be used to increase sales.

Assessment practice

- 1 Explain what is meant by an algorithm.
- 2 Identify and describe two characteristics of algorithms.
- 3 Explain the difference between the top-down and bottom-up approaches to solving problems.
- 4 Explain how using decomposition can simplify the solving of a complex problem.
- 5 Identify and describe two steps to identifying and recognising patterns when beginning to code.
- 6 Explain the differences between general and specific detail when using abstraction.
- 7 Describe two advantages of using a flowchart to represent an algorithm.
- 8 Compare the use of pseudocode and decomposition diagrams when creating an algorithm.
- 9 How can trace tables be used to check for errors in an algorithm?
- 10 Discuss the advantages of using a flowchart to represent an algorithm.

Core element 5: Digital environments

A digital environment is one where a wide range of digital devices communicate and support the content and activities within it. There are numerous components of a digital environment including the internet, the cloud, virtual environments, networks and physical environments. An organisation can implement a combination of these components to support its business functions. The components used depend on the size and function of the organisation, whether it is based in one location or several locations, and whether it is on a local or a global scale.

In this core element you will learn about the various environments, what they are, how they work and their importance to a digital environment.

Learning outcomes

In this core element you will learn about:

- 5.1** Components of physical computing systems and their applications
- 5.2** Types and applications of networks, hardware and software, and the functions of Internet of Things
- 5.3** The types and applications of protocols used to create networks and network referencing models

- 5.4** The components and benefits of virtual computing systems
- 5.5** The types, services and benefits of cloud computing
- 5.6** The methods and benefits of creating a resilient digital environment

5.1 Components and applications of physical computing systems

Physical computing systems are interactive systems that use different types of software and hardware to sense and respond to external stimuli. This external stimulus could be a software application, a problem, a need, an issue or just an idea. This shows that a physical computing system is a combination of input and output devices that work together as a single entity.

In this section you are going to look at the different components and applications associated with a physical computing system.

Chassis

This is more commonly known as the case or base unit of a physical computing system. The chassis is the housing that organises and protects the components that make up a physical computer system. It is also important to consider the form factors of the chassis. This relates to the size, shape and physical specification of the components that it will contain e.g. the size and orientation of the motherboard. Many people think that the only function of a chassis is to house all of the computer components, but it has other functions as well including:

- ▶ **Aesthetics** – it is more pleasing on the eye to look at a computer chassis instead of a motherboard with wires and components (it is also safer as well; you wouldn't want someone to electrocute themselves or damage the components).
- ▶ **Noise reduction** – many computers and their components require fans to keep everything cool and running properly. These fans can obviously generate noise. Having these all placed inside a chassis can reduce the overall noise of the system.
- ▶ **Cooling** – the chassis helps to keep the air flowing through the system and across the components. This helps to keep everything cool so that it will run properly.
- ▶ **Protection** – components are very sensitive and can be damaged easily. They are vulnerable to dirt, foreign objects, for example paper clips, and electrical interference (**electromagnetic interference (EMI)/radio frequency interference (RFI)**). It is important that the components are protected at all times.

Optical drive

This is a computer disk drive that reads and writes data from optical disks such as CDs and DVDs using laser beaming technology. An optical drive is sometimes referred to as an optical disk drive (ODD). Although an optical drive can be used to read and write data, it is mainly used as an input device. The optical drives rotate the inserted disk at a constant speed in revolutions per minute (RPM) and the data is read using a laser beam which is spread out across the inserted disk using the lens embedded in the optical drive's head.

Mainboard/motherboard

Motherboards have different form factors (size, shape) and are the main printed circuit board within a computer and contain the buses (these are the electrical pathways). Components such as the CPU, heatsink and fan assembly, RAM, BIOS, chipsets, sockets, expansion slots, internal/external connectors and ports are all located on the motherboard. Different motherboards have different form factors.

Central processing unit

The central processing unit (CPU) is the electronic circuitry within a computer system that carries out the instructions of a computer program by performing the arithmetic, logical, control and input/output operations that are specified in the instructions it receives.

Characteristics

- ▶ **Clock speed** – CPUs contain a clock (like a clock that you can hear ticking hanging on a wall or sitting on a shelf). Every time the clock ticks, an instruction is carried out. Depending on that the instructions are that are being carried out, they may only require one tick of the clock, whereas more complex and/

Key terms

Electromagnetic interference (EMI): this is the disruption of electronic operations and electronic devices from electronic emissions. EMI travels in waves and can cause devices to malfunction (which can result in dangerous outcomes).

Radio frequency interference (RFI): this is unwanted signals in the radio frequency spectrum used by Wi-Fi networks (most commonly 2.4 GHz and 5 GHz). Some other electronic devices use the same radio waves as Wi-Fi networks. This causes the prevention of the transmission of data and can create delays and performance degradation.

Characteristic	Features
Form factor A critical factor to consider when upgrading a system because any replacement motherboard must physically fit in the case and use the existing connectors for the power supply.	<ul style="list-style-type: none"> • Size • Shape • Position of the mounting holes • Connector type for power supply • Types of ports and their locations
Chipsets	<ul style="list-style-type: none"> • Determines the main characteristics of the motherboard, e.g.: <ul style="list-style-type: none"> – the processor it supports – the type and amount of RAM it can use – the bus types and speeds it supports – the standards it supports, e.g. AGP, USB • Usually contains two large chips although some chipsets can contain three or more • Determines motherboard performance and potential future upgradability

▲ Table 5.1 Types of motherboards and their characteristics

or larger instructions may require numerous ticks. This means that the faster the clock speed, the more instructions that can be carried out per second.

- ▶ **Cache** – The cache is similar to RAM in that the CPU gets instructions from it. Cache is faster than RAM when it comes to reading from it and writing to it and therefore temporary data that is frequently used is stored in it. This means that applications are able to load faster and even work ‘offline’, without having to be downloaded every time they are needed. As a result of these efficiencies, a higher cache value helps to increase the speed of the computer.
- ▶ **Cores** – A core is a processor with its own cache. Modern computers have a CPU containing multiple cores e.g. quad-core. This enables each core within the CPU to carry out a different process which in turn increases the speed of the overall system and the computer is able to ‘multi-task’.
- ▶ **Bit size** – A bit is one binary digit and the smallest unit of data. It can either have a binary value of 1 or 0. The instructions and data accessed by the processor is in binary code. In terms of the processor, the bit size (number of bits) relates to the registry size and the size of the data that it can work with at any one time. Bits are placed in group of 4, so a 32-bit processor would have 8 groups of

4 binary code (or bits), whereas a 64-bit processor would have 8 groups of 4 binary code. A group of 4 bits is known as a byte. A 64-bit processor is not necessarily faster than a 32-bit processor as there are other things that increase the speed of a computer, for example its clock speed.

Some of the different types of processors are presented in Table 5.2.

Random access memory

Random access memory (RAM) is sometimes referred to as main memory, primary memory or system memory. It is a hardware device that allows information to be stored and retrieved on a computer system. The data is accessed randomly (instead of sequentially) in the same way as data is accessed from a CD or hard drive. This means that access times are much faster. However, RAM is known as volatile memory and the data is only available if there is power to the system. If the computer is turned off, all the data contained in RAM is lost.

There are several characteristics of RAM.

- ▶ It is fast and has a long life.
- ▶ There is no need to refresh.
- ▶ It has a high power consumption.
- ▶ It can be expensive.

Key terms

External bus: sometimes referred to as the expansion bus. This is a connection between a computer and external devices.

Application Specific Integrated Circuit (ASIC): a microchip designed for a specific application such as a handheld digital device or as a transmission protocol.

Field Programmable Gate Array (FPGA): an integrated circuit consisting of internal hardware blocks. The hardware blocks have user-programmable interconnects to enable customisation of operations for a specific application.

Processor type	Uses	Characteristics	Features
Microprocessor	<ul style="list-style-type: none"> Computers Smartphones Vehicle speed controllers Traffic lights Military applications 	<ul style="list-style-type: none"> Consists of a CPU Uses an external bus to interface with RAM, read only memory (ROM) and other peripherals Expensive and complicated, with many instructions to process 	<ul style="list-style-type: none"> Provides inbuilt monitor/debugger program with interrupt capability Offers parallel input/output Instruction cycle times External memory interface
Microcontroller	<ul style="list-style-type: none"> Mobile phones Vehicles CD/DVD players Washing machines Security alarms Lighting systems Fire detection systems Keyboard controllers Watches Cameras Microwave ovens 	<ul style="list-style-type: none"> Consists of the following integrated on one chip: <ul style="list-style-type: none"> CPU Memory I/O Uses an internal controlling bus Inexpensive and straightforward with fewer instructions to process 	<ul style="list-style-type: none"> Contains a processor reset Program and variable memory (RAM) I/O pins Device clocking central processor Instruction cycle timers
Embedded processor (can be confused with microcontrollers)	Controls electrical and mechanical functions	<p>At a basic level, they are a CPU chip placed in a system that it helps to control</p> <ul style="list-style-type: none"> Similar functions to microcontrollers but it: <ul style="list-style-type: none"> integrates with the system it is part of in a different way (embedded processors require additional resources such as RAM and registers in order to control a system, whereas a microcontroller contains everything it needs in one single chip to carry out the same function) can also perform different functions (an embedded system is used to create an automated device as well as controlling devices using a microcontroller) Requires external components, e.g. integrated memory and peripheral interfaces Often a component within a microcontroller 	<ul style="list-style-type: none"> Simple design Limited computational power Limited I/O capabilities Minimal power requirements
Digital signal processor	<p>Used for measuring, filtering and/or compressing digital/analogue signals such as voice, audio, video, temperature, pressure or position and manipulates them mathematically</p> <p>Examples include:</p> <ul style="list-style-type: none"> speech processing image processing medical processing biometric processing seismology radar 	<ul style="list-style-type: none"> Processes signals such as voice, video, temperature, audio, position and pressure from the real-world in real-time that has been digitised. It then mathematically manipulates them so that they can be converted to another form of signal or display information. E.g. digital TVs use DSP to ensure that the TV is compatible with different types of video standards e.g. VGA, SVGA, SXGA, UXGA They have programmable processors so that their parameters can be changed to accommodate different applications e.g. for use in cell phones, digital TVs or sound cards Can quickly perform mathematical calculations such as add, subtract, multiply and divide 	<ul style="list-style-type: none"> Analyses and manipulates signals Can process signals using a computer, Application Specific Integrated Circuit (ASIC) or Field Programmable Gate Array (FPGA)

▲ Table 5.2 Processor types and their uses, characteristics and features

- ▶ The data is stored electrically on transistors.
- ▶ It is volatile (if a computer loses its power, all data in the RAM is lost).
- ▶ It stores the operating system, applications and graphical user interface (GUI).
- ▶ It is volatile memory and can be changed, upgraded or expanded easily by users.
- ▶ It is faster than secondary memory.

RAM should not be confused with **ROM (Read Only Memory)**. ROM is non-volatile and is used to store the instructions for the computer and other electronic devices such as smartphones. It is sometimes referred to as the firmware of the computer/device. It does not lose these instructions even when the system is powered down and is read only as per the name. It can be argued that the data stored on it can be edited, but this is not an easy task.

Graphics processing unit

The graphics processing unit (GPU) is an electronic circuit used to speed up the creation of both two-dimensional (2D) and 3D images. They can either be integrated (built into the computer's CPU or motherboard) or dedicated (a separate hardware component referred to as the video card). Due to the GPU having a separate processor, the CPU's resources can be used for other tasks.

Storage

Storage is often referred to as secondary storage for digital systems. Secondary storage is non-volatile, long-term storage. Without secondary storage, all programs and data would be lost the minute the computer system was turned off.

Device	Characteristics
Hard drive	<ul style="list-style-type: none"> • Is an electro-mechanical device • Uses one or more rotating disks • Relies on magnetic storage • Has slower access speeds than an SSD • Can be internal (within the casing of the PC) or external (connected by a cable to the PC which makes it removable) • Susceptible to damage from magnetic fields or by dropping or banging against a surface • Not as expensive as others
Solid state drive (SSD)	<ul style="list-style-type: none"> • No moving parts so more robust than hard drives • Data is stored electrically instead of magnetically • Most SSDs use flash memory • Has faster access speeds than a hard disk drive • Can be internal or external, the same as hard disk drives • External SSDs are more portable due to their smaller size • Has limited read/write cycles • More expensive than a hard disk drive
Flash drive	<ul style="list-style-type: none"> • Lightweight • Micro-portable • Used for file storage • Do have size limitations
Cloud	<ul style="list-style-type: none"> • Manages a system with minimal resources • Has different access methods – the protocol through which cloud storage is accessed • Performance is measured in bandwidth and latency • Is accessible to multiple users • Can be scaled up or down dependent on storage needs • Ability for the cloud storage provider to provide the data back to the user upon request • Customer is able to control and manage how the data is stored and the costs associated with the importance of the data • The more data stored the greater the efficiency • Able to reduce cost using the cloud, e.g. cost of purchasing storage, powering storage, repairing storage devices (when a drive fails) and managing the storage
Serial-attached SCSI (SAS)	<ul style="list-style-type: none"> • Faster and more reliable than SATA drives • SAS drives tend to be used for enterprise computing where high speed and high availability are critical • SAS drives have lower storage capacity than a SATA drive • Cables can be up to 10 metres in length • Power and data are provided through the same cable

Device	Characteristics
Serial Advanced Technology Attachment (SATA)	<ul style="list-style-type: none"> Tends to be used for desktops, data storage and backups SATA cables limited to 1 metre in length Data and power cables are separate
Small Computer System Interface (SCSI)	<ul style="list-style-type: none"> Uses a single cable Has its own unique controller Can work with different computer types Fast performance Is more expensive and costly Is hard to configure as each device has its own unique identification

There are three main types of secondary storage devices used for computer systems:

- ▶ solid state
- ▶ optical
- ▶ magnetic.

Not all computers require secondary storage, for example embedded computers such as those found in a central heating system or a washing machine. These do not need to store data when the system is powered off. Instead, the instructions needed to run them are stored in the ROM and the user data held in RAM. Below is a list of secondary storage devices and their characteristics:

Fan

This is a hardware device that keeps the entire computer system or a computer device cool. It circulates air to or from the computer system or component. The speed of the fan is measured in revolutions per minute. The higher the rating of the RPM, the louder the fan can be.

Different types of fans include:

- ▶ **CPU fan** – this is placed on the top of the computer processor and is used to help pull off and blow away the hot air from the processor thereby keeping it cool.
- ▶ **Power supply fan** – this is located inside the power supply and blows the hotter air away from the power supply and out of the computer case.
- ▶ **Video card fan** – this is situated on the video card and used to prevent it from overheating. This is especially important when playing video games, editing videos or other tasks that rely on the heavy use of the graphics processing unit.
- ▶ **Case fan** – is usually situated on the inside on one side of the computer chassis. It helps to circulate air in the chassis and to blow the hotter air out of the chassis.

Redundant array of independent disks card

This is the combining of multiple disk drives into a single unit (array). RAIDs reduce data loss and improve performance. Because the disks work in unison, they are more reliable and faster, reducing data loss and improving overall performance. The increases in speed and reliability depend on the type of RAID used.

RAID is a way to combine several smaller disks into a single storage option. There are many ways to use RAID, but its main purpose is storing the same data across multiple drives. This means that if one disk fails the system can survive, and restore data, due to the remaining drives.

Peripherals

Screen

The screen is also known as the monitor. There are different types of screens/monitors. Some are just output devices (enabling the user to read what is being displayed on the screen) or input/output devices. Input/output screen devices not only allow the user to read what is being displayed, but they also allow a user to input data using their fingers or a touchscreen pen.

Modern monitors are created using flat-panel display technology, backlit with light-emitting diodes. They interpret and display graphical output signals from the computer's graphics card.

Key term

Data redundancy: this is a condition that is created within data storage technology where the same piece of data is held in two separate places. Whenever data is repeated it is data redundancy. Although it can occur by accident, it can also be done deliberately for the backing up and recovery of data.

There are two main types of monitors, LCD (Liquid Crystal Display) and LED (Light Emitting Diode). Whilst both types of monitor use liquid crystals to help create the image, the difference is the backlights that are used. LED monitors use LEDs as the backlights whilst LCD monitors use fluorescent lights. They also use less power than LCD monitors and are therefore more friendly to the environment. Not all LED monitors provide the same image quality as it depends on the layout of the LEDs. If the LEDs are evenly placed across the entire screen they provide a better quality than when the LEDs are only placed around the edge of the screen. So, depending on the LED configuration, for example the edge configuration of the LEDs, there are instances when they do not provide such a good quality image as an LCD monitor. With LCD monitors the liquid crystals are placed between two sheets of glass for every pixel. The current from the monitor liquifies the crystals allowing the white light that is emitted from the backlights to pass through them.

LED monitors that are configured with LEDs across the entire screen will have a better viewing angle spectrum than the edge configuration. This is because the visibility of the edge configuration reduces as you move away from the central position of the screen, there are also more glare issues than with the full screen LED configuration. This is where an LCD monitor will win over an edge configurated LED monitor as the LCD will have better viewing angles and less glare because all areas of the screen is lit.

The edge-configured LED monitor is the thinnest and cheapest but as previously stated it has its disadvantages. But if space is of a premium, then they are worth considering. As with all things it depends on what it is being used for, for example gamers would need to purchase an LED monitor with the LEDs placed across the entire screen because of the various viewing angles available.

Touchscreens

These are commonly used for smartphones, tablets and laptops, although there are now many desktop monitors which have touchscreen facilities.

Their features include:

- ▶ being touch sensitive so react to fingers moving across the screen
- ▶ allowing the user to point, drag or select options on the screen as opposed to using a mouse
- ▶ containing two, sometimes three, simultaneous touchpoints (depending on the number of people

using the touchscreen at the same time or the requirements of a particular package); uses of touchpoints include to zoom and use two finger taps

Keyboard

Keyboards are input devices and there are many different types of keyboard, including:

- ▶ USB – does not require additional power source, not affected by external sources/signals, cyber criminals would need to install a key logger to access the information being typed in
- ▶ wireless – can be placed in any convenient location on the desk which reduces workplace clutter
- ▶ integrated (e.g. integrated into laptops) – smaller than a standard keyboard, more mobile than external keyboards
- ▶ on screen (e.g. smartphones, tablets, touchscreen devices) – more mobile than external keyboards.

Features include:

- ▶ allowing the user to input commands and control the computer
- ▶ used to input letters, numbers and symbols
- ▶ includes additional keys, for example **function keys**, **control keys** and **special purpose keys**.

Mouse

As with monitors there are different types of mouse, and they are used for input. Types include:

- ▶ USB – does not require additional power source
- ▶ wireless – can be placed in any convenient location
- ▶ laptops have a touchpad (and some laptops are also touchscreens)
- ▶ smartphones, tablets and touchscreen devices are controlled by the user's finger acting as a mouse.

Features include:

- ▶ allows users to control the on-screen cursor
- ▶ usually contains two buttons (left and right button)
- ▶ tracker wheel is used to scroll up and down pages on websites and documents.

Test yourself

- 1 Explain the purpose of a chassis used in computer systems.
- 2 Compare the different types of screens used in computer systems.
- 3 Identify two different types of fans used in a computer system.
- 4 Describe three different types of secondary storage.
- 5 What does the term 'RAID' stand for?

5.2 Types and applications of networks, hardware and software, and the functions of Internet of Things

Networks

There are several types of networks. Many of these networks have a wired connectivity option as well as a wireless connectivity option.

Personal area network

Personal area networks (PANs) are very small networks of connected devices within one building and used by an individual or very small business. PANs can be created using Ethernet cables, USB and/or Firewire. They have limited distance accessibility; hence they are small and not used by larger organisations. Think of a PAN as a network within a single room for a single user (or users if they are in the same room), whereas a LAN is a network for a building for multiple users.

Wireless personal area network

Wireless personal area networks (WPANs) are the wireless version of PANs; they use Bluetooth technology or WiFi and have a limited distance of accessibility.

Local area network

A local area network (LAN) is one of the most common and simplest types of network. It is the connection of groups of computers and low voltage devices across a short distance. A short distance can be within the same building or between a group of buildings that are in close proximity to each other and need to share information and resources. LANs use routers to connect to wide area networks (WANs) so that information can be shared, and data can be transferred quickly and securely.

Wireless local area network

These are basically the same as LANs but without the cables connecting the hosts and the servers. They are connected using wireless technology, commonly referred to as WiFi. Radio signals are used as the medium of communication with computer systems requiring wireless network cards. Most systems connect to the network using a router to communicate with other devices/systems on the network or for accessing the internet which is a Wide Area Network (WAN). The range of a WLAN can be within a room, a building or across buildings in close proximity to each other.

Metropolitan area network

A metropolitan area network (MAN) is a network that spans a large area, for example a town or city. It is smaller than a WAN. An example of a MAN is a series of wireless routers which are distributed across a town or city where the routers are linked to an internet connection. This allows the users to connect to the internet once they have connected to the MAN. They are also bridged together and that provides access points which have the same name and authentication method for access. Once a device is connected to one of the routers, the user is automatically connected to the routers that are in other locations within the MAN. Although there is no set limit to the size range of a MAN, they are mostly between 3 and 30 miles in diameter. MANs are sometimes considered as WANs because they cover large areas. But a MAN is a single network and not several interconnected networks which is what constitutes a WAN.

Wireless metropolitan area network

The wireless metropolitan area network (WMAN) is a form of wireless networking that spans the size of a city or town. They are **point-to-point** or **point-to-multiple** networks that have individual links that not only span distances of up to 30 miles, but they can also provide what is known as **last mile connectivity** in metropolitan environments. A WMAN is owned by an Internet Service Provider (ISP), a government department or a large corporation. Access to the WMAN is restricted to authorised users or subscriber devices.

Wide area network

Wide Area Networks (WAN) cover a wide area for communication between computers. The internet is a good example of a WAN. A WAN comprises a series of LANs that have been joined together. A router is used to connect the LANs to WANs. Many WANs like the internet are not owned by one person or organisation

Key terms

Point-to-point networks: sometimes referred to as P2P, this is a data link providing a path from one fixed point to another. This streamlines communication links between points.

Point-to-multiple networks: this is where a single data link is shared by more than two devices.

Last mile connectivity: this refers to the final stage of the telecommunications network, delivery to the end user.

but accessed by many individuals and organisations. Multinational organisations, however, invariably have their own WANs.

Wireless wide area network

WWANs use mobile phone signals as opposed to radio signals. The mobile phone signals are provided by mobile phone service providers and facilitate the transmission of signal over a wide area.

Virtual private network

A virtual private network is an encrypted connection over the internet from a device to a specific network. The encrypted connection ensures that sensitive data is safely transmitted. It prevents unauthorised people from '**eavesdropping**' on the traffic and enables the user to work remotely while maintaining security of data. VPNs are used a lot in corporate environments.

VPNs allows an organisation/individual to create a protected network which is very important when using a public network. A VPN masks the IP of the user that makes browsing almost untraceable. The VPN directs the Internet traffic through one of its servers after it has been encrypted. It is recommended to always use a VPN when connecting to public networks/hotspots. VPNs are used by organisations so that remote working employees can securely access internal company data and services irrespective of their location.

Hardware

Switch

This is a device that takes in the packets that are being sent by devices that are physically connected to its ports and sends them out again. However, it only sends them out through the ports that lead to the devices that the packets are intended for.

When a device is connected to a switch, the switch takes note of the device's **Media Access Control**

Key terms

Eavesdropping: also referred to as sniffing or snooping. Eavesdropping is when someone takes advantage of an unsafe or unsecure network in order to steal information transmitted through digital devices.

Media Access Control (MAC): this is a unique code in the device's Network Interface Card, identifying the physical device.

(**MAC**) address. The switch uses the MAC address to identify which device is sending out packets and where incoming packets need to be delivered to.

When a device sends a packet to another device, it enters the switch, which then reads the information (known as the header) to interpret what to do with the packet. It will match the destination address/addresses and send the packet out through the appropriate ports that lead to the destination devices.

Characteristics

- ▶ They use MAC addresses to send data packets to selected destination ports.
- ▶ They use packet switching to receive and forward packets from the source device to the destination device.
- ▶ They support one-to-one (unicast), one-to-many (multicast) and one-to-all (broadcast) communications.
- ▶ Transmission mode is full duplex which means that the communication in the channel can flow in both directions at the same time. This reduces collisions between the network traffic going to and from a connected device and the switch at the same time.
- ▶ They are classed as active devices which have network software and network management capabilities.
- ▶ They can perform some error checking before forwarding the packets to their destination port.
- ▶ They can be used to support virtual local area networks (VLANs) as they can also operate in Layer 3 of the OSI model.

Router

Routers are devices that communicate between the internet and the devices connected to the network. They 'route' traffic between the devices and the internet and are responsible for organising the communication between computer networks. A router takes data packets from devices and 'routes' them to the correct destination. They often use Internet Protocol (IP) addresses so that they know where to look for information about the devices they are communicating with. Routers enable computers to request files from a server or access the internet. They ensure that the information goes to the correct device that requested it.

Characteristics

- ▶ Routers are multi-port devices with high-speed backbones.

- ▶ They support filtering and **encapsulation**.
- ▶ They are self-learning because they can communicate their existence to other devices and learn of the existence of new routers, nodes and LAN segments.
- ▶ They consider the network as a whole when routing traffic. This confirms that routers have a high level of intelligence in order to perform this task.
- ▶ They constantly monitor the condition of the network as a whole and will dynamically adapt to changes in the condition of the network.
- ▶ They provide a certain level of redundancy and are therefore less prone to catastrophic failure.

Network Interface Card

A Network Interface Card (NIC) is a circuit board or chip that is installed on a computer so that it can connect to a network. An NIC will provide a computer with a dedicated, constant connection using either **Ethernet** or Wi-Fi. An NIC represents the device it belongs to and can prepare, transmit and control the flow of data on the network.

Consider the following example for how a NIC works:

A person requests access to a web page. This request is passed to the NIC which converts it into electrical impulses. These impulses are received by the web server on the internet which responds to the NIC by sending back the web page as electrical signals. The NIC then translates these electrical signals into data and transmits the data back to the computer and the data is displayed on the screen.

Originally these network controllers were expansion cards that were plugged into a computer port, USB device or router. More modern network-unique controllers are built directly into the computer motherboard chipset. There are different types of NICs as outlined here.

Types of NIC

The standard NIC is a circuit board that is installed into the computer so that it can connect with the motherboard. This can be achieved in several different ways.

- ▶ **Wired** – these have input jacks that are for plugging in the network cables. The most popular wired technology for a LAN is the Ethernet. These types of NICs are plugged into the peripheral component interconnect circuit boards. These PCI slots and associated NICs that fit the slots are becoming more and more obsolete as technology changes.

- ▶ **USB** – these are NICs that provide connections to a network through a device plugged into the USB port.
- ▶ **Wireless** – these NICs use an antenna to provide wireless reception through radio frequency waves. These are designed for Wi-Fi connection.
- ▶ **Fibre optic** – these are expensive and more complex NICs used as a high-speed support for network traffic handling on server computers.

Network interface devices

Network interface devices (NIDs) are sometimes referred to as network interface units (NIUs). They are the interface between the network provider and the customer and are usually situated outside the customer's premises.

Peripheral component interconnect network cards

Peripheral component interconnect (PCI) is a connectivity slot which is becoming obsolete but was used for installing NICs as already discussed.

Universal serial bus network cards

A universal serial bus (USB) port is a standard cable connection interface. It is an industry standard for short-distance digital data communications. USB devices such as network adapters (network cards) are connected to a system via a USB port.

Cabling

Wired connection methods use cables to connect devices to the network and/or internet. There are different forms of cabling, including:

Copper cable

This uses a type of coaxial copper cable and technology called **Data Over Cable Service Interface Specification (DOCSIS)**. Cat 5/Cat 5e (Category 5) cables are commonly referred to as Ethernet cables

Key terms

Encapsulation: information is taken from a higher level and a header is added to it, treating the higher layer information as data. The Internet Protocol packet is then encapsulated into a layer 2 Ethernet frame. The frame is then converted into bits at layer 1 and sent across the local network.

Data Over Cable Service Interface Specification (DOCSIS): an international telecommunications standard permitting broadband data transfer using the same cable systems that were used for transmitting cable television signals.

and used for providing the wired connection between devices and a network. Cat 5e has a higher throughput speed than Cat 5 and is also backward compatible.

There are three types of copper cable:

- ▶ **coaxial** – its effectiveness deteriorates over long distances
- ▶ **unshielded twisted pair** – this is made by twisting copper cables around each other. This reduces the deterioration over distances
- ▶ **shielded twisted pair** – uses copper shielding around the twisted wires to help protect them

against interference from electrical and magnetic forces.

The **advantages** of copper cable are:

- ▶ a cabled telephone is powered directly from the copper cable; this means that the telephone will still function even if there is no power
- ▶ it is cheaper to set up a network using copper cable than with fibre optic.

Its **disadvantage** is that it deteriorates over long distances.

UTP Categories

UTP Category	Maximum length	Data rate	Application
Cat 1	N/A	Up to 1Mbps	Old telephone cable
Cat 2	N/A	Up to 4Mbps	Token ring networks
Cat 3	100 metres	Up to 10Mbps	Token ring & 10BASE-T Ethernet
Cat 4	100 metres	Up to 16Mbps	Token ring networks
Cat 5	100 metres	Up to 100Mbps	Ethernet, fast ethernet, token ring
Cat 5e	100 metres	Up to 1Gbps	Ethernet, fast ethernet, Gigabit ethernet
Cat 6	100 metres	Up to 10Gbps	Gigabit ethernet, 10G ethernet (55 metres)
Cat 6e	100 metres	Up to 10 Gbps	Gigabit ethernet, 10G ethernet (55 metres)
Cat 7	100 metres	Up to 10 Gbps	Gigabit ethernet, 10G ethernet (100 metres)

Digital Subscriber Line

The Digital Subscriber Line (DSL) method uses standard phones lines to send and receive information. This enables the user to make telephone calls as well as access the internet and transfer data.

The **advantages** of DSL are:

- ▶ it does not require new wiring as it uses an existing phone line
- ▶ you can use the internet and the phone line at the same time
- ▶ it is cheaper than cable connections.

The **disadvantages** are that:

- ▶ it receives data faster but has a much slower transmission speed
- ▶ it is still not available in all rural areas.

Fibre optic

This is the fastest method of delivering electrical signals by converting them into optical signals,

transmitting them through a thin glass fibre and reconverting them to electrical signals. Fibre optic is a very reliable and secure transmission media that supports high bandwidths and can cover long distances.

The **advantages** of fibre optic are that:

- ▶ it has a higher bandwidth than copper cables
- ▶ it allows for data transmission over longer distances
- ▶ it has resistance to electromagnetic interference
- ▶ the cables are lighter, thinner and occupy less area than copper cables.

The **disadvantages** are that:

- ▶ it is not as robust as cables and usually requires special test equipment
- ▶ it is more delicate than copper wires.

Benefits and drawbacks of wired connection methods

Benefits	Drawbacks
Security can be stronger for a wired network because the network can be configured with firewalls and other similar security applications that prevents unauthorised access.	Wired networks are more time consuming to install than wireless networks. This is because of the requirement to install the cabling and the connection of routers, switches and hubs, all of which will require configuring as well.
Unauthorised users cannot connect to the network without the use of an Ethernet cable.	There is less mobility with a wired network e.g. if a person wants to take their device to the other end of the building, they will need to ensure that there was an access point for them to connect their device to.
Wired networks can be more reliable and stable than wireless networks. This is because the routers, hubs, switches etc and connected using physical cables and therefore the entire system is more robust. In addition, there is less chance of interference from other network signals that are in close proximity.	All networks require maintenance, but a large network will have one or more servers. The more devices that are connected, the more there is a need for additional requirements such as a server to manage the additional capacity on the network.
Wired networks are usually faster than wireless networks as each cable connected to a device transmits at the same speed.	Users wanting to access the network must have physical access via a cable as opposed with a wireless network where they only have to be in the proximity of the network.
Wireless networks can suffer from 'black spots' where signals are inaccessible or difficult to get through (e.g. very thick walls in a building). Wired networks do not suffer the same problem as there is always a connection via a cable.	

Wireless access point

A wireless access point (WAP) is a networking device that permits wireless-enabled devices to connect to a network. A WAP is used to create a wireless network within an existing wired network. WAPs can also be used to extend the signal range and strength of a wireless network and mitigate against 'dead spots'. This is especially useful in large office spaces and buildings. There are some common types of access configuration as identified below.

- ▶ **Root access point** – this is where the access point is connected directly to a wired LAN and creates a connection point for wireless devices. In order to allow users to roam from one area to another without losing the network connection, a number of access points can be used.
- ▶ **Repeater access point** – this is an access point that can be configured to extend the range of the network infrastructure or overcome obstacles that can block radio communication signals. The repeater will forward the traffic between the wireless users and the wired network. This is achieved by sending data either to another repeater or access point that is connected to the wireless network. The data is always sent via the route that will give the best performance.
- ▶ **Bridges** – access points that can be configured as **root** or **non-root bridges** in order to join multiple

networks. They will establish a wireless bridge with a non-root bridge and traffic is then passed over the wireless link to the wired network.

- ▶ **Workgroup bridge** – access points that are part of a workgroup bridge can link to other access points as 'clients' and provide network connections for devices that are connected to Ethernet ports.
- ▶ **Central unit in an all-wireless network** – the access points act as a standalone root unit. This is not attached to a wired LAN as the access points function as a hub linking all of the stations together. It acts as the focal point for communications and increases the communication range of wireless users.

Key terms

Root bridge: a bridge that is located at the starting point of a wireless infrastructure topology. It is usually connected to the main wired backbone local area network.

Non-root bridge: often referred to as a remote or repeater bridge. It establishes a connection to the root bridge or another repeater bridge to connect the wired local area network (LAN) to part of the bridged LAN.

Servers

A computer server can be hardware or software and is used to provide centralised services such as data and/or resources such as printers, applications to other devices (known as clients) on a network system. There are different types of servers e.g. database, mail, print, file etc.

The clients connected to the network sends a message to the server, for example sending a request to access email (from a mail server) or accessing an application (from an application server), and the server then responds to the request from the client providing them with the data and/or resource requested. Proxy servers act as intermediaries between clients and other servers, often to mitigate security risks.

Research activity

Research the following types of servers and complete the table:

Type of server	Purpose of server	How it works	Characteristics
File			
Application			
Database			
Print			
Virtual			
Mail			
Web			
Domain Name Server (DNS)			
Hybrid			
Proxy			

An operating system (OS) is a program that is installed onto a system and manages the other available application programs. An application program will request services through an application program interface (API). Users are able to interact with the operating system using a user interface such as a graphical user interface (GUI) or a command-line interface (CLI). Without an operating system, applications would have to have their own user interface as well as detailed code to deal with low level functionality such as network interfaces and disk storage to name but a few. This would make the development of software impractical.

Many of the common tasks e.g. displaying text on the screen, sending network packets, can be managed by the operating system (system software). It will act as the 'go-between' for the applications and hardware. An operating system provides a consistent process for applications to interact with the hardware.

Software

Operating systems

Proprietary software

This is any software that has been copyrighted and has restrictions against use, distribution and modification.

These restrictions are imposed by the publisher, vendor or developer. It remains the property of the owner/creator and is used by individuals and organisations under predefined licensed conditions. Proprietary software is sometimes referred to as closed-source software or commercial software. For example, the Windows operating system is the property of Microsoft and the macOS operating system is the property of Apple.

Open source

As opposed to the restrictions with closed-source (proprietary) operating systems, open-source operating systems are freely available for anyone to view, modify, use and share. Being able to inspect the source code has an advantage for people with technical knowledge as they can customise the operating system and fix problems as they arise.

Linux

The basis of most open-source operating systems available today is the Linux **kernel**. The kernel interacts with the computer's hardware, controlling how data is processed and parcelled out into memory. It controls how the system handles files and interacts with devices that are plugged into the computer, as well as many other fundamental tasks. Developers of operating systems use the Linux kernel as a basis for creating the operating system.

Type	Purpose	Functions/features
Batch operating systems	Collect programs and data together in a batch before processing	<ul style="list-style-type: none"> • Processes batches of data at regular intervals. • No user interaction required. • Batch processing carried out when least demand for processing power e.g. at weekends or at night. • Can be set to run at specific times e.g. at the end of the month for a payroll system. • Batches processed on a first come first served basis.
Multitasking/time-sharing operating system	Enables the use of a single computing resource for multiple uses at the same time.	<ul style="list-style-type: none"> • Involves the processor carrying out multiple tasks at a time e.g. a user using the internet and using a word processing package. • The programs being used are either waiting, runnable or running. • The OS schedules the processes to be executed by the CPU (when to change between the processes based on their waiting, runnable, running status). • As the OS facilitates multi-tasking, several applications can be stored in the RAM at the same time complex to set up.
Real-time operating system (RTOS)	An RTOS switches between tasks rapidly giving the impression that programs are being executed at the same time. It aids the management of different hardware resources and hosts the applications that run.	<ul style="list-style-type: none"> • Typically used for embedded applications i.e. systems within another application e.g. a car management system. • Data is processed as soon as it is received by the processor. • It is high performance – fast response time and based on user requirements. • Priority scheduling – will process high priority assigned tasks first. • Higher security and reliability standards – used for critical systems e.g. aircraft controllers. • It will always produce the same output if the same input is used. This is known as determinism.
Mobile operating system	This is the software platform to run mobile devices. It is responsible for determining the functions and features available on the mobile device, e.g. email, text messaging, synchronisation with other apps, keyboards, etc. The mobile operating system also determines which third-party applications (known as mobile apps) can be used on the mobile device.	<p>Types of mobile operating systems include:</p> <ul style="list-style-type: none"> • Android OS – Google's open and free software stack that includes an S, middleware and key applications for use on mobile devices (including smartphones). • iPhone OS/Apple iOS – only available on devices manufactured by Apple. It is derived from Apple's macOS. • Windows Mobile (on Windows phones) – a Microsoft operating system used in smartphones and mobile devices with or without touchscreens. Based on the Windows CE 5.2 kernel.

▲ **Table 5.3** Operating systems: their purpose and functions/features

Key terms

Kernel: a computer program that is the core of an operating system. An operating system has control over the computer system and therefore the kernel also has control over all aspects of the system. It is the most important component of an operating system. When a computer system starts up, the kernel is the first program to be loaded after the bootloader. This is because the kernel has to control the rest of the start-up process for the operating system. The kernel

remains in memory until the operating system is shut down. It is responsible for low-level tasks such as memory and disk management, task management and device management. It is an interface between the user and the hardware components of the computer system.

Middleware: software which is 'in the middle' of the operating system and its active applications. It allows communication and data management for distributed applications by operating as a hidden translation.

Features of the Linux operating system:

- ▶ It can co-exist with other operating systems.
- ▶ It supports multitasking.
- ▶ It can run multiple user programs.
- ▶ Individual accounts are protected due to appropriate authorisation.

Unix

Unix is a multitasking and multi-user operating system. The Unix system is built around a core kernel that manages the system and other processes. The kernel subsystems can include process, file, memory and network management.

Features of the Unix operating system:

- ▶ It is a multi-user system sharing the same resources with different users.
- ▶ It facilitates multitasking (users can carry out a number of processes at the same time).
- ▶ It has built-in networking functions.

Network operating system

This is one of the most important types of operating systems. The network operating system (NOS) runs on a server and provides the capability to manage users, groups, security, applications, data and other networking functions. It facilitates share file and printer access across multiple users.

Features of a NOS:

- ▶ The centralised servers are stable.
- ▶ The security of the network is managed by the server.
- ▶ Facilitates remote access to the servers from different locations and types of systems.
- ▶ Upgrades using new technologies and hardware are easily integrated into the system.
- ▶ The purchase costs and running costs are high.
- ▶ There is a dependency on a central location.
- ▶ Regular updates and maintenance are required.

File management utilities

Utility software is used to help manage, control and maintain the computer system and associated resources. Various operating systems have in-built utility software, for example disk scan or disk defragmentation, but there are also many programs available that can be installed onto a system. These include anti-virus and anti-malware software, registry cleaners and so on.

Application software

These are specific programs that are installed onto a computer system or made available via the Cloud, for end-users to perform a range of tasks. Application software can include graphics and CAD software,

office suite software such as Microsoft 365, and browser software such as Google Chrome and Firefox.

- ▶ **Productivity suites** – this is a group of programs that can include word processing, spreadsheet creation, presentation and presentation development software, which is accessible by opening one main application, for example Microsoft Office 365. Video editing software and image development software are other examples. Suites such as Microsoft Office, OpenOffice, Google Docs, Adobe Creative Cloud and Apple's iWork enable users to share data among the programs within the suite as well as download and use templates. These suites are available for multiple platforms including Windows, Mac and Linux systems.
- ▶ **Protection software** – this is software that is used to protect a computer system from cyber attacks, especially when accessing the internet and networks. There are different forms of protection software as follows:

- **Firewalls** – some operating systems, such as Microsoft Windows, have built-in firewalls. A firewall is used to control the incoming and outgoing traffic between networks. There are two types of firewall: a hardware component found in a router and a software component. Both protect the network and help to prevent the spread of viruses.
- **Anti-virus** – this seeks out and destroys viruses. Viruses are programs or code that are loaded onto a computer without the user knowing. There are many types of virus, and anti-virus protection software options have become increasingly complex over time. The anti-virus programs will look for issues on a hard disk and fix anything that is found which can cause problems. They must be kept up to date and have a dictionary that is used to search for and/or monitor all programs and inform of any suspicious behaviour.
- **Anti-spyware** – spyware is not the same as a virus. Spyware is software that gathers information (just like a spy), through an internet connection. Spyware is usually accidentally installed when trying to install free software. The program accesses information that it sells to advertisers, marketeers and anyone else that would be interested in the information.
- **Anti-malware** – malware is short for malicious software. This term incorporates everything from viruses, Trojans and worms. Anti-malware programs are designed to discover the newest and latest threats, and counteract them. The best protection for any system is a combination of anti-virus and anti-malware programs.

Web browsers

Web browsers are sometimes referred to as internet browsers or just browsers. They are software programs that explore and present content on the World Wide Web. The content includes text, images, videos and web pages. Web pages are connected using **hyperlinks** and classified with **Uniform Resource Identifiers (URIs)**. A URI is the identified for a specific resource, e.g. a document or image. A URL is also a special type of identified but it also tells you how you can access the resource, e.g. <https://> or FTP.

This is a list of current web browsers available:

- ▶ Google Chrome
- ▶ Microsoft Edge
- ▶ Mozilla Firefox
- ▶ Opera
- ▶ Apple Safari
- ▶ Amazon Silk.

When a web browser is opened, and the computer system is connected to the internet, the home page or a start screen with favourite pages is displayed. Once open, the user can browse the internet by using a **search engine** to search for what they would like to find, by entering a URI or by following hyperlinks.

Functions of the Internet of Things

First, it is important to understand the term ‘the Internet of Things (IoT)’. In its broadest sense, the IoT is the encompassing of everything connected to the internet. This has now increased to define devices or objects that ‘communicate with each other’. The IoT is made up of devices, for example smartphones, smart wearable devices, smart lights, smart doorbells and so on that are connected together.

When these smart devices are combined with automated systems, they can then gather information, analyse it and create an action. This can be to learn from a process or to help someone carry out a particular task. Think of the IoT as being about networks, devices and data. Devices that are on closed private internet connections are able to communicate with other devices on other private internet connections because the IoT brings these networks together. The IoT creates a connected world.

Data collection, analysis and manipulation

We are constantly surrounded by sensors that detect, measure and send data in some form or another. When devices and technology are connected over the IoT, they can monitor and measure data in real time. This data can be invaluable to save time, energy and money.

- ▶ **Edge computing** – edge computing is all around us. Think of wearable smart devices worn on the wrist, to computers controlling the flow of intersection traffic on motorways. Other examples are the safety monitoring of oil rigs, drone-enabled crop management and smart utility grid analysis. Edge computing relates to the processing of data that can occur in many different ways and in a variety of settings. To put it simply, edge computing is the capturing, processing and analysing of data near to where it is located. Due to the increase in the amount of data due to the growth of IoT, edge computing helps to reduce bandwidth and latency issues by minimising the distance of the communications between the clients (devices) and the server. For ‘edge’ devices to be smart, they need to be able to process the data they collect, share real-time information and, if necessary, take action. Edge computing requires edge devices that can handle data as described without having to have the data transmitted to another server environment.
- ▶ **Sensors** – Sensors are a form of input device to a computer system. A simple classification of sensors is that they are either **active** or **passive sensors**. A sensor can also be classified by the detection methodology

Key terms

Hyperlink: can be displayed as an icon, a graphic or text, and links to another file or object. The World Wide Web is comprised of trillions of hyperlinks that link pages and files to one another. A hyperlink is usually underlined and displayed in blue.

Uniform Resource Identifier (URI): this is also called the internet address, web address or Uniform Resource Locator (URL) (which is a form of URI). These terms are standardised naming conventions used to address documents accessible over the internet and intranet. An example of a URL is <https://www.ncfe.org.uk>, the URL for the NCFE website.

Search engine: this is software that is accessed via the internet which searches a database of information according to the query that has been input by the user. The search engine will provide a list of results that best match what the user is trying to find based on the search criteria that was entered. There are many different search engines available, for example Google, Yahoo, Bing and Ask.

Active sensors: sensors requiring an external signal or a power signal.

Passive sensors: do not require external power signals and directly generate an output response.

that it uses, for example electrical or chemical. They can also be classified per the way that they work with data: **analogue sensors** and **digital sensors**.

Types:

- ▶ temperature sensor
- ▶ humidity sensor
- ▶ pressure sensor
- ▶ seismometer
- ▶ breathalyzer
- ▶ smoke detector
- ▶ touch sensor
- ▶ vehicle speed sensor.

Network utilisation

As the number of IoT devices continues to grow, the network infrastructure that supports them must also adapt to the changes. Network infrastructures must be designed so that they can accommodate the traffic they carry. Networks have to be able to support voice, video and data, all of which have specific characteristics and requirements. The majority of IoT devices send and receive small amounts of data. The majority of the traffic is in the form of transmissions sent periodically, consisting of several lines of text containing things such as coordinates, switch positions, sensor measurements or just simple commands. This requires very low bandwidths. The main challenge for IoT is the number of connected devices as IoT applications can require thousands of local area network segments on a single network. It is not the bandwidth that presents the problem, it is as the data moves through the layers. This puts a huge strain on network resources. It is much easier to design a new network from the start to accommodate IoT traffic patterns. An existing network infrastructure must be modified, and this can become very expensive.

Use within an industrial context

This is commonly referred to as the Industrial Internet of Things (IIoT) and is an extension to the use of IoT in industrial sectors. IIoT focuses strongly on **machine-to-machine (M2M)** communication, big data and **machine learning**. It enables industries to improve the efficiency and reliability of their operations. IIoT can include medical devices, robotics and software-defined production processes. Therefore, IIoT is the linking of information technology (IT) and operation technology (OT). OT is the networking of the operational processes and **industrial control systems (ICS)**. This includes **human machine interfaces (HMIs)**, **supervisory control and data acquisition systems (SCADA)**, **distributed control systems (DCS)** and **programmable logic controllers (PLC)**.

Key terms

Analogue sensors: produce a continuous output signal relating to the quantity being measured.

Digital sensors: work with discrete digital data. The digital data is used for conversion and transmission.

Machine-to-machine (M2M): any technology that enables networked devices to exchange information and perform actions without the manual assistance of humans. It supports the communication between systems enabling them to make autonomous decisions.

Machine Learning: a form of AI (Artificial Intelligence) that learns from data by identifying patterns and makes decisions with minimal human intervention.

Industrial control systems (ICS): an important aspect of the operation technology sector. These are systems that are used to monitor and control industry processes, for example oil refinery cracking towers or power consumption on electricity grids. They are extremely critical for all industry processes.

Human machine interface (HMI): a user interface that connects a person to a machine, system or device.

Supervisory control and data acquisition system (SCADA): system software and hardware that enables industrial organisations to control industrial processes locally or at remote locations. It facilitates the monitoring, gathering and processing of real-time data and directly interacts with devices, for example sensors, valves, motors and pumps, through the use of human–machine interface software. It also records the events that occur in a log file.

Distributed control system (DCS): this is a system of sensors, controllers and other associated computers and technologies that are distributed across an industrial plant, for example an oil refinery. Each of the elements of a DCS serves a unique purpose. This includes data acquisition, process control, data storage and graphical displays. A DCS communicates with a centralised computer system through the industrial plant's local area network and makes automated decisions based on real-time production trends.

Programmable logic controllers (PLC): industrial computer control systems that constantly monitor the state of input devices and make decisions that are based upon a custom program to control these devices. They have the ability to replicate and change operations or processes while simultaneously collecting and communicating important information.

The combination of OT and IT enables industries to have improved system integration with respect to automation and optimisation as well as an increased visibility of supply chains and logistics. Sensors and actuators are used to monitor and control physical infrastructures within industrial operations, as well as providing remote control and access. Sensors and other types of information sources aid the 'decision making' due to the accessibility of real-time data. Machines are able to adapt and take on automated tasks that were previously a challenge to industry.

The continuous transmission and capturing of data enables industries to identify errors and inefficiencies, for example in a supply chain, and address them promptly. This, in turn, improves the efficiency of operations. IIoT can also improve the use of assets, communication of potential areas of issues/process failure and prompt maintenance processes. All of these would be automated using IIoT. In addition, industries are able to gather and analyse vast amounts of data which will improve scalability and performance as well as provide a more cohesive approach by linking different departments together, for example production departments with logistics departments and so on.

Use within a smart city context

Smart cities use a wide range of IoT devices such as lights, meters and sensors to collect and analyse data. This data is then used to improve the city's infrastructure, public services, utilities and a lot more.

Below are some examples of how smart cities provide a better and more efficient lifestyle for the residents.

Smart utility meters

Smart meters are attached to or inside buildings and are connected to a smart energy grid. This enables the utility companies to effectively manage the flow of energy to their customers. They also enable the utility companies to track the energy consumption of their customers and provide more accurate billing, as opposed to estimated costs.

Smart transportation

This is the integration of modern technology and management strategies into transportation systems. Examples include:

- ▶ **Car navigation** – this is the use of satellite navigation (SatNav) to obtain positional data which is then correlated to the position of a vehicle on

a road. When directions are required, routes are calculated and instructions given to the driver.

- ▶ **Traffic signal control systems** – these respond to the surroundings and adjust the traffic conditions. An example could be where a car is travelling on the road and (fortunately for the driver), all traffic lights are on green as they pass through. This is because dynamic signalling has set all traffic lights to green to maintain the flow of the traffic. This is particularly useful at very busy times when a holdup can create traffic queues. Smart motorways use similar techniques to open and close lanes on a motorway with set speed restrictions.
- ▶ **Automatic number plate recognition** – this system uses character recognition on images to detect and read vehicle registration plates. This identifies the location of the vehicle for electronic toll collection, pay-per-mile systems and law enforcement.
- ▶ **Speed cameras** – detectors are embedded in the road or within radar technology to detect vehicles that are moving in excess of the legal speed limit. A digital image is taken and sent to the driver. It is used as a prevention method to encourage safer driving.

Smart waste management solutions

Waste management is a very costly and inefficient process. Smart waste management can monitor how full dustbins are at a given day and time. The information is sent to waste management companies who plan the most efficient route to collect the rubbish. Some cities have smart waste bins that can inform the users what items should be composted or recycled.

Smart air quality monitors

The air is full of dust, dirt, chemicals, pollen and numerous other such airborne particles. Smart air quality monitors detect what particles are present and inform the users of potential pollutants.

Use within a domestic context

A smart home is powered by the IoT. This means that instead of manually interacting with a device in order for an action to be carried out, a smart device can be controlled via an app or voice commands. Below are some examples of IoT devices within a smart home.

- ▶ **Lighting** – smart lighting has become very popular with the development of light bulbs such as the Philips Hue. The lights can be scheduled to turn

on and off depending on the time of day and many people use them to set their lights to go on and off at specified intervals when they are away from home. This gives the impression that the person is still in the house and can deter potential burglars. Voice control can also be used to control the lights, turning them on or off and increasing or decreasing their intensity.

- ▶ **Doors** – doors are becoming ‘smarter’ where they automatically open and close through sensors identifying the biometrics of the person in control. This can be extended to lights automatically coming on as you enter a room and/or building and switching off when the room or building is vacant.
- ▶ **Shutters** – windows can have shutters installed that will automatically open and close when the sun rises and when the sun sets.
- ▶ **Thermostats** – the temperature within the home can be controlled remotely through an app or by sensing the temperature of different locations within a house and comparing them with predefined temperature requirements. The smart thermostat will then switch the heating on or off. Some smart thermostats will automatically set to ‘eco’ temperatures when you are not at home but switch on at a predefined time or as you are nearing the house and ensure that the house is warm for your return.
- ▶ **Irrigation systems for gardens** – these devices can sense when there is dryness in the soil and trigger the irrigation system to switch on and water the garden.
- ▶ **General home routines** – these can include smart sockets that automatically turn the power to devices on and off. Smart alarms can use sensors to detect motion and some even play music to wake you up. Smart ovens, washing machines and kettles can turn on and off at predetermined times that are set using an app or the devices itself. Voice assistants such as Amazon’s ‘Alexa’ can control entire routines for lights, appliances, thermostats and alarms to name but a few.

Test yourself

- 1 Explain the term ‘edge computing’.
- 2 Describe two IoT concepts used within a ‘smart city’.
- 3 Explain the term ‘network utilisation’ in associated with the use of IoT devices.
- 4 Compare and contrast a PAN, a LAN and a MAN.
- 5 Explain the difference between proprietary and open-source operating systems.

5.3 The types and applications of protocols used to create networks and networking referencing models

Protocols

A protocol is a set of rules used for the formatting and processing of data. Network protocols are a common language used by computers. Networked computers may use different hardware and software but still need to be able to communicate with each other. The protocols enable this to happen. Unless there is a language that they can both speak, a person with Russian as their first language and another with French as their first language would not be able to communicate. The same concept applies to computers. If both computers use an Internet Protocol (IP), they will be able to communicate.

Web protocols (applied to web communication)

People tend to browse the internet using a web browser. The web browser enables a computer to communicate with web servers around the world and provides the user with access to the required information. Different web browsers have different ways of retrieving information, but they all use web communication protocols. These protocols are used to transfer information across the internet. For example, a web browser uses the protocols to request information from a web server. This is then displayed on the browser screen as text and images. The extent to which the users can interact with the information depends on the protocol being applied.

- ▶ **HyperText Transfer Protocol (HTTP)** – this is a commonly used web browser communication protocol and you would see ‘http://’ before the rest of the web address. It is a ‘client–server’ protocol where a user clicks a link on the web browser (known as the client) and the browser transmits a request over the internet to a web server that holds the website that has been requested. The server then transmits back the content of the website in the format of text and images which are displayed in the user’s web browser (client). It is an unsecure communications protocol. This means that the data it transmits back and forth between the browser and the server is unencrypted and can be intercepted by a third party.

- ▶ **HyperText Transfer Protocol Secure (HTTPS)** – this is like HTTP, but it is combined with a security protocol called **Secure Sockets Layer (SSL)/Transport Security Layer (TSL)**. This provides a secure client–server communication over unsecure networks such as the internet. Websites such as Amazon and online banking will use HTTPS protocols because they request financial information. You can always tell if a website is using a secure protocol because the web address will start with ‘https://’.

Mail protocols

These are methods that establish a communication channel between two computers, and emails are transmitted between them. This is how mail protocols work:

- ▶ Assume that there is going to be email communication between two computers (users), one being the sender of the email and the other being the receiver.
- ▶ An email is sent to a mail server.
- ▶ The mail server stores the email and allows the receiving device/computer to access it and download it.

There are several protocols that can be used and they differ in the way that the connections are established, and in the way users are allowed to access emails.

Simple Mail Transfer Protocol

This uses a process referred to as ‘store and forward’. Simple Mail Transfer Protocol (SMTP) sends your email across networks. It is used alongside a mail transfer agent (MTA) to ensure that the email gets to the right computer and email inbox. SMTP dictates how the email moves from the user’s computer’s MTA (e.g. Gmail, Outlook, etc.) to the MTA on another computer (the receiver, whose MTA may be Yahoo or ME@mycompany.com).

Using the ‘store and forward’ feature, the message moves in steps from the sending computer to its destination. At each step, the SMTP will continue to carry out its function. SMTP provides sets of codes that simplify the communication of email messages between email servers. Think of this as a form of shorthand that enables a server to break up sections of the message into categories the other server can understand. When sent, the email is converted into strings of text that are separated by code words (or numbers). These identify the purpose of each of the sections.

SMTP can only transfer text; it cannot handle fonts, graphics, attachments and so on. However, Multipurpose Internet Mail Extensions (MIME) were developed that encoded all non-text content into plain text. Once transformed in this way, SMTP is persuaded to transfer the data.

Post Office Protocol

Post Office Protocol (POP) is used to retrieve emails from a remote mail server over a Transmission Control Protocol/Internet Protocol (TCP/IP) connection. It is a popular email protocol and is simple to configure, operate and maintain. Internet Service Providers use POP version 3 (POP3) to receive and hold emails for their subscribers (customers). The subscribers will use email client software to check their mailbox on a remote server and download their emails. Once downloaded, the emails are usually deleted from the mail server and are therefore only accessible on the computer/device they were downloaded onto (although there are some email clients which can be configured so that emails are copied or saved on the server for a period of time). Because POP3 is a basic method for storing and receiving emails, it is compatible with any email program that has been configured to host the protocol.

Internet Message Access Protocol

This allows the user to access their email on any device wherever they are. When reading an email using Internet Message Access Protocol (IMAP), the email is not downloaded or stored onto the computer or device. It is being read from the email service. This enables users to check for emails on different devices such as a smartphone, tablet, computer, laptop and so on. IMAP only downloads when the email is clicked on and attachments are not automatically downloaded. The attachments must be selected before they are downloaded.

Key terms

Secure Sockets Layer (SSL): standard technology used to keep an internet connection secure. Data that is transmitted between the user and the website (or between two systems) is encrypted and therefore impossible to read; this prevents unauthorised people from reading sensitive and personal information.

Transport Security Layer (TSL): an updated and more secure version of Secure Sockets Layer.

Routing protocols

Routing protocols learn available routes that exist on an enterprise network and build routing tables and make routing decisions. They are a set of defined rules that are used by routers to communicate between the source and destination. Routing protocols help to specify the way the routers communicate with each other. This enables the network to select routes between any two **nodes** on a computer network.

Routing Information Protocol

Routing Information Protocol (RIP) belongs to a family of internet protocols. It is an Interior Gateway Protocol (IGP) that is designed to distribute routing information within an **autonomous system (AS)**. The routers exchange network reachability information with their nearest neighbours. They communicate with each other the sets of address prefixes (sets of destination) that they can reach and the net address that the data should be sent to in order to reach those destinations. This is a dynamic routing protocol using hop counts (metric maximum 16 hops) to find the best path.

Open Shortest Path First

This is a method of finding the shortest path from one router to another in a local area network. As long as the network is IP-based the Open Shortest Path First (OSPF) will use its algorithm to calculate the most efficient way for the data to be transmitted. If there are a number of routers on a network, the OSPF will build a table (known as a topography) of the router connections. When the data is sent from one location to another, the OSPF algorithm will compare the available options and select the most efficient route for the data to be sent. This can mitigate against unnecessary delays in data transmission. This is a link-state routing protocol that exchanges topology information with its nearest neighbours.

Networking referencing models

Open Systems Interconnection model

The OSI model was developed by the International Organization for Standardization (ISO) in 1977. It was designed to show how a network system communicates and operates.

The ISO is covered in section 8.3, p. 207.

The OSI model divides the complex task of networking into layers. This allows someone to work on the design and debugging of one layer without affecting the others.

There are seven layers with the OSI model stack. They are split into two groups:

- ▶ Upper layers.
- ▶ Lower layers.

7	Application Network protocols to application	Upper layers
6	Presentation Data representation and encryption	
5	Session Interhost communication	

▲ **Table 5.4** OSI model stack (upper layers)

4	Transport End-to-end connections and reliability	Lower layers
3	Network Logical addressing	
2	Data link Physical addressing	
1	Physical Media, signal and binary transmission	

▲ **Table 5.5** OSI model stack (lower layers)

Each layer contains a different group of tasks required for a network to communicate. It must be remembered, however, that not all network systems implement layers using this structure.

The software in the upper layers performs application-specific functions, for example data formatting, encryption and connection management. Upper layer technologies include HTTP (Hypertext Transfer Protocol) and SSL (Secure Sockets Layer).

Key terms

Note: any physical device within a network that is able to send, receive and/or forward information. A computer is a node if connected to a network.

Autonomous system (AS): a large network or group of networks that have a unified routing policy. Every computer or device that connects to the internet is connected to an AS. This is because the internet is a network of networks.

The lower layers provide functions such as routing, addressing and flow control. Lower-level technologies include TCP (Transfer Control Protocol), IP (Internet Protocol) and Ethernet.

The OSI model simplifies how network protocols are designed. It was designed to ensure that different equipment, such as adapters, hubs and routers, are compatible regardless of which manufacturer builds them.

Application layer

This is the interface between the end-user and the network and provides support services to applications requiring network services. The most utilised service is file transfer because different file systems often use entirely different naming conventions and syntax data. The application layer must overcome these issues. The types of applications that reside in this layer include Google Chrome and Mozilla Firefox.

The protocols associated with this layer include:

- ▶ FTP (File Transfer Protocol)
- ▶ WWW (World Wide Web)
- ▶ HTTP
- ▶ NFS (Network File System)
- ▶ POP3
- ▶ SNMP
- ▶ SMTP

Presentation layer

This layer translates data into suitable formats so that it can be read (or understood) by the application. The presentation layer supports data compression, provides security through data encryption and determines the structure of the data. It communicates through gateways and application interfaces and uses services such as FTP and NFS.

The protocols associated with this layer include:

- ▶ JPEG
- ▶ MIDI (Musical Instrument Digital Interface)
- ▶ MPEG
- ▶ ASCH
- ▶ SSL
- ▶ TLS

Session layer

This layer allows applications running on different computers to communicate with each other. The connection is commonly known as the 'session'. The session-layer process is as follows:

- ▶ Establish the session
- ▶ Manage data transfer
- ▶ Tear down the session

The session layer provides a synchronised service where checkpoints are inserted into the data stream. If there is a problem during transmission, only the data transferred after the last checkpoint is resent.

It also manages the 'dialogue' between the computers on the network. An example of this is half duplex mode, this is when it is responsible for determining whose turn it is to transmit over the network.

This layer communicates through gateways and application interfaces and uses services such as TCP.

The protocols associated with this layer include:

- ▶ NFS
- ▶ SQL (Structured Query Language)
- ▶ RPC (Remote Procedure Call)
- ▶ NetBIOS
- ▶ SAP

Transport layer

This layer is responsible for ensuring reliable data delivery so that packets (formatted units of data) arrive error free and without loss. It uses messages that inform the sender that the data was successfully received. If data is not delivered, then the message received from the sender will result in a retransmission of the data. If the data received is in a damaged state, the message known as NACK (negative acknowledgement) is sent and retransmission is forced.

The transport layer provides a service for connection-mode transmissions and connectionless-mode transmissions. With connection-mode transmissions, a message is sent or received in packets which then need to be reconstructed into a complete message.

This layer communicates through gateway services, routers and brouters.

The protocols associated with this layer include:

- ▶ TCP
- ▶ UDP (User Datagram Protocol)
- ▶ SPX (Sequenced Packet Exchange)
- ▶ NetBEUI (NetBIOS Extended User Interface)

Network layer

This layer is responsible for moving data around a network of networks, commonly known as the internet. It transfers information between networks

by examining the logical network address and routing the packets using routers. The path or route taken to the destination network address is determined either statically or dynamically. The packet moves one step at a time through the internet to the target network. The hardware address is then used to move the packet to the target node. This process requires each logically separate network to have a unique network address. The Internet Protocol (IP) addresses make it easier to set up a network and connect to other networks.

In order to make it easier to manage the network and control the flow of packets, the network layer addressing is separated into smaller parts known as subnets. It is the subnet portion of the IP addressing that is used to route traffic between different networks. Routers must be configured specifically for the networks or subnets that will be connected to them.

Other functions carried out by the network layer include:

- ▶ Error control – detection of transmission errors and retransmission of correct data.
- ▶ Flow control – regulating the speed of data transfer.
- ▶ Fragmenting packets – breaking down packets into smaller chunks if required. The receiving network layer is responsible for rebuilding the packets.

This layer communicates through gateway services, routers and brouters.

The protocols commonly associated with this layer include:

- ▶ IP
- ▶ IPX (IP Exchange)
- ▶ RIP (Routing Information Protocol)
- ▶ ARP (Address Resolution Protocol)
- ▶ ICMP (Internet Control Message Protocol)
- ▶ RARP (Reverse Address Resolution Protocol)
- ▶ EGP (Exterior Gateway Protocol)

Data link layer

The data link layer is responsible for transferring data between devices. It responds to requests from the network layer above it and issues requests to the physical layer below it.

It is responsible for:

- ▶ Encoding bits into packets prior to submission and decoding the packets back into bits at the destination.
- ▶ The logical link control (LLC), media access control (MAC), hardware addressing, error detection and handling.

The data link layer is divided into two sublayers: LLC and MAC. The former controls how computers on the network gain access to the data and obtain permission to transmit it; the latter controls packet synchronisation, flow control and error checking.

Data link layer processing is faster than network layer processing because less analysis of the packet is required.

This layer communicates through switches, bridges and intelligent hubs.

The protocols associated with this layer include:

- ▶ HDLC (High-level Data Link Control)
- ▶ LLC
- ▶ SLIP (Serial Line Internet Protocol)
- ▶ PPP (Point-to-Point Protocol)

Physical layer

This is responsible for the transmission of data over network communication media. The physical layer includes the following:

- ▶ The network medium.
- ▶ Physical network topologies.
- ▶ The network card.
- ▶ The process of transmitting and receiving signals from the network medium including bit transmission, encoding and timing rules.

The four general functions of this layer are:

- ▶ Definitions of hardware specifications – each piece of hardware on a network will have a specification, for example the maximum length of cable, EMI protection or width of cable.
- ▶ Data transmission and reception – regardless of the network medium used, there has to be equipment that actually transmits the signal and equipment that receives the signal; for example optical transmission lines use equipment which can produce and receive pulses of light, such as amplifiers and repeaters.
- ▶ Encoding and signalling – this is a very important part of the physical layer and can be quite complicated.
- ▶ Topology and physical network design – the physical layout and structure of the network. k.

This layer communicates through repeaters, hubs, switches, cables, connectors, transmitters, receivers and multiplexers.

The table on the next page provides a summary of the layers, their purpose and their location within the OSI seven-layer model.

Layer no.	Layer title	Purpose	Location
7	Application Supports the applications and end user processes. It is not an application itself.	Messages and packets <ul style="list-style-type: none"> Identification of communicators (Is there anybody out there?) Assessment of network capacity (Will the network let me contact them now?) Data syntax (Can we understand the message?) User authentication and privacy (How do you know it is me?) 	Upper/host Application-specific function: <ul style="list-style-type: none"> Formatting Encryption Connection management
6	Presentation Usually part of the operating system	Packets Converts data into a suitable format so it can be understood by the application. It also: <ul style="list-style-type: none"> Supports data compression and encryption Decides data structure Communicates through gateways and application interfaces. 	
5	Session Allows applications running on different computers to communicate with each other	Packets <ul style="list-style-type: none"> Sets up the communication link between applications. Manages the link, e.g. if using half duplex, this layer determines whose turn it is to transmit data Terminates the link Authenticates and reconnects link after an interruption 	
4	Transport The postal service, ensuring that data packets arrive error free and without loss	Datagrams, segments and packets <ul style="list-style-type: none"> Puts the data into the correct packet format Delivers the packet Checks the packet has arrived Retransmit the packet if not received If data packet is damaged, arranges for resubmission 	Lower/media Provides: <ul style="list-style-type: none"> Routing Addressing Flow control
3	Network Transfers data around between the internet	Datagrams and packets <ul style="list-style-type: none"> Examines the logical network address Converts it into physical machine addresses on the receiving computer and reverses it when a message is sent back Routes packet using routers Detects transmission errors (error control) Retransmits correct data Regulates the speed of data transfer (flow control) If the packet is too large for a network on the route to handle, it is fragmented and reassembled by the receiving device (fragmenting packets) 	

2	Datalink Responsible for transferring data between devices. It responds to requests from the network layer above and the issues requests to the physical layer below	Bits and packets <ul style="list-style-type: none">• Encodes bits into packets prior to submission• Decodes packets back into bits Divided into two sublayers: <ul style="list-style-type: none">• Media access control (MAC) layer which controls how computers on the network gain access to the data and object permission to transmit it• Logical link control (LLC) layer controls packet synchronisation, flow control and error checking	
1	Physical Includes: <ul style="list-style-type: none">• Network medium• Physical network topologies• Network card• Process of transmitting and receiving signals from the network medium	Four generation functions: <ul style="list-style-type: none">• Definition of the hardware specification, e.g. maximum length of cable, width of cable, physical connectors, voltages• Data transmission and reception, e.g. amplifiers and repeaters• Encoding and signalling• Topology and physical network design, physical layout and structure of network	

Activity

Complete the table below by providing the full name of some of the protocols relevant to each of the OSI layers and a brief description of their role. The first part is completed for you as an example.

OSI layer	Protocol	Full protocol name	Description
Application	FTP	File transfer protocol	The simplest method for sending and receiving files over the internet, FTP splits the files into a number of segments and gives each one a reference number so that the...
	TELNET		
	WWW		
	HTTP		
	NFS		
	SMTP		
Presentation	JPEG		
	MIDI		
	MPEG		
	SSL		
Session	NFS		
	SQL		
	RPC		
Transport	TCP		
	UDP		
	SPX		
	NetBEUI		

Network	IP		
	IPX		
	RIP		
	ARP		
	ICMP		
	RARP		
	EGP		
	DLC		
Datalink	HDLC		
	LLC		
	SLIP		
	PPP		
Physical			

How data is transferred between network devices using the OSI seven-layer model

- ▶ Data is transmitted by the user from the digital device e.g. computer to the application layer.
- ▶ Data is then passed down through the layers to the physical layer. This is the only layer that is able to communicate with other devices and networks.
- ▶ The data is sent along the physical layer to the receiving device e.g. receiving computer.
- ▶ The data then works its way up through the layers to the receiving computer for access by the user receiving the data.

Application layer

This provides applications with the means to access the services of the other layers and defines the protocols used by the applications to exchange data. The most widely known protocols are used for the exchange of user information are as follows:

- ▶ HTTP – Hypertext Transfer Protocol (e.g. web pages).
- ▶ FTP – File Transfer Protocol (e.g. interactive file transfer).
- ▶ TELNET – used for logging on remotely to networks.
- ▶ SMTP – Simple Mail Transfer Protocol (e.g. transfer of email messages and any attachments).

The following protocols are used to assist in the management and use of TCP/IP networks:

- ▶ DNS – Domain Name System (for example linking a host name to an IP address).
- ▶ RIP – Routing Information Protocol (used for example by routers to exchange routing information on an IP network).

- ▶ SNMP – Simple Network Management Protocol (used for example to collect and exchange network management information).

Transport layer

This layer is responsible for providing the application layer with session and datagram communication services. The main protocols are:

- ▶ TCP – Transmission Control Protocol. This provides a one-to-one communication services and is responsible for the:
 - establishment of the TCP connection
 - sequences and acknowledgement of packets sent
 - recovery of packets lost during transmission.
- ▶ UDP – User Datagram Protocol. This provides a one-to-one or one-to-many communication service which is connectionless and unreliable. It is used when the amount of data to be transferred would fit into a single packet. It is used by network applications that want to save processing time.

Internet layer

This layer is responsible for the addressing, packaging and routing functions. The main protocols are:

- ▶ IP – Internet Protocol. Responsible for the IP addressing, routing and the fragmentation and re-assembly of packets.
- ▶ ARP – Address Resolution Protocol. It ensures that the address of the internet layer can be linked to the network interface layer address, for example the hardware address.

- ▶ ICMP – Internet Control Message Protocol provides the diagnostic functions and reporting errors when delivery of IP packets is unsuccessful.
- ▶ IGMP – Internet Group Management Protocol is responsible for the management of IP groups.

Network interface layer

This layer is responsible for placing TCP/IP packets on the network medium and receiving them off the network medium. TCP/IP can be used to connect different network types, for example LAN technologies such as token ring and WAN technologies such as frame relay.

Transmission Control Protocol/Internet Protocol

The Transmission Control Protocol/Internet Protocol (TCP/IP) model is a different model than the OSI model. It contains four layers instead of seven. It is the protocol used for communication between computers on the internet. It defines how devices should be connected to the internet and how data is transmitted between them.

The four layers of TCP/IP are as follows:

- ▶ Application layer
- ▶ Transport layer
- ▶ Internet layer
- ▶ Network interface layer.

Layer no.	Layer title	Purpose
1	Application	Provides applications with the means to access the services of the other layers and defines the protocols used by the applications to exchange data
2	Host–host transport	Provides the application layer with session and datagram communication services
3	Internet	Provides addressing, packaging and routing functions
4	Network interface	Places TCP/IP packages on the network medium and receives them on the network medium

▲ Table 5.7 TCP/IP layers

Data that is sent over a network (including the internet) is referred to as packets. Large packets of data are broken down into smaller datagrams. On reaching their final destination, the datagrams are reassembled as a single file or block of **contiguous data**. The term ‘packet’ and ‘datagram’ are similar in meaning. The protocol UDP uses the term datagram.

Data packets consists of a header, a payload and a trailer.

Header – this contains the instructions about the data and has several parts:

- ▶ originating address – the IP address of the sender of the data packet
- ▶ destination address – the IP address of the receiver of the data packet
- ▶ internet protocol – defining the type of packet being transmitted e.g. email, webpage, video etc
- ▶ the size of the header and the payload
- ▶ the number of **hops** – this is the number of routers that the packet will pass through on its journey
- ▶ **Time to Live (TTL)** – the amount of time it exists within the network before being discarded by the router
- ▶ flags – used to inform the router whether the packet can be divided into datagrams
- ▶ checksum – used to detect any errors during transmission
- ▶ packet number – the number of the packet where there is a sequence of packets.

Packet switching

This is where the data packet is divided into smaller data packets and transmitted individually across the network as opposed to transmitting one large data packet. It is used to reduce the chances of lost packets and facilitates the resending of data packets as well as reducing transmission latency. The packets are not necessarily routed along the same path within the network. This results in the packets arriving at their destination in no particular order. It is the responsibility of the destination to reconstruct the packets into an appropriate order to be able to retrieve the original message.

Key terms

Contiguous data: data that is stored in a collection of adjacent locations.

Time to live (TTL): the amount of time or ‘hops’ that a packet is set to exist inside a network before being discarded by the router. TTL is also used in Content Delivery Network (CDN) caching and Domain Name System (DNS) caching.

Hops: refers to the number of routers that a packet passes through from its source to its destination. A hop can also be counted when a packet passes through other hardware on a network such as switches, access points and repeaters. It is dependent on what role the devices have on the network and their configuration.

Test yourself

- 1 Explain the term HyperText Transfer Protocol Secure.
- 2 Explain the application layer of the TCP/IP model.
- 3 Discuss the OSI model. Include: what it is, what it does and how it is used for troubleshooting.
- 4 Explain the purpose of RIP.
- 5 Describe the differences between POP2 and IMAP.

Layer	Protocol suite					
Application	Telnet	FTP	SMTP	DNS	RIP	NMP
Host–host transport	TCP			UPD		
Internet	IP			IGMP	ICMP	
	ARP					
Network interface	Ethernet	Token ring		Frame relay	ATM	

▲ Table 5.8 TCP/IP layers and associated protocols

TCP/IP Model	OSI Model
Has four layers.	Has seven layers.
Uses a horizontal approach.	Uses a vertical approach.
Protocol orientated approach.	Based on the functionalities of the layers.
Combines the presentation and session layers into its application layer (so the application layer contains the application, presentation and session layers that are separate layers in the OSI model).	Differentiates between interfaces, services and protocols.
Combines the data link and physical layers and is referred to as the network layer (sometimes referred to as Network Access Layer).	Acts as an interaction gateway between the network and end-user.
Only connectionless transmission is available in the network layer. Connection and connectionless transmission is available in the transport layer.	In the network layer, connection and connectionless transmissions are provided. It only provides connection transmission in the transport layer.

▲ Table 5.9 The differences between OSI and TCP/IP models

5.4 The components and benefits of virtual computing systems

Components

Virtual machines

Virtualisation is technology that enables a single, physical hardware system to be separated into multiple simulated environments or dedicated resources. Software known as a **hypervisor** connects to the hardware and facilitates the splitting of one system into separate and distinct environments referred to as virtual machines (VMs). The VMs rely on the hypervisor to separate the resources of the machine from the hardware and distribute them. The hardware that is equipped with a hypervisor is called the host and the VMs are called guests. The VMs (guests) treat the resources such as CPU, memory and storage as a

pool of resources. These resources are controlled by operators so that the VMs receive only the resources they need and when they need them.

Key terms

Payload: this is the body of the data packet and contains the actual data that is being sent/received.

Trailer: this is sometimes referred to as the footer and is used to inform the receiving device that it is the end of the packet. The trailer also includes error checking, the most commonly used is the Cyclic Redundancy Check (CRC). The CRC will add up all the 1s in the payload and stores the results as a hexadecimal. On receiving the data packet, the receiving device will add up the number of 1s in the payload and compare it with the hexadecimal value stored in the trailer. When the two values match it is confirmation that there has been no error during transmission. If, however, the two values do not match, then the receiving device sends a request to the sending device asking it to resend the packet.

Examples of types of virtualisation include:

- ▶ **Data virtualisation** – enables organisations to treat data as a dynamic supply. This provides processing functions that can bring data together from multiple sources, transform data and accommodate new data sources.
 - ▶ **Desktop virtualisation** – allows an organisation to install multiple operating systems onto a single machine. It allows a central administrator (or an automated administrator tool) to install simulated desktop environments on very large quantities of physical machines simultaneously. Unlike the traditional desktop environments, they are physically installed, configured and updated on each machine. Desktop virtualisation allows the administrators to carry out mass configurations, updates and security checks on all virtual desktops.
 - ▶ **Server virtualisation** – you previously learned that servers are computers which are designed and configured to process high volumes of specific tasks. Virtualising a server provides it with the ability to perform even more functions and involves partitioning. This enables it to serve multiple functions.
 - ▶ **Operating system virtualisation** – this allows an organisation to run multiple operating systems side by side, for example Windows and Linux. This allows an organisation to make different operating systems accessible to different computers. This reduces the hardware costs and increases security as all virtual instances can be isolated and monitored. It also reduces the time required for updates to be installed.
 - ▶ **Network function virtualisation** – separates the network's key functions, for example file sharing and IP configuration, so that they can be distributed among different environments. When software functions are independent of the physical machines, functions can be packaged together to form a new network and assigned to a particular environment. It reduces the number of physical components required to create multiple and independent networks.
- Key features of virtualisation include:
- ▶ **Increased security** – a virtual machine manager can control and filter the activity of a guest's programs. This can mitigate the risk of harmful operations being carried out. Any resources exposed by the host can be hidden or protected from the guest.
 - ▶ **Managed execution** – the execution of sharing, aggregation, emulation and isolation can all be managed from a central virtual server.
 - ▶ **Sharing** – this is the creation of separate computing environments within the same host. It is used to reduce the number of active servers and limits power consumption.
 - ▶ **Aggregation** – as well as sharing physical resources among numerous guests, virtualisation allows aggregation. This is where a group of hosts are combined and presented to guests as a single virtual host. This is made possible through cluster management software.
 - ▶ **Emulation** – guest programs are executed in an environment that is controlled by a virtualisation layer. This is basically a program. In addition, a totally different environment with respect to the host can be emulated. This allows the execution of guest programs that require specific characteristics which are not available on the physical host machine.
 - ▶ **Isolation** – virtualisation provides guests with a separate environment, regardless of whether this is an operation system, application or other entity. The guest program interacts with an abstraction layer which provides access to the underlying resources. This allows the VM to filter the activities of the guests and mitigate the risk of harmful operations against the host. It also facilitates performance tuning, where the performance of a guest can be monitored and controlled through the fine-tuning of the properties of the resources available through the virtual environment. It therefore supports and implements a quality-of-service (QoS) infrastructure.
 - ▶ **Portability** – this differs with specific types of virtualisation.
 - ▶ With a hardware virtualisation environment, the guest is packaged into a virtual image. This means that it can be safely moved and executed on top of different virtual machines.
 - ▶ With programming-level virtualisation, the binary code representing application components can run without any recompilation on any installation of the corresponding virtual machine.

Clients

Virtual client computing (VCC) provides desktop virtualisation solutions that overcome the limitations of the conventional desktop environment. A VCC is operated centrally on a server and then accessed on a client device. A permanent network connection is not required for the operation of a client-based virtual machine. VCC decreases the overall risk and work effort as it eliminates difficulties and increases flexibility, as well as reducing costs.

VCC software separates all of the components of the system, for example operating systems, hardware, software applications, and facilitates the movement of the user applications and data from the user's machine to the data centre. This makes it more efficient, cost-effective and secure to manage client devices.

Virtual switch

This is a software program that allows one VM to connect with another. The virtual switch directs the communication on the network by reviewing the **packets** before passing them on. Sometimes the virtual switches are embedded into virtualisation software or even included in a server's hardware as part of its **firmware**.

Virtual switches work in a similar way to physical hardware switches, for example Ethernet switches, but they do not have some of the advanced functionality. The role of the virtual switch is to establish a connection between the virtual and physical network. The virtual switch detects which of the virtual machines are connected to each of its virtual ports. It uses this information to forward traffic to the correct virtual machines. Virtual switches are connected to physical hardware switches using **Ethernet adapters** to join virtual networks with physical networks.

Virtual router

Sometimes referred to as a vRouter, this is a software function that functions in the same way as a hardware-based Internet Protocol router. Virtual routing is a form of network functions virtualisation (NFV) where the functions of hardware-based network devices are converted to software and can run on standard commercial off-the-shelf (COTS) hardware. This lowers hardware costs.

Virtual routers are usually supported by two physical (hardware) routers. One router will carry out the normal routing functions while the other will facilitate redundancy in case of a failure of the system. Any

virtual router that is created is identified by a unique virtual router identified (VRID). The last byte of the address is the virtual router identified. Every virtual router that is in a network has a different number. Only one of the physical routers use a virtual router's address at any given time.

Servers

A virtual server is a server that is in an off-site data centre. Its resources are shared by numerous users, each of whom have control over it. One server is converted into several virtual machines each of which run their own operating system. The virtual machines can take full advantage of using the server's processing power and this enables the users (organisations) to share the cost of the equipment. Virtual servers are more efficient.

There are different types of server virtualisation:

- ▶ **Full virtualisation** – this uses software known as a hypervisor and they are based on the host–guest setup/standard. Each hypervisor can run thousands of virtual servers simultaneously.
- ▶ **Paravirtual machine (PVM)** – this is similar to full virtualisation and is also based on the host/guest standard. It can run multiple operating systems.
- ▶ **Operating system (OS) level** – this is not based on the host/guest standard. This means that the guests must use the same OS as the administrator/host. In addition, partitions are completely separated from one another which means that any problems cannot affect any other areas/guests.

Key terms

Packets: a small segment of a larger message. Any data sent over computer networks is divided into packets. They are combined back into the larger message by the computer/device that receives them.

Firmware: a small piece of software that makes hardware work as intended. Firmware consists of programs that are used to make devices work. Without firmware, many electronic devices would not work at all.

Ethernet adapter: also referred to as a Network Interface Card, it plugs into a slot on the motherboard. It enables the computer to access the network. Many NICs are now built into the chipsets on the motherboards of PCs and laptops as opposed to being a physical card.

Advantages of server virtualisation include:

- ▶ **Reduction in costs** – when a physical server is partitioned into several virtual machines, they can be configured to deploy, operate and manage several operating systems at any given time. This means that money does not have to be spent on buying several physical servers.
- ▶ **Reduction in the number of physical servers** – this means that it saves space as a business does not have to try and allocate space for several physical servers.
- ▶ **Independent user environments** – everything is kept separately, and this means that applications and processes can be run, for example software testing can be carried out by software developers on a virtual server, and not have an impact on any other processes running.
- ▶ **Reduction in power consumption** – as there is a reduction in the number of physical servers required by an organisation, this reduces the power consumption. This is particularly important with the emphasis on '**Green IT**'.

Hypervisor

This is software that creates and runs VMs. A hypervisor, which is sometimes referred to as a virtual machine monitor (VMM), isolates the hypervisor operating system and resources from the virtual machines. This allows it to create and manage the VMs. It handles the requests between the physical and virtual machines and manages and monitors the support for the virtual machines. As well as enabling multiple operating systems to share the same hardware, it allocates the portion of hardware required for each workload.

Type 1

A type 1 hypervisor directly runs on the physical hardware of the host machine and is therefore referred to as a bare-metal hypervisor. So, the basic structure of a type 1 hypervisor is:

- ▶ a physical server
- ▶ the hypervisor installed on the hardware
- ▶ several guest virtual machines.

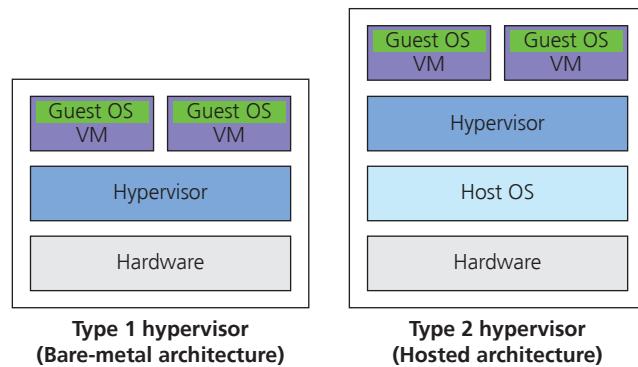
Because type 1 hypervisors are a very basic OS running virtual machines, the physical server can only be used for virtualisation and nothing else. A separate management console is required to perform activities such as creation and migration of the VMs. The management console, therefore, is used to manage the operations of the virtual environment. Examples of type 1 include Microsoft Hyper-V and VMware ESXi.

Type 2

This hypervisor software runs the operating system on the physical host machine and is often referred to as a 'hosted hypervisor'. The hypervisor is hosted on the OS and runs as a separate layer of software to facilitate virtualisation. The structure of the type 2 hypervisor is:

- ▶ a physical machine
- ▶ OS installed on the physical server hardware (e.g. operating systems like Windows, Linux and macOS)
- ▶ virtual machine instances/guest VMs.

Type 2 hypervisors are used where there are a small number of servers with no requirement for a separate management console to set up and manage the virtual machines. The management operations are done on the server on which the hypervisor is hosted. The hypervisor is viewed as an application on the host system.



▲ **Figure 5.1** Configuration of a type 1 and a type 2 hypervisor

Benefits of virtual computing systems

More cost-effective in larger digital environments

The software is separate from the physical host computer; therefore, organisations can run multiple operating systems on one single piece of hardware. This will save the organisation time, physical space and

Key term

Green IT: this is related to the practice of environmentally sustainable computing. The aim is to minimise the negative impact of IT operations on the environment by improving the design, manufacture, operation and disposal of computers and computer-related products in a more environmentally friendly way.

management costs. VMs can also support legacy apps and this can reduce or even eliminate the requirement and cost of migrating an older app to a newer and updated version and/or operating system.

Issues created through malware can also cause problems within a standard computing system environment and can have an impact on the running of a business (time is money). Software used by a VM cannot be 'tampered with' as it is stored on a host computer. Therefore, malicious software and code cannot spread so easily.

There is also a reduction in hardware costs as the organisation does not have to purchase, install and configure several servers, but can access one server that has been configured as multiple environments.

Easier to manage and maintain larger environments

The execution of sharing, aggregation, emulation and isolation can all be managed from a central virtual server. The portability differs with specific types of virtualisation.

- ▶ With a hardware virtualisation environment, the guest is packaged into a virtual image. This means that it can be safely moved and executed on top of different virtual machines.
- ▶ With programming-level virtualisation, the binary code representing application components can run without any recompilation on any installation of the corresponding virtual machine.

Resilient

Resilience refers to how well an application is able to recover when a resource or vital component is missing. When thinking about virtualisation of environments, one of the main considerations is what will happen to an application that is critical to the functioning of the business when the virtual machine becomes unavailable. This will include what would happen to any transactions that are currently being processed and the effect on the experience of the end user. As well as sharing physical resources among numerous guests, virtualisation allows aggregation. This is where a group of hosts are combined and presented to guests as a single virtual host. This is made possible through cluster management software. Clustering is the creation of separate computing environments with the same host. It reduces the number of active servers that is required.

Environmental

Virtual computing systems reduce the space required to maintain and expand the IT capabilities of an organisation. As previously stated, the number of physical servers required by an organisation is reduced and therefore this reduces power consumption. The creation of separate computing environments with the same host reduces the number of active servers and associated hardware, and limits the power consumption. Redundant software and hardware can also be minimised because the guest machines are accessing a virtual environment.

Disaster recovery options

Many disasters can have a major impact on an organisation, for example loss of corporate network access or loss of corporate database systems.

Virtualisation streamlines the disaster recovery process by replicating the servers off-site (usually in the cloud). VMs are independent of the underlying hardware, and the same physical servers that are off-site are not required to support a secondary recovery site. Should a disaster occur, the system can be back online in just a few minutes with an easy and cost-effective backup and disaster recovery solution.

Efficient testing environments

The testing of hardware and software can be carried out using a separate virtual server environment which will not have an impact on any live operations on other areas of the virtual site. It is much easier to have a virtual server to carry out any testing to mitigate against any potential issues arising which may impact on the main processes being carried out by the end users.

Education and training platform

The use of virtual learning infrastructures can be very beneficial for the education and training sector. It can help to reduce the time and effort required to manage the endpoint devices. Setting up an environment for a particular student/apprentice and then removing it can be a slow process that requires manual effort. Through using virtual desktops, an automated process can be implemented quickly. Virtualisation therefore ensures that there is faster device allocation and deletion.

In an educational environment, for example a school, college or university, students and the teachers/trainers can bring their own devices. This improves flexibility

and reduces organisational costs. In addition, operating systems, applications and other software do not need to be manually installed or updated. They can be carried out from a central location.

Security is always a big issue for any digital environment. Again, because the data relating to the students and the teaching staff is stored on a centralised database, the security of the data is greatly improved.

Virtualisation also means that the students can access their courses and homework remotely and can therefore submit their assignments from home or study remotely as required.

Test yourself

- 1 Explain the difference between type 1 and type 2 hypervisors.
- 2 Describe the term 'virtual router'.
- 3 Discuss the benefits to large environments of using virtual machines.
- 4 Explain three different types of virtualisation.
- 5 Describe the three types of virtual servers.

5.5 The types, services and benefits of cloud computing

Cloud computing refers to the outsourcing of IT services and infrastructure, making them accessible remotely via the internet. Utilising cloud computing models can boost productivity and provide organisations with a competitive edge. There are a number of different types of cloud delivery models providing a variety of cloud solutions, depending on what an organisation wants to outsource.

There are four different categories of cloud models. These are:

- ▶ Public – these are used by a range of end-users ranging from large organisations to an individual. They can be accessed through a digital device with an internet connection. To be able to access and use a public cloud users must pay a subscription or on a pay-to-use basis. A public cloud is usually hosted by one cloud vendor. Examples of a public cloud include Amazon Web Service (AWS), IBM Cloud or Google Cloud.
- ▶ Private – these are used by a specific organisation and can be hosted on site premises or remotely through virtualisation. Access to a private cloud

is restricted by a firewall which is managed by the organisation. A private cloud requires that the organisation installs and maintains infrastructure, including hardware, software and networking components.

- ▶ Community – a community cloud is one that is designed for and used by a group of organisations working in a particular industry, for example the financial sector. By using a community cloud the financial sector can transfer money between banks, process credit and debit card payments and liaise with international banks. An example of a community cloud is the SWIFT banking system.
- ▶ Hybrid – the hybrid model is the 'best of both worlds' and incorporates the best aspects of private and public clouds. For example, an organisation can utilise some services on the public cloud but has a private cloud for sensitive services or data.

Delivery models of cloud computing

There are six commonly used cloud delivery models.

These are:

- ▶ Infrastructure as a Service (IaaS)
- ▶ Platform as a Service (PaaS)
- ▶ Function as a Service (FaaS)
- ▶ Software as a Service (SaaS)
- ▶ Data as a Service (DaaS)
- ▶ Everything as a Service (XaaS)

DaaS is covered in section 7.4.3

Each delivery model has a different purpose. More than one delivery model can be used by an organisation to provide a complete cloud service which meets their needs.

IaaS provides organisations with infrastructure. The infrastructure provided by the IaaS provider can include a network, servers, storage areas and an operating system (OS). This means that the organisation can reduce the costs and physical presence of hardware. One of the benefits of using an IaaS is that organisations only pay for what they use and so can increase, or decrease, the infrastructure they use. This is called scalability and means that the organisation can be flexible as the organisation's requirements change. Examples of IaaS include Amazon Web Services (AWS), Microsoft Azure and Oracle Cloud.

PaaS includes all the features of IaaS and builds on these to include software including development tools. But it is still possible for the organisation to use their own application software. PaaS is commonly used during the development and testing of a (usually)

web-based software application. The PaaS provider provides the platform, hardware and software to develop the software application on, and the organisation remains responsible for developing and deploying the application. As with the IaaS model, PaaS is scalable. Examples of PaaS include Google App Engine and Microsoft Azure.

FaaS offers an organisation the facilities to create high-quality functions that people are unable to write for themselves. These are then converted into a service that people can use. FaaS places a function onto a cloud instance which means that it can be accessed by a range of people and computers and it does not rely on the user's system and hardware in order to work as intended.

Functions are accessed through one or more triggers that will have been defined when the function was created. The network infrastructure is managed by the vendor and the functions are managed by the client.

SaaS is a very popular delivery model with organisations and, increasingly, individuals. SaaS provides the software applications and services, for example a cloud storage area, that the end-users can access. As the software provided by SaaS is not location dependant, software can be accessed from a range of devices in different locations as long as an internet connection is available. The software is accessed through a subscription service; this may be a fixed fee with limitations, such as the number of devices that can access the software, or on a pay-to-use basis. Examples of SaaS include Microsoft 365 and Google Docs.

Each delivery model differs in the way in which responsibility and ownership of resources are distributed between the subscriber and service provider.

XaaS is known as 'Everything as a Service' but is often referred to as 'Anything as a Service'. It relates to products and tools that are purchased 'as a service'. It therefore can include IaaS, SaaS, DaaS and PaaS. It is a method used to create a resilient digital environment by delivering any service to the digital devices. The purchaser identifies their needs and then purchases the relevant service. This could be for software, hardware, servers, data etc.

Benefits of cloud computing

Cloud portability

Cloud computing facilitates the quick and easy movement of services. There are three areas of portability to consider:

- ▶ **data portability** – the reuse of data components across different applications
- ▶ **application portability** – the reuse of application components across cloud PaaS services and traditional computing platforms
- ▶ **platform portability** – there are two forms of platform portability:
 - reuse of bundles containing applications and data with supporting platforms (machine image portability)
 - reuse of platform components across cloud IaaS services and non-cloud infrastructure (platform sources portability).

Cloud sourcing

This is where organisations (known as the subscribers) will outsource business processes to a third party (referred to as a service provider). Subscribers will pay the service providers for services such as IaaS, PaaS, SaaS and DaaS. Dropbox is a well-known cloud source used by individuals for the storage and sharing of data and files.

Cloud sourcing provides subscribers with an easier option for scalability (whether this is upward or downward). Subscribers only need to contact their providers and renegotiate the fee in order for their needs to be met. In addition, the onus is on the service provider to ensure that the services they offer are up-to-date and maintained as opposed to subscribers having to employ technical teams to maintain these services for them.

The market for cloud sourcing has expanded rapidly from small service providers to much larger ones. The smaller service providers have to consider new and innovative ways to retain their share of the market.

Elastic cloud

This is where an organisation can increase or decrease the services that it receives from the cloud providers as and when the business's needs dictate that a change is required. This could be additional storage, additional software and/or hardware and so on. This means that it is more cost-effective for an organisation as they are not having to purchase additional costly resources which would require setting up and configuring. It is instantly accessible from the cloud.

Storage

Cloud storage is generally more affordable because the cloud service providers share the costs of their infrastructure and services across many businesses.

The cloud storage provider maintains, manages and supports the storage solution for the organisations. This means that organisations do not need employees to spend time carrying out the tasks for keeping data safe and maintaining the servers. The data is uploaded to servers in a data centre, which provides a high level of security. Data that is stored in the cloud is accessible to authorised people wherever they are based and not necessarily in one location, for example the office. The main benefit of cloud storage is that it is scalable, and an organisation can easily have the capacity increased (for a fee) as and when required. An organisation's data is also backed up on multiple servers, so should one server crash it is always readily available.

Cost-effective

Cloud providers can save organisations a lot of money. Cloud providers buy computing resources in massive quantities at low costs. When organisations use these resources, which are shared with other organisations, they avoid having to pay large amounts of money up front to implement their own expensive IT infrastructure. Also, organisations can opt for the pay-as-you-go pricing model. This means that they only pay for the resources they use and can scale up and down the resources required as and when they are needed.

Test yourself

- 1 Describe the term 'hybrid cloud'.
- 2 Explain the difference between 'IaaS' and 'PaaS'.
- 3 Explain how cloud portability is a benefit to organisations.
- 4 Besides cloud portability, identify three benefits of cloud computing to organisations.
- 5 Describe the term 'XaaS'.

5.6 The methods and benefits of creating a resilient digital environment

Methods of creating a resilient environment

Digital resilience involves:

- ▶ understanding the risks involved with having a digital environment and identifying how these risks can be mitigated
- ▶ being able to identify when a problem has occurred and what to do

- ▶ being able to recover from problems
- ▶ learning from experience and implementing processes and procedures to mitigate any future occurrences of the same or similar problems

Strong digital resilience is when organisations manage digital risk and, at the same time, continue to deliver its products/services to its stakeholders regardless of the situation. It is a combination of business resilience and cyber security.

Business processes are becoming more and more reliant on technology, and should a problem occur that disrupts the functionality of the business, it can result in the loss of customers, revenue and reputation, as well as important/sensitive business data. It is therefore important that businesses have plans in place that enables them to adapt to these problems allowing them to function with minimal disruption to the business and to their stakeholders. It also involves businesses considering new technology and embracing the opportunities that this technology provides, to ensure that they remain competitive within the marketplace.

When considering digital resilience, organisations must be able to balance the opportunities for technological change, business expansion and security whilst complying with current legislation and regulation.

Installation of software upgrades and updates

Businesses are always trying to cut costs, but it is vital that business software is upgraded and/or updated on a regular basis. Relying on outdated software can put a business at risk. Here are four reasons why businesses should ensure that their software is up to date.

- ▶ **Improved collaboration** – with more and more people working remotely from home, it has become even more important that collaboration continues to ensure business success. The latest software offers collaboration, for example Microsoft Teams, Skype or Zoom. In addition, many software packages enable people to co-author documents in real time.
- ▶ **Time efficiency** – using cloud-based software means that the employees of an organisation use the most up-to-date and current applications. When using the cloud, there is no requirement for the IT technicians to walk around the building trying to install updates and/or patches manually. Up-to-date software also means greater security for the data held on the system. If an organisation uses cloud-based software, then the applications being used are automatically updated in the background.

In addition, as the business evolves, the cloud-based software evolves at the same time, providing additional features and functions.

- ▶ **Greater security** – data security is becoming more and more complex and increasingly important to businesses and their customers. Outdated software invariably has security breaches resulting in sensitive information being leaked or hacked.
- ▶ **Mobility** – many employees within an organisation now use mobile technology such as tablets, laptops and smartphones and so on. It is important that the employees can use any device to access the work they are required to plan, do and/or review.

Replacement and removal of hardware

Hardware is constantly changing and updated versions of hardware become available that are more efficient, reliable and, in some instances, include additional security measures. Also, old hardware will eventually break and will either fail altogether or have to be constantly replaced (with the possibility that replacement ‘parts’ will no longer be available). If a piece of hardware comes under the banner of End of Service/Support (EOS) this means that the manufacturers will not be providing any further support for the product. This can include repairs, limited technical support and even the availability of parts. Although these may be accessible for a short time frame until the stocks are depleted. If hardware comes under the banner of End of Life (EOL), then a date will have been set by the manufacturer to indicate that they will no longer be manufacturing a particular piece of hardware. These factors are major considerations by individuals and organisations when considering the replacement and removal of hardware. E.g. if a piece of hardware is reaching its EOL date say within the next three months, would this be a good time to make the changes rather than wait until EOL is reached and there is a potential for the hardware to fail. While an organisation will not want to purchase new hardware all the time, a constant review of the digital resilience strategy can highlight when and if changes are required. Alternatively, wherever possible, many organisations are electing to use the cloud for their systems as the issues of upgrades and replacements lie with the cloud vendor.

Adding redundancy into systems

Both redundancy and resilience provide ways to produce a dependable system (system dependability) and data belonging to an organisation. They are critical for the design and deployment of computer networks, data centres and IT infrastructure. However, resilience and redundancy are not the same thing. A combination of

resilience and redundancy provides fault tolerances within a system, allowing it to remain functional should an issue occur.

- ▶ **Resilience** is the system’s ability to recover from a fault and maintain a dependable service.
- ▶ **Redundancy** is the intentional duplication of a system’s components and/or the organisation’s data which also improves the dependability of the system.

Resilience and redundancy complement each other when combined to create a system and provide data that is reliable and dependable.

Decommission and remove legacy hardware and software

The decommissioning and removal of legacy hardware and software (which collaboratively is a system) requires careful consideration and planning. Organisations can accumulate many legacy systems that are rarely used but nonetheless contain vast amounts of data. These legacy systems may need to be kept and maintained due to legal regulations and legislation, or some of the data may have a value to the business. Holding onto this data on a legacy system is extremely expensive with respect to the running costs and the digital footprint that makes migration to another system very expensive. The benefits of decommissioning and removing legacy hardware and software include:

- ▶ **Finance** – running and maintaining older systems can be extremely expensive due to the support costs for the infrastructure, software and hardware. By decommissioning legacy hardware and software, an organisation can save up to 80% of the total cost.
- ▶ **Sustainability** – legacy hardware has a higher power consumption and space requirements compared to more modern hardware. Removing and moving the data to a newer system will contribute towards the organisation’s environmental objectives in line with ‘Green IT’.
- ▶ **Reduction in risks to the business** – legacy hardware and software have a number of business risks. This is because legacy hardware can be unreliable, and some software is no longer supported. In addition, an organisation can receive hefty fines if their digital systems no longer comply with current legislation and regulation requirements.
- ▶ **Restriction of opportunities** – the maintenance of legacy hardware and software can detract resources, such as staff and costs. This staffing and money could be put to better use on other projects and/or business priorities.

Device hardening

Device hardening is the methods/processes used to eradicate any means of attack. This can be achieved in many ways e.g.:

- ▶ disabling unused network ports
- ▶ strict password management and file permissions
- ▶ using multi-factor authentication using hardware tokens as well as passwords on networks
- ▶ updating computer systems with security patches as they become available (but it is also important that the system is tested to ensure that the patch update has not created any functional issues)
- ▶ removing all non-essential services and programs - the bigger the 'surface area' of the system (by this we mean how large the system is and what it contains), the greater the opportunity for potential hacker to access the system; by removing non-essential services and programs, the 'surface area' is reduced
- ▶ setting time limits on access, e.g. using a timeout system so that a person is automatically logged out of a system/application if there is no evidence of its use. This comes with its drawbacks as it can be frustrating for the user to be locked out after a short period of time because they have, for example, answered a phone call. This can slow down the workflow and, therefore, productivity.

Careful planning has to take place when implementing device hardening. The implications to workflow and productivity must be considered as well as the potential for reducing the attack surface areas of the system.

Research

Research other device hardening activities. Try to find at least three additional examples.

Maintaining effective backup systems

It is important that, should an incident occur, an organisation is able to access up-to-date and reliable data in order to continue functioning. Even if a digital system can be recovered quickly, it can still create problems for an organisation if the data is unavailable or out of date.

There are four main types of backup.

Full backup

A full backup is the backup of every file and folder stored on the system. They are more time consuming to complete and require sufficient space for all of

the data. It is a faster method to use when there is a requirement to restore lost data. Because it includes all files and folders it is more robust and reliable than other forms of backup. Full backups are particularly important if the data within an organisation change significantly on a regular basis. It is storage hungry, and this has to be considered by a business. There is little point in carrying out regular full backups if the data does not change very often. It is also time consuming, and consideration has to be made as to how often the full backups should take place.

Incremental backup

After a full backup of the system is created, an incremental backup can be used. This is when only the data that has changed since the last backup has been created. for example a person starts working on a report and saves it to the system. The report is not complete as they have further work to carry out. The incremental backup will backup a copy of the report. The following day, the person continues working on the report and finalises it. The incremental backup that takes place, will create a backup of the report if it has changed since it backed it up originally. Incremental backups do not use as much storage space as a full backup but use additional resources so that it can compare the current state of the data with its previous backup and identify what data has changed and what requires backing up. It is more time consuming to restore data from an incremental backup than a full backup. This is because it has to analyse the data within the backup to establish the timestamp for when the data changed. Therefore, several incremental backups may be required to restore the data.

Differential backup

The data initially undergoes a full backup procedure. It will then only backup the data that has changed since the last full backup. Take, for example, the report we discussed in the incremental backup section. This report will be continually backed up (even once it has been completed) until the next full backup takes place. Some people confuse differential and incremental backups. An incremental backup only backups data (files and folders) that has changed since the last back up (regardless of the type of backup). A differential backup will continually back up any data (file/folder) that has changed since the last full backup. It is easier to recover the data as all that is required is the last full backup and the latest differential data backup. Differential backups do require more storage than the other types of backups.

Mirror backup

A mirror backup (sometime referred to as a mirror image) is not only a backup of the data, but also of the entire system, including operating system, applications, configurations, preferences, booting procedures and hidden files. Consider a home computer and taking a mirror backup of the hard drive. If the hard drive fails, a new hard drive can be installed, and the mirror backup taken from the failed drive can be restored onto the new hard drive. Mirror backups are faster than other backup types and create a 'clean' copy without old or outdated files/folders.

On-premise

This is where a copy of the data is saved onto in-house storage devices. These could be a network attached storage device, storage servers or a tape/disk. Many organisations will initially begin by using on-premise backups because it is simple to implement. When data is lost, it is the IT team who must recover the lost data which can be just files or even entire hard disks. The recovery time is based on what is required to backup and how and when it will be carried out. Sometimes these backups can take hours, days or even weeks to complete depending on the type of storage used and the location of the storage. On-premise backups are vulnerable to disasters, such as fire, theft, mismanagement and flood. On-premise backups can also be quite expensive due to:

- ▶ cost of electricity for the power and maintaining the hardware
- ▶ cost of resources such as the purchases of the backup storage hardware (e.g. storage server), as well as any upgrades or repairs that may be required
- ▶ cost of IT expertise to provide the support for emergencies and repairs that may arise.

Off-site/remote

This is the backing up of critical data from in-house computer systems and storing them securely in another location (off-site). Off-site backups are safer and more efficient than on-premise backups. They can store past and current versions of sensitive data. Off-site/remote can mean to backup data to the cloud or in another remote location such as a different building.

The issue with another remote location is that, if the organisation requires their backups to be used to reinstall critical lost files and/or data, then time will be taken to retrieve the backup from the location and bring it 'in-house' to upload the data. This is in addition to the various costs that can be involved as with on-premise backups, as well as the vulnerability issues.

Cloud

Cloud backups are stored in data centres that have built-in redundancy. They also have to comply with highly regulated safety measures and 24 hour monitoring. The three main factors for using cloud backups are:

- ▶ **Cost** – traditional backup solutions can be time-consuming and costly. There is the initial cost, ongoing upgrades, routine maintenance, software and hardware updates and repairs. In addition, an organisation needs to hire a team of IT specialists to manage the backups. When using cloud backups, there is only the fee for using the cloud storage provided by the supplier. All aspects of costs are shared between the organisations using the service and covered within the fee paid by the organisations.
- ▶ **Recovery time** – cloud backups are available 24/7 and can be accessed immediately.
- ▶ **Security** – it is important that an organisation's data is safe and not at risk or vulnerable. Cloud backup storage provides end-to-end encryption and data centres have to follow compliance-based security measures (e.g. complying with regulation and legislation with respect to security of data).

For any organisation, using cloud storage facilities is by far the most efficient and cost-effective solution.

Appropriate and reviewed standard operating procedures

A standard operating procedure (SOP) is a set of step-by-step instructions developed by an organisation to assist their employees to carry out work activities in a clear and consistent manner. Consistency is very important in a regulated environment, for example banks, so that the outcomes from the work activities are reliable at all times. SOPs are put in place to reduce errors and maintain product quality. Data that is held within a digital environment must be compliant with regulations, for example Data Protection Act 2018, Computer Misuse Act 1990 and so on. If an organisation is functioning across different countries, then they must comply with the legislation for those countries as well. SOPs are in place to ensure the security and integrity of the data. SOPs apply to all users, whether they are on-site or working remotely. SOPs usually include the following:

- ▶ **Backup and data recovery** – that backups should be carried out on a routine basis as a data protection measure. Data should be restored in situations where issues have arisen, and these restorations should be carried out promptly.

- ▶ **Security administration** – system users must have log-in and password processes that will uniquely identify them and their levels of access and approval authorisation to the system and data that is stored.
- ▶ **Change control** – the processes that must be followed to ensure that any changes to the system do not have a negative effect on the functions of the organisation. Change control includes the IT infrastructure, software and procedures.
- ▶ **Operations and maintenance** – this applies to all aspects of the maintenance of the digital environment including the servers and networks, virus protections and other cyber issues.
- ▶ **Disaster recovery** – unforeseen issues can always occur, but they must be identified and evaluated as a risk. Measures must be developed so that the organisation can resume operations within a specified timeframe.

Structure training for staff

New hardware/software

Whenever there is a change to hardware and/or software, staff are invariably faced with a new way of doing things. This can be stressful and in order to minimise the stress of the staff so that maximum performance is maintained, training is essential. Training the staff to utilise the new ‘tools’ and capabilities available with the improved/additional IT resources makes their job easier and more efficient.

Here are some reasons why staff training is important when new hardware/software has been implemented:

- ▶ minimise confusion and mistakes when using the system
- ▶ ensure staff take advantage of the additional functions, features and capabilities of the new system
- ▶ minimise the waste of money upgrading systems that are then not used
- ▶ minimise the need for IT staff to solve minor problems due to user error/misunderstanding
- ▶ empower staff by updating their skills and making them feel valued.

Staff induction

Staff induction supports staff so that they have the skills to get their work activities completed safely and more efficiently. Staff who feel comfortable and safe in their environment are known to have high productivity levels. Investing time and money in induction training shows staff that they are valued. This can increase loyalty and staff retention. Staff induction can reap the following benefits:

- ▶ **Reduction in staff turnover** – staff who receive a good induction and further development training are more likely to stay with the organisation because they feel valued and respected.
- ▶ **Saving of time and money** – during induction, staff receive training and information relating to the work activities and duties that they will be carrying out. The training and information enable them to perform these duties promptly, safely and efficiently.
- ▶ **Improvement in communication** – ensuring that new staff know the structure of the organisation and the named people responsible for the different roles, instils a level of confidence within the new member of staff and sets the framework for good employee/management communication.
- ▶ **Safer working environment** – it is important that staff have knowledge of their working environment, their individual responsibilities, job role and health and safety procedures. This will reduce potential risks and injuries within the working environment.

New and updated policies and procedures

Organisations often have to develop new, or update, policies and procedures. This can be due to new or revised legislation and regulation, changes to the IT systems, changes in the market in which it functions as a business or changes to job roles and responsibilities. It is important therefore that staff are not only made aware of these new and updated policies and procedures, but they also receive training. The benefits to an organisation of delivering this training reaps the same benefits as previously discussed for staff induction and when implementing new and/or updated hardware and software.

It is important to remember that a well-trained workforce is a highly productive workforce.

Benefits of a resilient digital environment to the organisation

Increased security

Greater security does not necessarily mean more resilience. Although a less secure technology may create access vulnerabilities, a more secure solution may introduce assumptions that are flawed. Processes which are not resilient can lead to disastrous business inflexibility. The implementation of any new digital infrastructure must be assessed with respect to its overall impact on business resilience in terms of the opportunities and the risks. An organisation will

improve their security of data and systems if they focus on ensuring that:

- ▶ digital systems (hardware and software) are up to date
- ▶ decommissioning and removal of legacy hardware and software is carried out effectively, efficiently and securely
- ▶ employees are well trained with respect to using the digital systems, following processes and complying with health, safety and security requirements
- ▶ regular backups of data are carried out and stored remotely.

Secure transfer of data

Data that is transmitted/transferred across a network and/or the internet is always at risk of being intercepted by unauthorised people, for example cyber criminals. By implementing the range of digital resilience techniques discussed above, organisations will benefit from the data being more secure during transfer. This can involve using such things as data encryption, securing networks and setting access permissions for employees.

Secure storage of data

Customer, supplier and employee data must be stored securely by an organisation as failure to ensure that the data is safe and secure can result in litigation against organisations and potentially very hefty fines. Business sensitive and critical data must also be stored securely to ensure that there is no risk of loss, or access to unauthorised organisations and/or people. The loss of this data can have major impacts on the functioning of a business. Good digital resilience within the organisation will result in the implementation of strategies to maintain the secure storage of data.

Reduced system vulnerabilities

Part of any digital resilience strategy is to review all systems and processes and identify the risks of system failures and unauthorised system access. The risks are further considered with the potential impact on the organisation. By conducting a review of digital resilience for the organisation, vulnerabilities in the system can be identified and actions taken to mitigate the risk of harmful events occurring.

Reduced probability of targeted cyber attack

In the previous sections, you saw that digital resilience looks at the risks to systems and data, as well as the potential impacts and the likelihood of something going

wrong. Potential solutions to mitigate against or address promptly any problem that can arise will ensure that the systems and processes are less vulnerable. This includes potential cyber attacks. As every aspect of the organisation is looked at in detail, the probability of a cyber attack can be greatly reduced.

Increased reputation and profile

Customer confidence

An organisation that can demonstrate that they are aware of the risks associated with the use of digital technology will instil customer confidence in the business. Customers will consider whether an organisation has implemented a strategy to mitigate against risks (does the customer believe their data is secure?). In addition, customers will expect the business to consistently function as expected. An organisation that can maintain full service to their customers at all times will also instil confidence from the customers.

Brand image

Bad press due to security breaches, loss of data or system failures that prevent a business from functioning can easily destroy the brand image. Through careful planning and the implementation of a digital resilience framework, an organisation can mitigate against these types of potential issues and ensure that the brand image is maintained positively and not damaged.

Lower downtime of services

Throughout this section you have read how organisations can ensure that the systems are safe, secure, up to date and well maintained. The implementation of these strategies will reduce the potential downtime of a system by ensuring that any potential issues are prevented or, at the very least, addressed promptly.

Test yourself

- 1 Compare and contrast the different forms of backup systems.
- 2 Explain why structured staff induction and training is important for an organisation when implementing a digital resilience strategy.
- 3 Describe the term 'device hardening'.
- 4 Identify two advantages of using cloud backup storage to an organisation.
- 5 Describe the term 'standard operating procedures (SOPs)'.

Project practice

A global market research and analysis company has teams of analysts who work remotely not only in different locations within the UK but also in Europe. The analysts collect data from a variety of sources in relation to products sold by various global businesses.

Data is gathered in many different ways including online through social media, email, web-based surveys and people who stop people in the street and ask them questions. The answers to the questions are typed into an online form and, at the end of every day, emailed into the main office. The teams meet every month to provide updates and in order to allocate further market research. This is conducted through teleconferencing.

Currently each location has their own files stored on their own PC/laptop/smart device/network. There is no central location for storage and everything is shared via email.

Due to the rapid expansion of the business, the board of directors (non-technical) and IT Support (technical) want advice on the following:

- ▶ the types of network that should be implemented
- ▶ advice on whether the use of cloud computing would be beneficial and what forms of cloud computing they should consider
- ▶ explanation of virtualisation and what forms of virtualisation would benefit the business
- ▶ what they should include in their digital resilience strategy and what the benefits would be of its implementation.

Produce a report or a presentation with detailed speaker notes.

Remember you are preparing this for the board of directors (non-technical) and IT Support (technical), so make sure you justify any recommendations/suggestions.

Assessment practice

- 1 Compare the different types of keyboards that are used in digital devices.
- 2 Explain how data collection can be achieved using the Internet of Things.
- 3 Discuss the key features of virtualisation and the benefits to an organisation.
- 4 Describe the seven layers of the OSI model.
- 5 Explain how an incremental backup is created.
- 6 Identify three types of servers.
- 7 Explain the term 'device hardening'.
- 8 Explain the term 'SaaS'.
- 9 Discuss the benefits of cloud computing to an organisation.
- 10 Discuss the benefits of digital resilience to an organisation.

Core element 6: Diversity and inclusion

Today's world seems to include the use of digital systems in all areas of life. Lots of services, such as accessing bank accounts, doing shopping, and even applying for the driving theory and practical tests, have moved online. While this is a good use of time and reduces the need for resources and a physical presence, it is important that access to digital systems and services is inclusive.

When digital systems are being created it is important to consider all potential end users so that no one is disadvantaged. This means that websites, apps and physical digital systems should be accessible to all potential end users. Legislation and guidelines have been created to ensure inclusivity. These include the Equality Act and the Web Content Accessibility Guidelines (WCAG). The benefits of the use of digital systems increase when organisations consider, and apply, the principles of inclusivity, including consideration of the diverse range of end users.

Digital systems, and the services they supply, need to be available to all end users. You will learn about how demographics need to be considered to ensure that no group is disadvantaged and unable to access the digital systems they need. By ensuring that all demographic groups can access digital systems, these systems become inclusive. By ensuring inclusivity, the benefits to individuals and organisations will increase.

However, where inclusivity has not been considered this can have an adverse effect on individuals and organisations. You will learn about the adverse effects that can be caused by the lack of inclusivity.



Learning outcomes

In this core element you will learn about:

- 6.1** The principles of digital inclusion, and legislation relating to equality and diversity
- 6.2** The business benefits of diversity and inclusion

- 6.3** Approaches to addressing demographic imbalance in the digital sector
- 6.4** How digital inclusion affects individuals and organisations in the digital sector

6.1 The principles of digital inclusion, and legislation relating to equality and diversity

Industry tip

The details of each piece of legislation/Regulation were correct when this book was published. During your study for this course, you must make sure that you know about and understand the most up-to-date versions of each piece of legislation, including any changes or additional pieces of legislation that are relevant to digital support and business systems.

Digital inclusion principles

There are some general principles which should be considered to ensure, as far as possible, that access to digital systems, and the services they provide, is inclusive. This means that no individual, or group of individuals, should be excluded.

One of the principles of data inclusion is to make sure that no one is disadvantaged by a digital system. There are many people who have specific needs which should be considered. These needs can include a visual, auditory or physical impairment. When digital systems are being created these needs should be considered. For example, a website should always include special features such as Alt Tags and a screen magnifier feature so that individuals with a sight impairment can still use the website. Guidelines on making digital systems inclusive are included in the Web Content Accessibility Guidelines (WCAG).

WCAG are covered in section 8.1, p. 198.

There are different peripherals, assistive technology, that can be used by individuals with physical impairments. These include head wands, roller ball mice and a range of different types of keyboards. Access to digital systems becomes more inclusive by ensuring that a digital system can interact with a range of assistive technologies.

Checking for bias

Organisations collect, store and process data to assist in their day-to-day functioning. Data can be stored and used by the organisation who collected it, or data can be accessed from a big data set. Large amounts of data are stored in data warehouses, data repositories and data lakes.

Data lakes, repositories and warehouses are covered in section 3.1, p. 76.

To maintain, and increase, inclusivity, data should be checked for **bias** before it is processed. This could include, for example, checking that the data fully represents all demographic groups. If biased data is processed, then, obviously, the results will be biased and not representative. This, in turn, could lead to a reduction in inclusivity. If biased data is used by an organisation, then this could lead to incorrect business decisions being made at an operational level.

Key term

Bias: a tendency, inclination or prejudice toward or against something or someone.

Access to technology

It is important that all end users are able to access digital systems to ensure they can complete the actions they need to take. There are some potential issues which can arise, which can be referred to as the digital divide.

Many people have limited access to technology. For example, some families may only have access to one device, or they might be using outdated technology. The limited access may be caused by financial issues or lack of knowledge and confidence to upgrade their technology.

The effects of limited access to technology were seen during the pandemic of 2020–21 when many pupils had to carry out their schooling at home through online lessons. It was highlighted that some pupils did not have access to their own device and were unable to access the lessons. Charities and the UK Government provided some devices to make sure pupils were able to continue with their education. Many employees were advised to work from home, with employers having to relocate devices to employees' homes for them to be able to complete their work.

Research

Research the impacts of lack of access to technology on end users.

Discuss your findings with the rest of your group.

Connectivity

In 2017 the UK Government published the UK Digital Strategy. This strategy set out seven strands, which include connectivity and digital skills and inclusion.

To be able to fully access digital systems and the services they provide, **connectivity** to the internet needs to be available. Connectivity across the UK can vary with some areas still not able to access a broadband connection that is stable or of a high enough speed to avoid buffering. The Digital Economy Act (2017) also sets out legally binding broadband speeds that end users can expect.

The Digital Economy Act is covered in section 8.1, p. 196.

Research

Find heat maps on the internet that show broadband and mobile data connectivity for the UK.

Which areas have the lowest and highest rates of broadband and mobile data coverage?

What are the reasons for this?

There are some areas where the infrastructure needed for high-speed broadband and mobile data is challenging. Many of the large providers will not provide connections to, or will charge very high prices for connection to, villages and homes in remote areas. To combat this issue, and to conform to the strands of the Digital Strategy, the UK Government set up a voucher scheme to assist communities with the cost charged by the providers to provide the infrastructure.

Research

Investigate providers such as AirBand and B4RN (Broadband for the Rural North), which provide the infrastructure and broadband access to rural and remote communities.

How do the schemes work?

What involvement do the residents have in the project?

What are the benefits and limitations to these schemes?

Connectivity and access to the services provided by digital systems can also be an issue for those end users who have legacy technology. Many people's mobile devices, unless these are very up to date, may not be able to access the current highest speed 5G mobile data network. This means that there is a decrease in inclusivity.

Codes of best practice

There are codes of practice and guidelines to help increase the inclusivity of digital systems. By following these codes of practice and the guidelines, every end user will be able to access and use the digital systems they need. The most comprehensive code of practice is that of the WCAG.

WCAG are covered in section 8.1, p. 198.

Technical knowledge and skills

To be able to effectively use digital systems, the end user must have some technical knowledge and skills.

Without knowledge and skills, end users may be under-confident when using digital systems. The

demographics of those with a lack of digital skills tend to be people who have:

- ▶ not been brought up in the digital age
- ▶ a disability
- ▶ come to the UK from a different country where digital skills are not part of the educational curriculum.

Without the digital skills, end users may be reluctant to use digital systems and so will not be able to access the services they offer. The lack of digital skills may also have a detrimental effect on employment opportunities, access to services such as the NHS, and day-to-day tasks such as shopping and banking.

The UK Digital Strategy has set down in part 2, Digital skills and inclusion, the plan for increasing the digital skills of the UK population.

Research

Investigate the UK Digital Strategy, part 2, Digital skills and inclusion. What are the main points of the plan?

Research news websites to confirm if the plans set out in part 2 have been realised.

Discuss your findings with the rest of your group.

Key term

Demographics: the characteristics of people, for example age, ethnicity and gender.

Test yourself

- 1 Identify two data storage types.
- 2 What is bias?
- 3 Identify two different assistive technologies.
- 4 Identify two tasks that can be carried out using a digital system.
- 5 How many strands are there in the UK Digital Strategy?

Research

Investigate the Glossary of Terms on the Equality and Human Rights Commission website.

Can you think of any terms that are not included, but should be?

Legislation

To increase access and inclusivity to digital systems, legislation and statutory codes of practice have been created. The legislation and statutory codes of practice make it illegal for any demographic group to be discriminated against in a range of situations, including access to the digital systems and services.

The Equality Act 2010

The Equality Act (EQA) 2010 became law in October 2010. The aim of the Act was to provide equality of opportunity for all people. The Act protects people from any form of discrimination in society and the workplace.

The Act replaced and combined over 116 different pieces of legislation related to discrimination, harassment and victimisation. This made the legislation easier to understand and apply. The Equality Act defines the different ways in which it is unlawful to treat people.

The Act provides a legal framework to protect the rights of individuals and to advance equality of opportunity for all. It provides Britain with an anti-discrimination law which protects individuals from unfair treatment and promotes a fair and more equal society.

The Equality Act protects everyone in all situations, including in the workplace. This is because the Act protects people against discrimination, harassment and victimisation because of their protected characteristics (see Figure 6.1). It is those protected characteristics that makes us all individual and unique.

As with all legislation, the Equality Act contains specific terms. The Equality and Human Rights Commission has a Glossary of Terms on their website.

Types of discrimination (protected characteristics)

The Equality Act defines nine protected characteristics. These are:

- age
- disability
- gender reassignment
- marriage and civil partnership
- pregnancy and maternity
- race
- religion or belief
- sex
- sexual orientation.



▲ **Figure 6.1** The nine protected characteristics defined in the Equality Act

How individuals can be discriminated against

There are different types of discrimination that can be applied to each of the characteristics. The four main types are shown in Table 6.1.

Type	Meaning	Example
Direct discrimination	This means treating one person worse than another person because of a protected characteristic.	An older employee is not trained on a new software system as the employer feels that they will be retiring soon so to train the employee would be a waste of time and money.
Indirect discrimination	This can happen when an organisation puts in place a rule or a policy or a way of doing things which has a worse impact on someone with a protected characteristic than someone without one.	A new digital system is introduced which uses a touch screen. The system does not support assistive technology so employees who need assistive technology are moved to a lower paid job role.
Harassment	This means people cannot treat you in a way that violates your dignity, or creates a hostile, degrading, humiliating or offensive environment.	Employees who are unable to complete their job role due to a new digital system are the victims of derogatory name calling in the workplace.
Victimisation	This means people cannot treat you unfairly if you are making a complaint of discrimination under the Equality Act or if you are supporting someone else who is doing so.	Employees who cannot use a new digital system which uses a touch screen make a complaint to their employer. These employees are the first group to be made redundant when a restructuring takes place.

▲ **Table 6.1** The four main types of discrimination

Each characteristic is covered by different types of discrimination. Most of the characteristics are covered by the four main types of discrimination, as shown in Table 6.1. However, you will notice that some characteristics are covered by other types of discrimination.

Table 6.2 shows the types of discrimination that can be applied to each characteristic.

Activity

Select one of the protected characteristics. Investigate examples of discrimination for your protected characteristic.

Create a digital communication detailing what is meant by the characteristic and showing examples of discrimination.

Discuss your findings with the rest of your group.

- have contact with public bodies like your local council or government departments.

www.equalityhumanrights.com

The aim of the Equality Act is to provide a framework for inclusivity in the workplace and society. However, there are some circumstances where being treated differently, in terms of the protected characteristics, is acceptable.

For example, an organisation providing help and advice for immigrants from India may specify that all their employees must be of Indian descent and speak one of the native Indian languages.

Research

For each protected characteristic, investigate the circumstances where being treated differently to the Equality Act is acceptable.

Where individuals are protected

You have already learned that people are protected in the workplace and in wider society. There is a defined range of situations where a person is protected from discrimination. These are when you:

- are in the workplace
- use public services like healthcare (for example, visiting your doctor or local hospital) or education (for example, at your school or college)
- use businesses and other organisations that provide services and goods (like shops, restaurants and cinemas)
- use transport
- join a club or association (for example, your local tennis club)

When to take action against discrimination

An individual could take action if they feel they have been discriminated against. The action could be to:

- complain to your employer either informally or using a formal grievance process
- ask for help and support from, for example, a trade union, equality organisation or the Citizens Advice. Someone from these organisations can be asked to act on your behalf. This is sometimes called a mediation process.
- begin Employment Tribunal proceedings.

There are organisations that can help if an action against discrimination is being considered. These organisations include professional bodies, trade unions, citizens advice and the dedicated Equality Advisory & Support Service (EASS).

Characteristic	Types of discrimination
Age	Direct discrimination Harassment Indirect discrimination Victimisation
Disability	Direct discrimination Discrimination arising from disability Failure to make reasonable adjustments Harassment Indirect discrimination Victimisation
Gender reassignment	Direct discrimination Harassment Indirect discrimination Victimisation
Marriage and civil partnership	Direct discrimination Indirect discrimination Victimisation
Pregnancy and maternity	Unfavourable treatment Victimisation
Race	Harassment Victimisation
Religion or belief	Direct discrimination Indirect discrimination
Sex	Direct discrimination Harassment Indirect discrimination Victimisation
Sexual orientation	Direct discrimination Harassment Indirect discrimination Victimisation

▲ **Table 6.2** The types of discrimination that can be applied to each protected characteristic

The Public Sector Bodies (Websites and Mobile Applications) Accessibility Regulations 2018

These regulations provide mandatory details relating to the accessibility of websites and mobile apps. By

following these regulations the inclusivity of websites and mobile apps can be increased.

The Public Sector Bodies (Websites and Mobile Applications) Accessibility Regulations 2018 is covered in section 8.1, p. 198.

Equality and Human Rights Commission Statutory Code of Practice for 'Services, Public Functions and Associations' under the Equality Act

Following the implementation of the EQA, the Equality and Human Rights Commission (EHRC) created a statutory code of practice for Services, Functions and Associations. This came into force on 1 January 2011.

Services and functions are covered in Part 3 of the EQA while Associations are covered by Part 7.

The code aims to provide guidance relating to protected characteristics and how those providing a service or function should ensure that there is no discrimination when these are being accessed. Associations are also included in the code of practice and how these can alleviate the risk of discrimination. By following the code of practice those offering services and functions and those involved in associations can increase inclusivity and equality.

Research

Find the EHRC Statutory Code of Practice for 'Services, Public Functions and Associations' on the internet.

Looking specifically at Core elements 11 and 12, how can those offering services and functions using digital systems increase equality and inclusion?

What are the main points relevant to associations and how could these be applied to any association you belong to?

Discuss these with the rest of your group.

Test yourself

- 1 Identify three protected characteristics under the Equality Act.
- 2 What is meant by direct discrimination?
- 3 Identify two situations where a person is protected from discrimination.
- 4 Who created the Code of Practice for 'Services, Public Functions and Associations'?
- 5 In which part of the EQA are services and functions covered?

6.2 The business benefits of diversity and inclusion

By proactively considering and applying the principles of **diversity** and inclusion, a business will be able to achieve many benefits. In a business, organisation or company, diversity means that the employees have a range of backgrounds and different perspectives. Inclusion means that everyone, no matter how they interact with the business, feels involved, valued, respected, treated fairly and important to the business.

Key term

Diversity: the range of political beliefs, race, culture, sexual orientation, religion class and/or gender identity differences.

An inclusive workplace means that everyone feels valued and feels safe to:

- put forward their ideas
- raise issues and suggestions
- try to do things in a different way (with the approval of management).

By making sure that the workplace is inclusive and that all policies and procedures are implemented, an organisation can increase the diversity and inclusion for all employees irrespective of demographic characteristics.

One benefit is that the business will be able to expand their customer base because few, if any, demographic groups will be excluded. By increasing the customer base, the business will be able to increase its profits.

More innovative products

If diversity and inclusion are considered when products are being designed, then it is likely that this will result in more innovative products. People who are involved in the development of new products will not be afraid to 'speak out' to provide a different idea, improvement or criticism.

Greater appeal to potential employees

Many large organisations, businesses and companies actively advertise that they are a diverse and inclusive employer. Every year a listing of the top 100 diverse and inclusive companies is published.

Research

Find the latest list of the top 100 diverse and inclusive companies.

What type of sectors rank highest?

What are the benefits of being on the list to the companies?

By advertising that an organisation, business or company is inclusive and diverse, then this may lead to an increase in applicants for advertised jobs. Through the reduction of bias and discrimination, the HR department will be able to select the most appropriate applicant. This will be based on the skills and experience required for the job rather than someone being rejected because of their racial background, gender, or even the type of school or college they attended.

Many employment agencies and websites now advertise posts. There is a growing trend in the working practices of these employment agencies and HR departments to remove any personal details, such as name, gender or racial background, before beginning the selection for the interview process. This is called **inclusive recruitment**. By doing this, the applicants are considered only on their qualifications, skills and previous experience.

Many applicants will research an organisation, business or company before they apply for a job with them. By having an inclusion and diversity policy, which should be available on the website, applicants can be sure that the company aims to be inclusive, celebrates diversity and does not discriminate against any demographic group.

Research

Investigate the diversity, inclusion and equality policy in your centre or workplace and, if possible, talk to the relevant member of staff responsible for implementing the policy.

What are the main points of the policy and how is the policy enforced? Are there any omissions in the policy?

Discuss your findings with the rest of your group.

Inclusive products

Inclusive product design means that products are designed that are accessible and usable by as many people as possible. This means that the products

should be usable and accessible without any special adaptations.

For example, an inclusive website would:

- ▶ Make sure that the website provides a comparable experience for every end user ensuring that all tasks can be carried out in a way that meets their needs. For example, providing an alternative such as a transcript for a video, audio description or Alt Tags.
- ▶ Enable end users to access and interact with the website to meet their needs. For example, use the load more options feature instead of scrolling or pinch-to-zoom gestures on touch devices.
- ▶ Offer the end user a choice of how to carry out a task. A website that offers a range of ways to carry out a task allows end users to select the way based on their circumstances at that time. For example, an end user may have had an eye operation so, while they are recovering, they may need to carry out a task on a website in a different way to usual. If the website has lists of content, then a grid or list option should be included. By doing this larger images can be provided or smaller rows.
- ▶ Ensure that it is consistent in terms of use of colours, layout and fonts used. This could be achieved by using the website owner's house style. Each action taken by an end user should be carried out using the same action. For example, text should be of the same colour, which should be readable and contrast with the background. Red and green together should be avoided, to help people with colour-blindness.
- ▶ Help the end users to focus on the task they need to complete. The main purpose of the website should be clear with the information and functionality of the website being relevant to this purpose. For example, new and important information should be included on the home page and not 'buried' within other web pages.

Ability to connect authentically to Black, Asian and minority ethnic groups

To maintain diversity and inclusion, a business, organisation or company must ensure that they connect with all existing and potential customers and clients. This connection should include all demographic groups, considering in particular those who are often and historically excluded or marginalised, such as individuals from Black, Asian and Minority Ethnic (BAME) backgrounds. A properly diverse and inclusive

workplace allows all employees to bring their whole selves to work, rather than being favourable to one group or another.

The Equality Act, covered in section 6.1, provides legal requirements that everyone should be treated equally.

Reduce risk of reputational damage from non-inclusive products

The risk of reputational damage is diminished by ensuring products are inclusive, including online services. If these are not inclusive this could mean that some individuals are excluded from their use. This could result in legal action under the Equality Act.

By removing these barriers and increasing the inclusivity of products and services it is probable that the reputation of the organisation will increase leading to more customers and more profits.

Test yourself

- 1 What does diversity mean?
- 2 Describe one characteristic of an inclusive workplace.
- 3 Identify two demographic characteristics.
- 4 How can bias and discrimination be reduced when considering job applications?
- 5 Identify one way inclusivity can be demonstrated on a website.

6.3 Approaches to addressing demographic imbalance in the digital sector

It is important that everyone is included and able to use all digital systems and services. Where one demographic group is less included than others, this is known as the **demographic imbalance**. There are a range of approaches that can be taken to attempt to rebalance the demographics.

Increasing cultural awareness of different types of bias

There are many different types of bias which can be applied to any demographic group. Bias can come from, for example, forming friendships exclusively with

people who share the same interests or background as you. This results in bias, possibly unconscious, against those who do not share the same interests or background as you.

Bias can take many forms including gender and age. People should be treated equally irrespective of, for example, disability, racial background, gender or age. Their skills, qualifications and experience should be more important.

By highlighting the different types of bias, and through training, conscious and unconscious **cultural bias** can be reduced. One approach is that of inclusive recruitment. By utilising the inclusive recruitment approach, bias can be reduced as no demographic information is provided to those carrying out the selection for interview process.

Inclusive recruitment is covered in section 6.2, p. 160.

Inclusion by design of digital technologies and systems and digital inclusion principles

It is important that digital inclusion and accessibility are considered when digital systems and technology are being designed. This includes the design of assistive hardware and web-based content. During the design process it is important to consider digital inclusion principles. By doing this, it is likely that the technology and systems will be as inclusive as possible.

Inclusive products are covered in section 6.2, p. 160.

To fully address demographic imbalance, digital inclusion principles can be implemented. Digital inclusion means that everyone, irrespective of their demographic, can access digital systems and services.

There are many digital inclusion principles, but all have the same aim – to make digital systems inclusive for all. You have already learned about some of these in section 6.1 of this core element. Other digital principles could include:

- low cost and accessible connections
- motivation to go online
- access to appropriate and connected devices
- skills, confidence and safety.

To achieve these principles:

- training may need to be offered and accepted by end users
- people's digital rights need to be clear
- connectivity should be defined as a basic need.

Research

Investigate digital inclusion principles.

Make your own list of the ten principles you feel are the most important.

Discuss your list with the rest of your group and make a definitive list of ten principles.

Explain how each principle would be achieved.

detailing how the Government attempted to reduce the digital exclusion that arose, but also set out a range of initiatives to take the reduction forward. One of these initiatives is The Skills Toolkit. The Skills Toolkit covers digital areas, including digital design and marketing, coding and AI.

Activity

Access 'The Skills Toolkit' on the UK Government website. Look at the courses provided relating to the digital industry.

If you have any gaps in your knowledge which are covered by one of the courses, complete the course.

Government initiatives

The UK Government's digital inclusion checklist includes:

- Start with user needs – not our own.
- Improve access – stop making things difficult.
- Motivate people – find something they care about.
- Keep it safe – build trust.
- Work with others – don't do it alone.
- Focus on wider outcomes – measure performance.

The UK Government has a range of initiatives to enhance digital inclusion. Two of these are 'Making your service accessible' and 'Assisted digital support'. These initiatives aim to provide a benchmark for government services with the aim of increasing inclusion.

The UK Government has created a Digital Inclusion Scale which rates the UK population on a scale of 1–9. This scale can be used to assess progress on increasing digital inclusion. The scale can be used across a range of government departments to track the targets and actual progress.

Research

Find the latest UK Digital Inclusion graph.

What can be done to increase inclusion?

The Digital Economy Act and the UK Digital Strategy also brought in legislation commitments about increasing digital inclusion. In 2021, the UK Government provided details about how the digital divide – digital exclusion – had been exacerbated during the Covid-19 pandemic. Steps were set out

Test yourself

- 1 Identify one demographic where bias can occur.
- 2 How is bias reduced when using inclusive recruitment?
- 3 Identify two items in the UK Government's digital inclusion checklist.
- 4 What scale is used in the Digital Inclusion Scale?
- 5 What digital areas are included in The Skills Toolkit?

6.4 How digital inclusion affects individuals and organisations in the digital sector

Positive effects

Digital inclusion can have positive effects on individuals and organisations in the digital sector.

Positive effects of digital inclusion on individuals

There are many positive effects of digital inclusion on individuals. As increased speeds to the internet become more common, the opportunities, and inclusion, increase. This means that all demographic groups will benefit from enhanced access and connectivity to digital technology.

Due to increased inclusivity, individuals, regardless of the demographic group they belong to, are able to access services such as government websites, retail and finance. If these services conform to the Web Content

Accessibility Guidelines and have been designed using an inclusive design process, then accessibility and inclusivity will be increased. This means that there is a lower risk of people being excluded from these services. There is also an increased probability that if individuals need assistive technology to meet their needs, then this will be available.



▲ **Figure 6.2** A braille display device being used

An increased enhanced quality of life is linked with the increase in access to websites and the services they provide. Many of the services that are needed will be available from people's own homes. There could also be an increase in the ability to communicate with friends and family. This communication can be enhanced with increased broadband speeds and the inclusivity of communication features and websites. Websites and communication features such as social media, video conferencing and online messaging can reduce social isolation.

Many job roles in the digital industry can now be carried out remotely. This is because of the increased use of the cloud and online communication facilities. The increased availability of assistive technology also means that individuals who have additional needs can access the technology required to help them successfully carry out their job role. This can also be applied to the physical workspace. This means that increased access to career opportunities, along with the utilisation of inclusive recruitment, are available which, in turn, leads to an increase in social mobility.

Positive effects of digital inclusion on organisations

There are many positive effects of digital inclusion on organisations in the digital sector. Digital inclusion aims to reduce digital exclusion for all demographic groups. By increasing inclusion, a greater variation in employment demographics can be achieved. This can be achieved by

considering, among other things, the Equality Act and by using inclusive recruitment procedures.

The retention of employees will also be increased as policies and procedures are developed and implemented to increase inclusion in the workplace. As the retention of employees increases, it is possible that organisations will contribute towards the cost and time that employees need to enhance their qualifications. This will lead to a more qualified and skilled workforce, who have the skills and qualifications relevant to the function of the organisation.

The UK Government has provided a legally binding Universal Service Obligation (USO) of minimum download speeds of 10 Mbps. This USO provides a possible increase in stable broadband speeds and is linked with the publicly funded broadband providers, such as B4RN (Broadband for the Rural North). This means that remote and rural communities are able to access the internet and the facilities it provides, so increasing inclusion. This could lead to an increase in the customer base of an organisation. Using websites, linked with the increase accessibility of the internet, an organisation can now reach potential customers in previously inaccessible areas. It is also possible for organisations across the world to communicate and do business together. This, and the increased access to customers, should lead to an increase in profits.

Research

Investigate how increased inclusion can lead to an increase in innovation.

Adverse effects when principles of digital inclusion are not applied

If digital inclusion is not considered and applied, then this can have a negative, or adverse, effect on individuals and organisations.

Adverse effects on individuals

If access to websites is not available, then it is possible that individuals will have reduced access to services, for example financial services or retail, including special offers. Individuals can also suffer adverse effects if the technology they need to carry out their everyday work tasks is not available or provided. This can lead to a decrease in employment opportunities which, in turn, may lead to a decrease in quality of life. Linked to this may also be a reduction in the ability to access paid employment.

Social isolation

Social isolation may also occur as a result of decreased inclusivity. Many people rely on online services to communicate with family and friends. If stable broadband at the UK Government's USO speed is not available, or the websites offering these facilities do not have accessible options, then this communication will be reduced. Not being able to access employment opportunities due to the lack of assistive technology may also lead to a decrease in work-based social interaction, leading to an increase in social isolation.

Adverse effects on organisations

If an organisation does not consider and implement digital inclusion practices, this may result in adverse effects. By limiting accessibility to applications for promotion or new job roles, there may be a decrease in applicants with the correct skills and qualifications. If assistive technology is not provided to help employees carry out their job roles, then this may also lead to a reduction in people who have the skills and qualifications to meet the organisation's function and needs.

If a range of demographic groups are not included when products are designed/produced, it is possible that innovative ideas which focus on making the products inclusive may not be thought of. This can apply to products, services and the digital platforms used by the organisation. This could lead to a restriction in service, and reduced accessibility to all demographic groups.

If an organisation fails to consider a range of demographic groups when designing and creating products and services, it may restrict the potential audience, leading to a reduction in profit.

The Equality Act, and the WCAG, set down how organisations should be inclusive and provide

mandatory guidelines relating to the types of discrimination that should be avoided.

The Equality Act and WCAG are covered in section 6.1, p. 156.

If the WCAG are not conformed with, then it is possible that an organisation's website will not be accessible to all visitors. This may lead to a decrease in the number of customer interactions and therefore a decrease in profits.

If the Equality Act is breached by an organisation, or by one of its employees, then financial penalties can be imposed. The details of most breaches of the Equality Act are available publicly so it is highly probable that the reputation of the organisation will diminish if they are found guilty of the breach.

Research

Investigate breaches of the Equality Act.

What were the circumstances of the breaches and what was the outcome?

Discuss your findings with the rest of your group.

Test yourself

- 1 Identify two methods of digital communication.
- 2 What is the download speed defined by the USO?
- 3 How can assistive technology be used to increase inclusion?
- 4 Identify one adverse effect on individuals of the lack of digital inclusion.
- 5 What are the effects of the WCAG not being followed?

Project practice

A charity specialises in advising organisations about diversity and inclusivity. You have been asked to prepare a presentation, with speaker notes, to introduce organisations to the principles of diversity and inclusion.

You have also been asked to create an information booklet aimed at organisations. The booklet needs to provide details about diversity and inclusion including:

- ▶ legislation and regulation and how these can be conformed with
- ▶ the penalties for not conforming with the legislation and regulations
- ▶ the benefits of diversity and inclusion
- ▶ the positive effects of inclusion on an organisation
- ▶ the negative effects of not applying inclusion on an organisation.

Assessment practice

- 1 Describe, using examples, what is meant by demographics.
- 2 Define the term 'bias'.
- 3 Define the terms 'perceivable' and 'operable' as used in the Web Content Accessibility Guidelines.
- 4 Why is it important that the Web Content Accessibility Guidelines should be considered when creating a retail website?
- 5 Compare, using examples, direct and indirect discrimination.
- 6 Identify and describe three different types of discrimination that can be applied to the protected characteristic of disability.
- 7 Identify and describe two business benefits of diversity and inclusion.
- 8 Explain two approaches that could be used to address demographic imbalance in the digital sector.
- 9 Identify and describe two positive effects of digital inclusion on individuals.
- 10 Identify and describe two adverse effects on organisations when the principles of digital inclusion are not applied.

Core element 7: Learning

In this core element you will learn about the advantages of personal and professional development in the digital sector. The digital sector is constantly evolving with new developments in technology, updates to software packages, and new hardware and software being released by vendors. By continuing with personal and professional development, you can keep up to date with these developments and enhance your employment opportunities in the digital sector.

The digital sector is always creating and developing emerging and innovative technologies. You will learn about some of these technologies and their applications in the commercial and domestic contexts. Some emerging technologies have been developed to provide very specific applications while others can be used for a range of applications in a range of settings.

In the digital sector many tasks and projects are carried out. You will learn how design thinking enables the task or project to fully meet the needs of the end users. Mistakes are made during the completion of tasks and projects. It is important that you learn from these mistakes to help improve your performance when carrying out future tasks and projects. You will learn about reflection techniques that provide a framework that you can use to reflect on the experience and mistakes. By using a reflective technique, you will be able to highlight your mistakes and shortcomings and use these as a basis for self-improvement.

For the completion of tasks and projects, you will need information sources. These sources will provide information and knowledge. You will learn about a range of information sources that can be used to gather information and knowledge. While selecting information sources, it is important that you can assess the validity and reliability of the information contained in them and the knowledge you will gain from them. You will learn about the factors that you need to consider when assessing the reliability and validity of an information source as this will have an impact on the knowledge that you can gain from it.

Learning outcomes

In this core element you will learn about:

- 7.1** The advantages of personal and professional development in the digital sector
- 7.2** Areas of emerging technology and innovative applications within a commercial and a domestic context

7.3 Types of reflection and creativity techniques and how they influence practice within the digital sector

7.4 Sources of knowledge within the digital sector and the factors that need to be considered when assessing the reliability and validity of a source

7.1 The advantages of personal and professional development in the digital sector

The digital sector seems to be constantly changing and evolving. As technology evolves in terms of hardware, software and the uses of the internet, for example cloud and edge services, so skills and knowledge can very quickly become out of date. The digital sector requires those who work in it to keep up to date with these changes which means an almost constant updating of skills and knowledge. This is referred to as **personal and professional development**. Many of the professional bodies related to the digital sector offer courses leading to accreditation in a range of areas.

There are many advantages to completing personal and professional development when working in the digital sector. One advantage is that you can achieve an increase in competence and knowledge. This is important as there is constant development in the digital sector. You can gain knowledge about updates to software, technological changes in hardware, and the evolving development of new and emerging technologies, such as quantum computing and extended reality (XR), through professional development.

By completing professional development and keeping up to date with advances in the digital sector it is possible that you can increase your employability potential. For example, it could mean you can apply for different types of job roles or gain promotion. By completing professional development it is also possible to increase your employment security. This is because there is a demand for skilled digital sector professionals who can develop, use and maintain up-to-date technologies including hardware, software and emerging technologies to meet the needs of their employers and end users. The completion of professional development can also help to ensure that the skills and knowledge you acquire are relevant to your employer, maintaining currency and relevance to industry.

There are many professional bodies related to the digital sector. These include the British Computer Society (BCS), Institution of Analysts and Programmers (IAP) and the Chartered Institute of Information Security (CIISec). It is advantageous to join a professional body when working in the digital sector.

Professional bodies related to the digital sector, their codes of conduct and industry standards are covered in section 8.3, p. 206.

It is possible to join more than one professional body, but you should consider the time and cost implications before doing this. At the start of a career in the digital sector it may be beneficial to join one and then join another one, or more, at a later stage when you are carrying out different job roles.

By joining a professional body, members can:

- ▶ access professional development courses
- ▶ gain accreditation for a specific job role or discipline
- ▶ gain knowledge about recent and emerging technologies
- ▶ network with others carrying out the same job roles.

Most professional bodies run conferences on topics such as emerging technology where, for example, updates in the digital sector are discussed and considered. The conferences are also a way of increasing members' professional networks.

Joining a professional body can also increase your employment opportunities and security. This is because there is a standard of knowledge and skills that has to be achieved before membership is granted at the higher levels. Joining a professional body and maintaining the membership requirements will demonstrate to an employer your motivation, ability and aptitude, to continue learning by completing professional development.

Many of the professional bodies related to the digital industry are involved in developing, and maintaining, industry standards. Membership of a professional body will ensure that these industry standards are known about, understood and adhered to.

Research

There are many different professional bodies related to the digital sector. Get into groups of two or three. Each group should select a different professional body and research:

- ▶ the benefits provided to its members
- ▶ the different levels of membership and how these can be achieved.

Present your findings to your teaching group.

Test yourself

- 1 What is professional development?
- 2 Identify one way employability potential can be increased.
- 3 Why is employment security increased when professional development has been completed?
- 4 What can members access as part of their membership of a professional body?
- 5 What are professional bodies related to the digital sector involved in?

In 2021 DNA data storage began to be used in an experimental way. One of the main sectors where DNA data storage was beginning to be used experimentally was in molecular storage for biotechnology.

Research

One experiment relating to DNA data storage was the Stanford Bunny.

Investigate this experiment and create a leaflet aimed at non-digital specialists about the experiment.

7.2 Areas of emerging technology and innovative applications within a commercial and a domestic context

New technologies seem to be created within the digital sector every day. Some of these emerging technologies are updates and improvements on current technology but some are innovative. All developments within the digital sector have an impact, in some way, on both the commercial and domestic contexts.

New mediums for storing information

Information and data used to be stored in proprietary file formats, which depended on the type of data and information being stored. For example, text could be stored in a word processing file format, while spreadsheets were used to store numbers, perform calculations and create graphs. The amount of digital data being produced and needing to be stored is growing exponentially compared to the amount of storage space on magnetic and optical media available.

It is now possible to store data and information in a range of different mediums. DNA data storage is the process of algorithmic coding and decoding of binary data using synthesised strands of DNA – our genetic material.

DNA data storage is able to store up to 1 exabyte per cubic millimetre. But, because of the high cost and very slow read and write times, the use of DNA storage is still very limited in its application.

The DNA Data Storage Alliance (DDSA) was formed in 2020 by Microsoft, Twist Bioscience, Illumina and Western Digital. The aim of the alliance is to

'organize the industry and think of how to build the whole ecosystem for DNA data storage.'

Quantum

Quantum is a rapidly developing area and is based on three principles:

- ▶ Entanglement
- ▶ Interference
- ▶ Superposition.

Quantum computers

Quantum computers are, in 2021, still in the research and development stage and have not, at the time of writing, moved into mainstream use. Research and development in areas related to quantum is currently being carried out by different companies and academic institutions including:

- ▶ Cambridge University
- ▶ Google
- ▶ IBM
- ▶ Microsoft
- ▶ MIT
- ▶ Oxford University.

Activity

Find and watch the Beginners Guide to Quantum Computing by IBM Research. Discuss the contents of the video with the rest of your group.

The theory behind the processing used by quantum computers has its roots in quantum theoretical physics and the observable state of anything; in the case of a quantum computer, the anything are the bits, known as qubits.

A quantum computer carries out calculations and operations in a different way to the standard computer. Standard computers carry out calculations and logical operations using bits in a binary state, 1 or 0, on or off. This is known as a 'definite position of a physical state'.

A quantum computer performs operations and calculations based on the probability of an object's

state, the quantum state, before it is measured or observed. This is the qubit.

Quantum computers view the qubits as being on or off or in both the on and off state at the same time. This is known as a superposition. This can be explained by Schrodinger's cat theory.

Activity

Find and watch the explanation of Schrodinger's cat by the character Sheldon Cooper, in The Big Bang Theory.

Another analogy can be when a coin is tossed in the air. Until the coin lands it is not possible to clarify if the coin is showing heads or tails as it is spinning, the superposition. It is only when the final state is observed, when the coin lands, that it can be seen if it has landed heads or tails. It is at this point that the superposition has collapsed and moved to a physical state.

Quantum computers use a number of qubits when processing calculations and logical operations. Each qubit is in a superposition. Pairs of qubits can be entangled. This means that the state, superposition, of one qubit is not able to be changed without affecting the state of the other qubit it is entangled with. The state of the first qubit, therefore, can be 'read' by looking at the behaviour of the qubit it is entangled with. This means that the outcome of the operation or calculation will be mathematically related, but the definitive answer will not be known until the final state of the qubit is known – the physical state.

An algorithm is used to solve the maths involved in the superpositions of the entangled qubits. The algorithm enables complex problems to be solved very quickly. It is unlikely that the complex problems that can be solved by a quantum computer would be able to be solved by a standard computer.

Algorithms are covered in sections 4.1 and 4.2 p. 101–110.

Potential applications of quantum computers

The real-world applications of quantum computers are still largely unknown. It has been mooted that the potential applications could include:

- ▶ analysis of big data sets
- ▶ AI
- ▶ cyber security including producing security codes and encryption keys
- ▶ financial modelling
- ▶ mathematical and science-based problem solving

- ▶ medical drug development
- ▶ weather forecasting and climate change modelling.

Activity

Find, and listen to, the podcast from Oxford University Futuremakers called 'Could quantum computing change the world?'

The quantum internet

It is thought that a quantum internet could enable quantum computers, and other quantum devices in the future, to be interconnected and communicate using teleportation of qubits. This will match the pattern of the internet which enables digital devices to be interconnected and share information and data.

The quantum internet will consist of a network of many remote quantum computers. The qubits will be sent between these connected quantum computers. The qubits will be sent in the superposition state, but, as the distance between the source and destination quantum computers increases, the qubits may collapse to their physical state.

At the moment, qubits can degrade or get lost when using a traditional transmission method like fibre-optic cables. This means that quantum signals between quantum computers have a high error rate and cannot travel over long distances. However, it is hoped that information from one entangled qubit could be transmitted (teleported) to the other entangled qubit without having to use any traditional physical methods.

The quantum internet will not be used as the internet is used today. It will not be used to share data and information, photographs or communicate with each other. The most probable use of the quantum internet is in cyber security.

Quantum cryptography

In the 'normal' world, data is kept secure by using a key which is shared between the sender and receiver of the data. This key is used to encrypt the data by the sender. The receiver uses the same key to decode the data.

The encryption keys are generated using an algorithm. The encryption keys created by the algorithm are difficult to decipher but not impossible. By moving the process of creating encryption keys to quantum technology, the probability that the keys can be deciphered can be decreased. This process is called quantum key distribution (QKD).

Encryption is covered in section 10.4, p. 246, and section 10.6, p. 252.

The process of QKD entails a classical encryption key being coded into qubits. These qubits are sent to the receiver who measures the qubits to gain the key values. Currently, the qubits are sent through optic-fibre cables. But, as with the concept of the quantum internet, the qubits degrade during transmission which can affect the level of security of the quantum key.

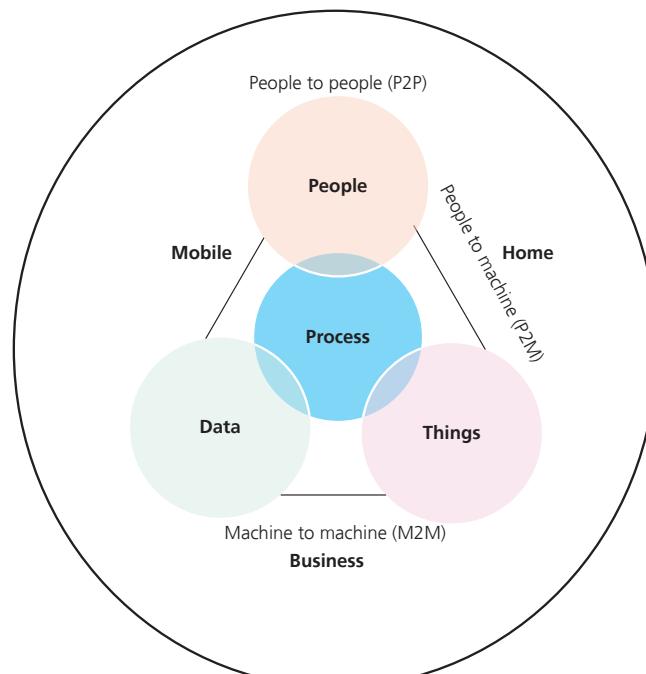
Test yourself

- 1 How much data can be stored in DNA data storage?
- 2 What are the states of qubits?
- 3 Identify two possible applications of quantum computers.
- 4 In what position will qubits be sent in the quantum internet?
- 5 What does QKD stand for?

Internet of Things

The Internet of Things (IoT) is a system of interrelated, internet-connected objects which collect and transfer data over a wireless network without human intervention. It is built on a connection between people, processes, data and things. These are called the pillars. Each pillar increases the capabilities of the other three pillars.

The IoT is also covered in section 5.2, p. 127.



▲ Figure 7.1 The Internet of Everything

People

The way people connect to the internet has changed dramatically over the last two to three decades. People now use wearable technologies and smart devices which have transformed the way we obtain and share information. There are self-monitoring devices such as the 'Fitbit' that allow people to track exercise, monitor the function of vital organs such as their heart, and even the quality of their sleep. It is the connecting of people in the most relevant and valuable ways.

Process

The Internet of Things (IoT) is a network of physical objects. These objects are the 'things'. They are embedded within software, sensors and other technologies, which enables them to connect and exchange data with other devices and systems over the internet.

The IoT has revolutionised the way organisations work and how they manage their business. Think of an e-commerce company such as Amazon and how people's shopping habits have changed by buying online, combining the convenience of shopping from home with fast delivery times. (Of course, this also has a negative impact on the high street stores.) The process comprises the delivery of the correct information to the correct person/machine at the correct time.

IoT sensors are used in warehouses by businesses like Amazon. They use IoT sensors to monitor the operating conditions of equipment and machinery and the data captured is processed and analysed by advanced machine learning algorithms. This enables the operators to predict failures of equipment e.g. forklift failure and other critical handling equipment. Warehouse managers can then address the problems promptly, minimising the risk to a reduction in productivity by keeping costs and downtime to a minimum.

Data

Data can be maximised into more useful information for decision making. The world is flooded with data and one of the main functions of the IoT is to gather huge amounts of data to improve operations and functionality. Data could be hours of footage from a surveillance camera, how much exercise you have done in a day, what TV programmes people watch and so on. These are examples of individual data but imagine the vast amounts of data that can be collected, processed and analysed from organisations on a global scale. Consider social media platforms such as Facebook, Twitter, LinkedIn and so on and how much data they collect.

Things

These are the physical devices and objects connected to the internet and each other for intelligent decision making. There are many devices in a domestic context that people can interact with on a daily basis that are connected to the internet. Mobile phones can be used for online banking, paying for goods or just checking the weather. The lighting and heating in homes can be controlled by smart devices connected to the internet.

Research

Investigate the range of domestic devices that can be connected to the IoT.

Create a digital communication detailing the purpose, advantages and disadvantages of each device. The leaflet should be aimed at people aged 11 to 14.

The personal and business possibilities from the IoT are vast.

Businesses are motivated to use the IoT due to the opportunities for increasing profits, reducing operating costs and improving the efficiency of the business. The IoT provides data which can be analysed to:

- ▶ automate work processes and streamline workflow
- ▶ develop visualisation patterns of usage
- ▶ enable organisations to effectively compete in a continuously changing business environment.

Research

Research two different business sectors, for example retail and entertainment, and how the IoT has been implemented in them.

Produce an infographic highlighting the key outcomes from your research.

Artificial intelligence

AI is the development of computer systems to perform tasks that would normally require human intelligence. This can include speech recognition, visualisation or visual perception, decision making and translations between languages. Therefore, it is the development of computer systems to think and work like humans. The purpose of AI is to learn and solve problems without the intervention of humans. This can lead to computer systems being able to make accurate decisions without human involvement.

There are two main types of AI. These are:

- 1 Weak AI, which can also be known as narrow AI, where the AI only focuses on one task, for example diagnostics based on user input. These are usually programmed by a person therefore tend to simulate the actions of a human.
- 2 Strong AI, which can carry out a range of functions and can eventually learn to solve a new problem. Autonomous cars are an example of strong AI.

Artificial intelligence, machine learning and deep learning

First of all, you need to understand the difference between AI, machine learning and deep learning.

- ▶ **AI** – the development of computer systems to perform tasks that would normally require human intelligence. This can include speech recognition, visualisation or visual perception, decision making and translations between languages. Therefore, it is the development of computer systems to think and work like humans.
- ▶ **Machine learning** – an application of AI where computer systems automatically learn and improve with experience without being programmed. The focus is on the development of computer programs that facilitate access to data which is used to allow it to learn for itself.
- ▶ **Deep learning** – a function of AI that imitates how the human brain works with respect to the processing of data and creation of patterns in order to make decisions. This is sometimes referred to as deep neural learning or deep neural networking.

Because machine learning can access and learn from vast amounts of data it is used effectively in the manufacturing sector. Machinery is linked to the network and there is a constant stream of data being provided on the functionality and production rate of each machine. This is sent to a local point for analysis. Because this data can be so vast it is difficult for a human to analyse it all quickly and therefore critical situations can be missed. Machine learning quickly analyses data, identifies patterns and can therefore identify anomalies promptly. If a particular piece of machinery is not functioning as required, this will be quickly identified and the decision-makers within the organisation will be notified. They can then immediately address the problem. Because the machine is learning as it works, it becomes faster at identifying patterns and problems.

Deep learning is a more specific version of machine learning and uses neural networks to facilitate **non-linear thinking**. This is critical to performing more advanced functions by analysing a wide range of factors simultaneously. Consider self-driving cars. Deep learning is used to contextualise information picked up from the car's sensors, for example the distance from objects, the speed of travel and a prediction of where they will be over time. All of these are calculated at the same time so that the car can make decisions rapidly, such as stopping quickly or changing lanes.

Machine learning algorithms can tend to reach a state where there is little or no change. Deep learning models, however, continue to improve their performance as more data is received. Therefore, deep learning models are more scalable and detailed, and far more independent.

The challenges of AI on society and individuals

AI will require the workforce to evolve. Many people are fearful that jobs will be lost to machines. The challenge is to encourage humans to motivate themselves by taking on new responsibilities that require the unique abilities of humans.

AI will have economic, legal and regulatory impacts on society that need to be prepared for. Consider again, the self-driving car. Who is at fault if a person is injured coming into contact with a self-driving car?

It is important that AI does not become so good at doing the work intended that it crosses the ethical and legal boundaries. Any AI algorithm must be developed to align with the goals of humans.

Of course, there is also the issue of privacy being compromised due to the collection of data about every minute of every day of people's lives. If businesses and governments make decisions based on the intelligence they gather about people, it could devolve into social oppression.

Key term

Non-linear thinking: the ability to make connections and draw conclusions from unrelated concepts or ideas.

Positive impacts of AI on society and individuals

AI can improve dramatically the efficiency of the workplace and the work humans do. AI can take over repetitive and dangerous tasks which allows the human workforce to carry out work that involves creativity and empathy. If a person carries out work that is more engaging for them they are happier and have job satisfaction.

AI has had a real positive effect on the healthcare sector as it helps to improve the monitoring and diagnostic capabilities when dealing with patients. These improvements can reduce operating costs and therefore save money which is needed to employ more staff. Personalised treatment plans for patients and drug protocols, as well as wider access to information across medical facilities, which help to inform patient care, are important positive aspects of the implementation of AI.

AI in organisations

AI can save businesses time and money, as well as increasing productivity and improving operational efficiency. This is achieved by automating and improving tasks, workflow and processes.

AI includes the use of cognitive technologies that can make faster business decisions based on resulting outputs from other processes. Cognitive technology is a product within the field of AI that is trained to think and behave like a human. Think of the use of robotics for building cars. They can carry out the actions a human would do and do not need to stop working for breaks etc. There is always a risk of human error within any task that is carried out. A good AI system will avoid mistakes and 'human error'.

Quality data analytics also benefits from the use of AI as it can be programmed to process vast amounts of big data which a business can use to make constructive and effective business decisions.

Extended reality

Extended reality (XR) is a mixed reality environment that combines virtual and real-world environments and realities. There are different forms of XR including:

- ▶ augmented reality (AR)
- ▶ virtual reality (VR)
- ▶ mixed reality (MR).

Augmented reality

Augmented reality is covered in section 3.6, p. 89.

- ▶ **Visualisation** – when an object or concept is brought to life which otherwise could only be imagined, inaccessible or difficult to understand.
- ▶ **Annotation** – using AR to guide someone through a task, navigate a new environment or provide real-time descriptions of what is happening around them. This has been used in the workplace for field service repairs and training where experts annotate what the engineer is looking at to guide them through the repair process. This remote assistance concept has been extended to healthcare scenarios in remote locations where medical experts, such as consultants, may not be readily available.
- ▶ **Storytelling** – AR changes the way we tell, share and even remember stories by ‘bringing them to life’. The National Gallery in Prague uses **haptics**, to help visually impaired people to experience the artwork. By wearing haptic gloves, the person can visualise 3D virtual sculptures through a series of touch vibrations to the fingertips, palms and hands.

Virtual reality

VR is the computer-generated simulation of a 3D image or environment. It can be interacted with in what appears to be a very real or physical way. People need to use special electronic equipment such as a helmet with a screen inside, VR glasses and gloves fitted with sensors.

VR has been implemented by the military within the UK and USA to train military personnel. VR can be used to transport military personnel into a wide variety of locations, situations and environments. Such examples currently in use include flight simulations, battlefield simulations, vehicle simulations and medical training. VR is totally immersive with a visual and sound-based experience available. It can replicate dangerous situations to train and prepare military personnel without putting them at risk. A key benefit to using VR for training (besides the decreased risk to the well-being of the personnel) is the reduction in costs.

Key term

Haptics: using technology to stimulate the senses of touch and motion to reproduce the sensations that would be felt by someone interacting directly with the physical object.

VR has also been used in schools where students are able to interact with each other in a virtual environment which is 3D. Students can be taken on virtual field trips, for example museums, and go back in time for history lessons.

The fashion industry is also adopting the use of VR by creating virtual simulations of their retail outlets. This helps businesses to design their signage and product displays before committing to a costly redesign of their premises. Some retailers offer a 360° experience to their customers so that they can try on clothes virtually.

Research

Virtual and augmented reality can have positive and negative impacts on society, individuals and organisations.

Research the use of AR and VR within the tourism sector and create a presentation with speaker notes explaining the positive and negative impacts.

Mixed reality

MR blends the real-world environment and digitally created content which coexist and interact with each other in real time. This means that MR is not just real world or virtual but is a mix of reality and virtual reality. It is this mix that provides the name.

MR includes a link to the real world so is not a fully immersive experience. The content seen through MR will react in the same way as in the real world. For example, as a user moves closer to an object, it will move closer to the user. It is then possible to interact with the object, for example turning it using a gesture.

To use MR an MR device is needed to be able to create the experience. The MR device could be a headset or translucent glasses with motion controllers. However, MR does use greater amounts of processing power than VR or AR.

One application of MR is in the car industry. Car manufacturers are using MR technology when prototyping new cars in a virtual environment. Other possible applications of MR are in engineering and design modelling.

MR takes the best features from VR and AR to create the latest iteration of immersive technologies. However, is the next iteration a combination of VR, AR and MR which would enable a user to move between these based on their defined needs in a specified moment in time?

Research

Investigate the many MR products available.

Create a digital communication providing details of how they work, and their advantages and disadvantages.

Test yourself

- 1 Identify the four pillars of IoT.
- 2 Explain the term 'deep learning'.
- 3 Describe the impact of AI on society.
- 4 Explain the difference between AR and VR.
- 5 Identify one example of how VR is used by the military.

Blockchain

A blockchain is a chain of blocks that stores data and information. When data is recorded in a blockchain, it is extremely difficult to change or remove it. For example, it is not possible to change the properties, for example the date stamp, of any digital documents or **transactions**. The data and information stored in a block depend on the purpose of the blockchain. Blockchains enable a permanent record and histories of transactions. However, the permanence of the record is based on the permanence of the network.

For example, a blockchain can be used to securely transfer money without requiring a third-party intermediary like a bank. When data is stored in a blockchain, it is very difficult to change it.

Blockchains are a software protocol and need the internet to be able to function. Blockchains are referred to as meta-technology as they are made up of several technologies including a database, a software application and internet-connected digital devices.

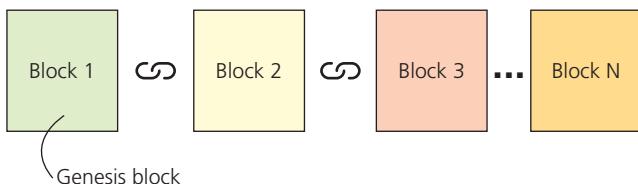


Figure 7.2 Blockchain is a chain of blocks containing data

Key term

Transaction: when something is added to a blockchain. Also known as an entry.

The initial block in the blockchain is known as the Genesis block. As Figure 7.2 shows each block in the chain is linked to the previous one. As new blocks are added, they are added to the end of the chain.

Each block contains three items:

- ▶ data/information
- ▶ hash
- ▶ hash of the previous block.

Each block includes a hash which is unique to that block. The hash identifies the block and the data/information it holds. When the contents of the block change, the hash changes. As all blocks contain the hash of the previous block in the chain, it is this that makes blockchains so secure.

Figure 7.3 shows how a transaction can be added to a blockchain. Users in the network who have validation control verify the proposed transaction and either agree or block the transaction.

There are several different types of blockchain including public, permissioned and private blockchains.

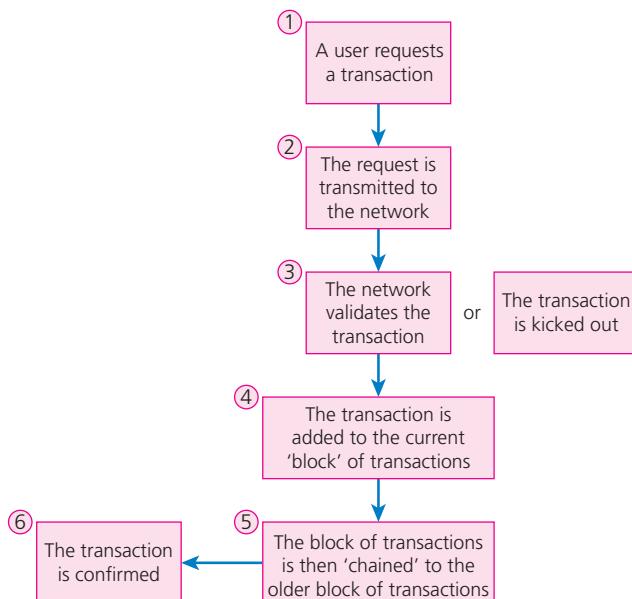


Figure 7.3 Adding a transaction to a blockchain

Public blockchains

Public blockchains are large, distributed networks that operate using a native token. Anyone can participate at any level. The public blockchain usually has open-source code that their community maintains. An example of a public blockchain is Bitcoin, but:

- ▶ a blockchain is the technology that facilitates Bitcoin but is not Bitcoin

- ▶ Bitcoin is a digital token with the blockchain keeping a record of who owns the digital token in a ledger
- ▶ you cannot have Bitcoin without blockchain, but you can have blockchain without Bitcoin.

Permissioned blockchains

Permissioned blockchains control the roles that people have when managing or accessing the blockchain network. This type of blockchain is usually a large and distributed system that uses a native token. The code may or may not be open source. An example of a permissioned blockchain is Ripple.

Private blockchains

Private blockchains are smaller than public and permission blockchains. A private blockchain does not usually need a token for access. As the name suggests the number of people who can access a private blockchain is controlled and limited. Private blockchains tend to be used by consortiums who have very trusted members who trade confidential information.

Activity

Research the other types of blockchains including hybrid, consortium and permissionless.

Create a digital communication to explain your findings to the rest of your group.

Test yourself

- 1 What is a blockchain?
- 2 What is the first block in a blockchain called?
- 3 Identify one item that a block contains.
- 4 What is the purpose of a hash in a block?
- 5 Identify one type of blockchain.

Application of 3D printing

3D printing is the process of making a three-dimensional object from a digital file. The object is created using an additive process. This means that thin layers of material are added on top of each other until the object is completed. Each of these layers is a thinly sliced cross-section of the object.

Some of the **advantages** of 3D printing are explored here.

Cost

3D printing only uses one machine – a 3D printer. This means that only one machine has to be bought

instead of lots of machines as is typically the case in the traditional manufacturing process. Because there is only one machine, the time cost is also reduced. Once the 3D printer has begun to create the object, no further intervention is required.

Limited wasted materials

A 3D printer will only use the exact amount of material to create the object. This is because the process is additive, so when the object is finished the process stops. In traditional manufacturing there is always waste which is usually non-recyclable. This also has a cost advantage as it reduces the amount of materials needed.

Quality and consistency

The creation of the object is taken from a digital file where the object has been designed using a **CAD** package. This means that once a prototype object has been created and, if necessary, amended, the 3D printer will create the same object to the same quality and design each time the file is accessed. This means that the final object created from the file will be exactly the same in terms of quality and consistency as the first object.

Some of the **disadvantages** of 3D printing are explored here.

Manufacturing job losses

Typically many machines are used in traditional manufacturing to create objects. Using a 3D printer means that the number of people needed to operate the machinery is reduced. This means that job losses are inevitable if manufacturing moves to the use of 3D printers.

High initial capital outlay

3D printers and the materials used to create the objects are expensive. This can, in turn, lead to a higher cost to customers for the object. However, a company could send their design files to a 3D printing company or hire a 3D printer, instead of buying a printer themselves.

Uses of 3D printing

There are many uses and applications of 3D printing including:

- ▶ architectural scale models
- ▶ entertainment, including props for theatre and film
- ▶ fashion, including clothes, footwear and eyewear
- ▶ home furnishings, including furniture

Key term

CAD: Computer Aided Design.

- ▶ industrial products, including manufacturing tools, prototypes, car and consumer parts
- ▶ medical, including dental and prosthetics.

Research

Investigate 3D printing including the advantages and disadvantages, and applications.

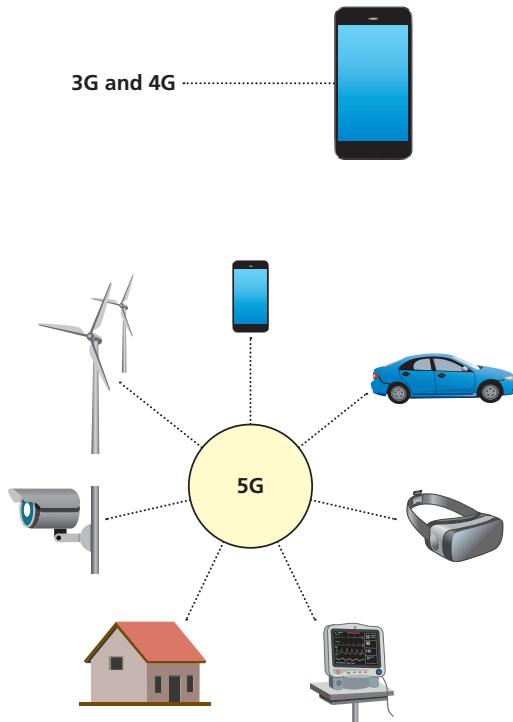
Create a digital communication aimed at manufacturing students explaining your findings.

Test yourself

- 1 What is 3D printing?
- 2 How is a 3D object created?
- 3 What does CAD stand for?
- 4 Identify one advantage of 3D printing.
- 5 Identify two applications of 3D printing.

5G

5G began to be rolled out in the UK in 2018 as the new generation of wireless technology.



▲ Figure 7.4 The difference in connected devices between 3G, 4G and 5G

The 5G mobile telecom network follows on from the rollout of 3G and 4G. The introduction of the 3G network led to the introduction of the smartphone while 4G provided a faster mobile browsing experience.

5G is designed to provide faster download speeds, low **latency** and greater capacity.

5G cells expand mobile networks by boosting capacity as users need it, for example in a sport stadium or festival. They can extend coverage by using indoor cells that use internet connections to ensure people always have a signal. Low latency is one of the main advantages, meaning the closer network processing is to the user, the lower the latency times. Spectrum offload can also be utilised, which allows operators to offload traffic from busy areas to relieve congestion through tighter frequency re-use.

5G also enables billions of devices to be connected, including in the areas of virtual reality, the Internet of Things and AI. 5G technology can achieve this by conforming to the eight specification requirements of:

- ▶ up to 10 Gbps data speed
- ▶ 1 millisecond latency
- ▶ up to 1000 times the bandwidth per area compared to 4G
- ▶ up to 100 times the number of connected devices per area compared to 4G
- ▶ 99.999% availability
- ▶ 100% coverage
- ▶ 90% reduction in network energy usage
- ▶ up to 10-year battery life for low power IoT devices.

The applications of 5G could include:

- ▶ driverless vehicle navigation systems
- ▶ drones and robotics
- ▶ industrial and manufacturing real-time monitoring and communication systems
- ▶ medical monitoring systems.

However, it is important to consider the level of security and privacy. With the increased availability of 5G services, more sensitive data will be transferred over the 5G network as well as the increased use and accessibility of devices connected to the IoT.

Key term

Latency: the delay between the instruction for transfer and the start of the transfer.

Research

Investigate the possible applications of 5G, for example Smart Cities.

Create a digital communication explaining the applications, including the advantages and disadvantages.

Test yourself

- 1 Identify two specification requirements for 5G.
- 2 What is latency?
- 3 What are drones also known as?
- 4 How can drones be flown?
- 5 Identify one use of drones.

Drones

A drone is an aircraft without a pilot, crew or passengers onboard. A drone is also known as an unmanned/uncrewed aerial vehicle (UAV).

A drone can be controlled (flown) by remote control by a human operator; this is known as a remotely piloted aircraft (RPA). Drones can also be flown with a range of autonomy such as using autopilot for some of the flying time, up to fully automated flying with no human intervention.

Drones were originally developed for use by the military, but they have now expanded into commercial and personal use. The military developed drones for times when the use of traditional aircraft is too risky. Drones can provide the military with 24/7 surveillance, known as 'the eye in the sky'. Drones can stay in the air for approximately 17 hours which enables surveillance over an area while constantly sending a real-time video stream back to the control centre on the ground.

The use of drones has now expanded into a range of areas, including:

- ▶ archaeology research
- ▶ disaster relief
- ▶ emergency services investigations
- ▶ film and tv
- ▶ infrastructure inspections.

To fly a commercial or personal drone in the UK, the **CAA** require users to register and take a test which must be passed before the user can legally fly. The CAA has also created a code (The Drone & Model Aircraft Code) which is legally binding.

Research

Investigate the uses of drones. Select one use from your investigation.

Create an infographic, including text and images, explaining how drones are used and the benefits and limitations.

7.3 Types of reflection and creativity techniques and how they influence practice within the digital sector

At the end of each project or task there is an opportunity for evaluation or reflection. It is also possible to use a reflective technique to evaluate and reflect on a new situation or a process that is being considered for implementation.

Meaningful reflection is both cognitive and emotive. The process of reflection techniques includes stepping back and questioning a range of areas including emotions, feelings and actions.

Many people find that they learn from experience or doing. But, if they do not reflect on the experience, including how they could do better next time, they may not learn from their experience.

Reflection techniques

There are three reflective techniques that are included in this course:

- ▶ Kolb's experiential learning cycle
- ▶ Gibbs' reflective cycle
- ▶ Boud, Keogh and Walker's model.

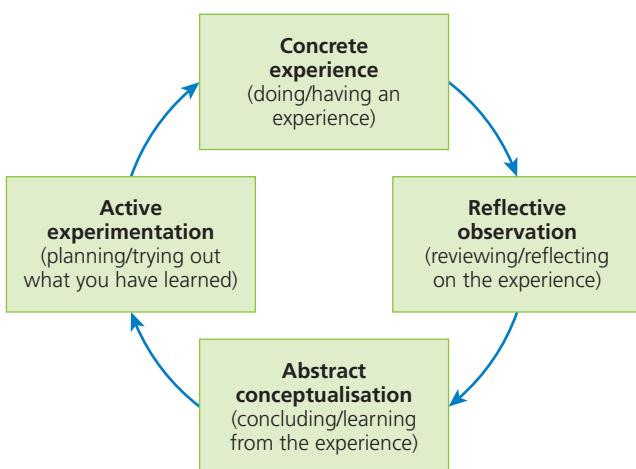
Kolb's experiential learning cycle

Kolb developed his theory of experiential learning cycle in 1984 with the basic premise that people learn through doing – the direct experience. The theory focuses on an individual's perspective and personal development and that the learning process is guided by the individual.

Kolb defines four stages which can be seen to be a circle or cycle as shown in Figure 7.5. Each stage builds on the knowledge and skills developed, with the whole process being seen as a holistic approach where

Key term

CAA: Civil Aviation Authority.



▲ Figure 7.5 Kolb's experiential learning cycle

ideas are continuously created and implemented for improvement. Learning is only effective when each of the four stages has been completed. The four stages of Kolb's theory are outlined here.

1 Concrete

In the first stage an individual has an experience that is the basis for observation. The new experience creates an opportunity for learning. Kolb states that an individual cannot learn from just reading or observation. The focus of this stage is that the individual takes part in the experience so that they can learn from it – learning through feelings or experiences.

2 Reflective observation

In the second stage the individual reflects on the experience from the concrete stage. This is known as reflective observation. This means reviewing, reflecting on, what has been done and experienced from a personal viewpoint. In this stage, the change from seeing and doing to reflection can increase the understanding of the experience. For example, an individual is shown how to successfully complete a task and during reflection considers how it could be applied in different situations. This should include any inconsistencies that have occurred between experience and the understanding. The focus of this stage is the review of the experience and the meaning of the experience.

3 Abstract conceptualisation

In the third stage an individual will create new ideas or change their current abstract ideas based on the reflections from stage 2 – reflective observation. In this stage it is possible to identify how previously learned ideas can be applied to their situation. It is also possible that theories will be developed based on previous experiences. Recurring problems, commonality and issues can be

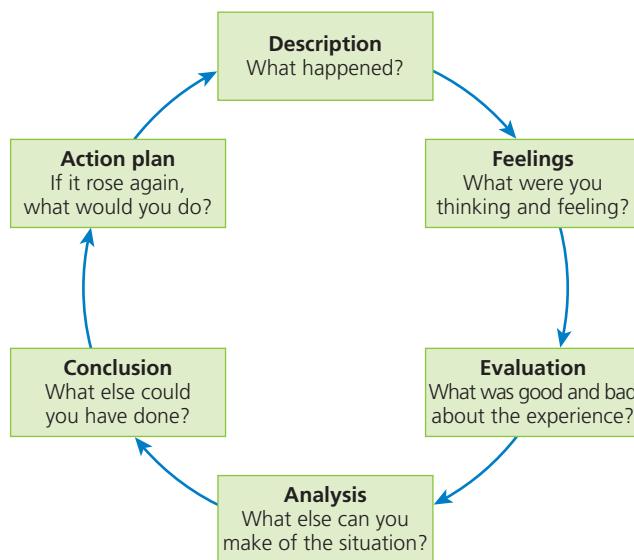
identified which can be taken forward to create ideas and theories which can be applied in the future. The focus of this stage is learning from reflections and thinking.

4 Active experimentation

In the fourth stage the individual will learn from the practical application of ideas and consider how they are going to put what they have learned into practice, including how the learning can be applied to a different situation. This may include the consideration of any changes that may need to be made when the same experience happens again. This will allow them to develop theories and make decisions to solve the experience in the future. This will enable the individual to improve their reaction to the same or similar experiences in the future which will, in turn, result in new experiences.

Gibbs' reflective cycle

Gibbs published his reflective cycle theory in his 1988 book *Learning by Doing*. His theory has become one of the most well-known and used reflective theories.



▲ Figure 7.6 The six stages of Gibbs' reflective cycle

Gibbs defines six stages of reflecting on experience which are shown in Figure 7.6. Each stage has questions that need to be answered before moving onto the next stage. Answering these questions will enable the reflection process to be as useful as possible. It is, however, very important that the questions are answered honestly and truthfully to be able to fully reflect on the experience or situation.

Using this six-step model should help to identify strengths, areas for development and actions that can be taken to enhance professional, and personal, skills. Stages 1 to 3 relate to what happened during the

situation, task or project. Stages 4 to 6 focus on how it could be improved and the outcome in the future.

The six stages are outlined here.

1 Description

In the first stage of the cycle, the situation, task or project needs to be fully described without making any judgements or coming to a conclusion. This stage is just about what happened, conclusions come later in the cycle. The description needs to set the scene and record the key components of the situation, task or project but must keep to being descriptive. Questions that could be answered in this stage include:

- ▶ When and where did this happen?
- ▶ Who was there?
- ▶ What did you and other people do?
- ▶ What was the outcome?

2 Feelings

In the second stage of the cycle, the focus is on the feelings and reactions that occurred during the situation, task or project. A description of the reactions and feelings is needed, but as with stage 1 no analysis or conclusion should be made. It can be very difficult to be honest about feelings and reactions, but to enable the process to be productive, honesty is the best policy. Questions that could be answered in this stage include:

- ▶ What did you feel before this situation took place?
- ▶ What did you feel while this situation took place?
- ▶ What do you think other people felt during this situation?
- ▶ What did you feel after the situation?
- ▶ What do you think other people feel about the situation now?

3 Evaluation

In the third stage of the cycle, the focus is on evaluating, or reviewing, the positive and negative actions and outcomes. The situation and the responses that were made are considered objectively in order to make the first value judgement. The situation should be considered from the perspectives of all the individuals who are involved. By doing this, it can be ascertained if the situation was a positive or negative experience for all or only some of the individuals. The focus should be on the positive *and* negative even if it was mainly one or the other. Questions that could be answered in this stage include:

- ▶ What was positive and what was negative?
- ▶ What went well and what didn't go well?
- ▶ What did you and other people do to contribute to the situation (either positively or negatively)?
- ▶ If you are writing about a difficult situation, did you feel that the situation was resolved afterwards?

4 Analysis

In the fourth stage the focus is on analysing, or reflecting, on the process and outcomes of the situation, task or project. This stage attempts to explain why the experience was positive or negative and should form the largest section of the reflection. At this stage ideas from outside the experience could also be considered. Points made in the previous steps should be considered and factors that helped should be identified, for example previous experiences, carrying out research or consulting with others. This is where sense should be made about what happened, using the theory and the wider context to develop understanding. Questions that could be answered in this stage include:

- ▶ Why did things go well or badly?
- ▶ How did you contribute to the success or failure of this experience?
- ▶ What was really going on?
- ▶ If things did not go to plan, why was this? For example, was it a lack of preparation or external factors beyond your control?
- ▶ Did other people involved have similar views or reactions to you? If not, why do you think that was the case?
- ▶ Could you have responded in a different way?
- ▶ What might have helped or improved things?

5 Conclusion

In the fifth stage the actions and outcomes from a situation, task or project should be summarised. Gibbs actually proposed two conclusions: a general one, which could be transferable and a specific one, focused on your personal situation. These are now normally merged but it is best practice to consider both. The conclusion should be based on the response to the previous stage(s) and focus on what has been learned.

Questions that could be answered in this stage include:

- ▶ What have you learned, generally and specifically?
- ▶ What can you now do better?
- ▶ Could/should you have done anything differently?
- ▶ What skills have you developed as a result of the situation, task or project?
- ▶ What skills do you need to develop to handle this better?

6 Action plan

The final stage is to formulate an action plan recording future plans and areas for improvement. This is based on the responses to all of the previous stages. The action plan should include anything that needs to be known and done to improve for next time. This stage should be considered as very important because formulating, and following, an action plan can inform

professional development and improvement. Questions that could be answered in this stage include:

- ▶ What can be done differently next time?
- ▶ What steps can be taken based on what has been learned?
- ▶ How will you adapt your actions or improve your skills?
- ▶ What specific actions can be taken to build knowledge or skills including training?
- ▶ How/where can you use your new knowledge and experience?
- ▶ If the same thing happened again, what would you do differently?

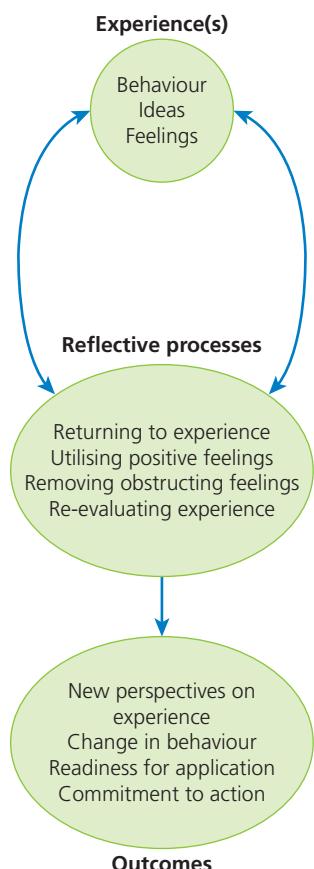
Research

Use Gibbs' or Kolb's theory and reflect on a practical task you have completed.

Create a document detailing your reflection for each stage of your chosen theory.

Boud, Keogh and Walker's model

Boud, Keogh and Walker developed their theory of reflection on practice in 1985 which focuses on learning by reflecting on practice.



▲ Figure 7.7 Boud, Keogh and Walker's model

They define three stages of reflection as shown in Figure 7.7. The stages can be revisited during the process of reflection. Anyone can reflect on their own practice to understand their activities and background to enable them to improve their work responsibilities.

The stages are outlined below.

1 Experience

This is the starting point of the reflective process; you return to the experience in this first stage. To facilitate reflective learning you need to return to the experience and consider what happened. In this stage, you consider the behaviour, ideas and feelings that occurred.

2 Reflective

During the second stage you reflect on the experience, including the feelings, behaviour and ideas that you identified in the experience stage. There is some iteration, as shown in Figure 7.7, between this stage and the experience stage. During the reflective stage, the negative feelings and behaviours you identified are removed, with the focus being on the positives that occurred. When you have removed the negatives during the reflective process, it is possible to return to the experience and view this in terms of only the positive behaviour, ideas and feelings. By doing this, you can return to the experience and re-evaluate it in a positive way.

3 Outcomes

The final stage expands on the positive reflection and perspective of the experience. By carrying out the previous stages, experience and reflective, you can gain new perspectives on the experience. These new perspectives will inform changes in your behaviour, being ready to apply these identified changes, and most importantly, being ready and able to commit to the changes that need to be made.

Test yourself

- 1 Identify the first two stages of Kolb's theory.
- 2 What happens during the active experimentation stage of Kolb's theory?
- 3 What is the second stage of Gibbs' theory?
- 4 Identify two questions that could form part of the analysis stage of Gibbs' theory.
- 5 Between which two stages of Boud, Keogh and Walker's model does iteration occur?

Creativity technique

Design thinking

This is a technique that can be used to identify solutions to a problem that may not be easily identified. The process of design thinking attempts to understand the end users by encouraging designers to 'think outside the box'. By doing this, the problem can be considered from an end user's perspective and focus can be on what is important for the end users – the user experience (UX).

When using the design thinking process, designers should understand and solve the evolving changes in users' environments and behaviours. The design thinking process is an iterative approach which encompasses ways of working and thinking, as well as a range of hands-on methods. The process includes research, prototyping and usability testing. The main focus of this process is 'what is important for the end users'.

There are five stages in the design thinking process. Each stage has a number of tasks, as shown in Figure 7.8.



▲ **Figure 7.8** The five stages of the design thinking process

It is important to remember that, although the stages are shown as a linear process, the design thinking process is an iterative one.

Stage 1 Empathise

In this stage the user needs should be identified and understood. This is likely to be completed by research, covering a range of demographics. An empathetic understanding of the identified users' needs must be developed. Empathy needs to be developed as this enables the design team to put aside their own views and assumptions to fully understand the users' needs rather than their own.

Demographics are covered in Core element 6.

Stage 2 Define

In this stage the information gathered in stage 1 is considered and analysed. The problem to be solved is clearly defined. This should also lead to ideas which will include, for example, functions, features and other concepts which may help to solve the identified problem. It is important that empathy with the users is still maintained. If empathy is not demonstrated, then it is possible that the solution will not enhance

Key term

Hypothesis: An idea or assumption that is suggested so it can be tested to confirm, or deny, its truth

the UX but match the assumptions of the design team. Questions can be asked which can help to formulate ideas to solve the problem. From this analysis, a **hypothesis** is created which will form the basis for solving the problem and leads to stage 3.

Stage 3 Ideate

In this stage ideas to solve the problem are developed. It builds on the understanding and knowledge from the previous two stages. This is the stage where the designers can 'think outside the box'. By doing this a range of alternative views of the problem can be formulated and alternative solutions to the problem can be identified. It is good practice to develop a range of solutions so that if one solution is found to be problematic, on iteration back to this stage, these other ideas can be taken forward. Any suggested solutions must be challenged to ensure that they conform to the defined users and their needs, rather than the assumptions of the designers. This means it is very important that the UX and the defined users and their needs are constantly considered and referred back to.

Stage 4 Prototype

In this stage, prototypes of a range of solutions, identified in the ideate stage, are created. The prototypes are not the complete solution but may focus on one, or more, feature, function or concept as defined in stage 2. This stage can also be referred to as the experimental stage as the prototypes created are experimental. The prototypes need to be considered and tested by a range of people, for example the design team, other teams, or a group of potential users. Based on the feedback provided, each prototype can be accepted, improved or rejected. As each improvement is made, the same process happens again. This forms the prototype feedback loop. At the end of this stage, any problems with the proposed solution are identified and the designers will know and understand how the users will behave, think and feel when interacting with the end product.

Stage 5 Test

In this stage, the prototypes evaluated and created in stage 4 are tested, with qualitative research carried out. Following testing and research, it is possible that previous stages will be returned to – iteration. This may be to redefine the identified problem including validating or disproving the assumptions made about the UX and user

needs, and the proposed solution. By using an iterative approach, alterations and refinements can be made and alternative solutions created. The UX and the solution should be considered in terms of the understanding of the users and the conditions of use, in order to empathise with how the users will think, behave and feel. During this phase, alterations and refinements can be made to rule out problem solutions and derive a full and complete understanding of the product and its users.

By carrying out the five design-thinking stages the final product should provide a solution to the identified problem which fully enhances the UX, meets the needs of the end users and provides a solution which can be used by a range of demographic groups.

Test yourself

- 1 What does the process of design thinking aim to achieve?
- 2 What is the first stage of the design thinking process?
- 3 What happens in stage 3 of the design thinking process?
- 4 Where does iteration occur in the design thinking process?
- 5 Who tests the prototype?

7.4 Sources of knowledge within the digital sector and the factors to consider when assessing the reliability and validity of a source

There are many sources of knowledge available. Some may say there is too much information and knowledge available. Finding reliable and valid sources of information and knowledge can be difficult.

Sources of information and knowledge

The different sources of information and knowledge available are explored here.

Academic publications

Academic publications include academic papers, research journals and magazines, also known as periodicals.

The main advantage of using these types of academic publications is that the focus of each is usually one topic/subtopic area. New and varied perspectives on these topics can be presented. The time taken

between the article being written and then appearing in the public domain can be relatively short, so the information and knowledge they provide is as up to date as possible. The version number, if provided, or date of publication, will help to check how up to date the publication is. This can also apply to textbooks, where it is possible for newer versions to be released to update the content. It is important to use the most up-to-date or current version.

One of the biggest disadvantages of academic publications is the level of language used, which can sometimes be inaccessible without a pre-existing good level of knowledge. Academic journals are generally more current than textbooks published at the same time. However, where a topic area is the subject of a lot of research it is possible that the time delay between submission and publication can be in excess of 18 months.

Textbooks usually focus on the theory element of a course, like this one, or a module. The aim is to provide an overview of the topics included in a course or module which can then be built on through directed research, case studies and questions. Textbooks are well researched to provide this overview and are quality checked by the different stages of the publishing cycle.

As the publishing process takes over a year between submission and publication, and with new and emerging applications in the digital sector, some elements of a textbook may become out of date very quickly. However, the basic fundamentals of the digital sector do not change.

Websites

There are a vast number of websites that can provide information and knowledge. These include forums, social media, blogs, statistical websites and wikis. Websites can be found using a search engine.

There are a range of search engines available. A search engine will provide a list of websites based on keywords that are input by the user. The websites will be provided on a search engine results' page (SERP). The results shown on the SERP will be based on an algorithm that ranks the results based on relevance to the user input criteria. The search engine algorithms aim to understand how users search and give them the best answer to their query. This leads to the highest quality and most relevant websites being at the top of the SERP.

Research

Search engines use three main processes, crawling, indexing and ranking, to provide results based on user input search criteria.

Investigate these processes and create a digital communication to explain how each process works. The communication's audience is students in years 8 and 9.

By using a search engine to locate relevant and useful websites, results including forums, social media, blogs and vlogs, statistical websites and wikis can be returned. While these may appear to provide information and knowledge it is important to consider carefully the validity and reliability.

The advantages of using websites to access information and knowledge include the speed. It is much quicker to input a search and have results returned, often within 5 seconds, compared to visiting a library to look for material. Websites tend to be more up to date than academic publications as they can be quick to update. Websites, particularly forums and wikis, tend to be focused on one specific area. For example, user forums can provide help and information when troubleshooting a technical issue. The chances are that someone on the website will have encountered the issue before and will be able to offer a possible solution.

Other websites that can be useful are blogs and vlogs. These can provide reviews of new technologies and opinions on topical issues in the digital sector. However, it must be remembered that the contributors to these may include unreliable information and biased opinions.

The World Wide Web (WWW) is not regulated: it is an open and democratic platform for all. This was one of the principles expressed by Tim Berners-Lee who is credited with developing the idea that became the WWW. However, he also predicted that his invention could, in the wrong hands, be a destroyer of worlds.

As the WWW is unregulated, anyone can create a website about anything. Material, information and views which are on a website are not quality checked meaning that some of the information can be unreliable or not of an acceptable academic standard.

As the number of websites increases every day, this is also causing a problem with locating information and knowledge on the WWW. The number of results of a user search provided on the SERP can be very large. This means that it can become very difficult to identify the best and most reliable results.

Research

Some of the negative aspects of the WWW include fake news and breaches of user data.

Investigate the negative aspects of the WWW, giving examples.

Discuss how the WWW could be transformed into the concept created by Tim Berners-Lee.

e-learning

e-learning is learning that takes place electronically, usually on the WWW. Learners use connected digital devices to access the e-learning course, which can also be known as an e-learning package. The biggest advantage of e-learning is that learners can access their courses anywhere or at any time as long as they have a Wi-Fi or data connection.

As e-learning is delivered electronically, there are many different formats of resources that can be used. Many e-learning courses include resources such as videos, text files, animations, audio and so on, providing guidance for practical skills and interactive quizzes to check progress.

Many e-learning courses can be delivered through **MOOCs**. They are known as MOOCs because they are:

- ▶ massive – the number of learners taking the course can be very large as there is no limit on numbers, unlike a course run in a physical environment
- ▶ open – anyone can take part in the courses – there is no admissions process
- ▶ online – this is obvious, because the courses are delivered online
- ▶ course – the courses teach a specific subject.

It is also possible to complete recognised vendor qualifications through e-learning. This includes qualifications from Cisco, Microsoft and CompTIA. Completing e-learning vendor qualifications can contribute to professional development within the digital sector.

The advantages of professional development are covered in section 7.1, p.167.

Key term

MOOCs: Massive Open Online Courses.

Research

Research the advantages and disadvantages of e-learning.

Discuss your findings with the rest of your group.

Test yourself

- 1 Identify one type of academic publication.
- 2 What does a SERP show?
- 3 What did Tim Berners-Lee predict about the WWW?
- 4 What type of resources can e-learning package include?
- 5 What does MOOC stand for?

Professional networks and peers

As people progress through their career, they create their own professional network. These network contacts can be, for example, their peers or colleagues and other members of professional bodies.

Many people in the digital sector belong to a professional body. As discussed earlier in this core element, professional bodies run conferences and network meetings. The conferences provide discussions, lectures and access to subject matter experts. The network meetings can be held in a geographical area which will enable a person to meet their peers and expand their personal network.

One of the advantages of gaining information and knowledge from conferences and peers is that it will be reliable. This is because those who attend conferences and network meetings organised by a professional body will have met the membership requirements and had their qualifications and experience validated. Conferences usually present an opportunity to gain an insight into the latest developments in the digital sector and expand a personal network.

Another advantage could be that if you encounter a problem or issue, it is possible that it will have already been encountered by other network contacts. It is, therefore, probable that a solution will have already been found.

There are very few disadvantages to gaining information and knowledge from professional networks and peers. One minor disadvantage is that it is very difficult to select which lecture or discussion

group to join at a conference as there can be so many to choose from. There is also the time issue. It may be very difficult to get time off work to attend conferences and network meetings but by advising an employer of the benefits, this can usually be overcome.

Developer kits

There are a range of different types of developer kits available. The most common type is a software development kit (SDK). These can be hardware and operating system specific or generic.

An SDK is usually a range of application development tools, including a compiler, debugger and a software framework. The SDK usually takes the form of an **application programming interface (API)**. The SDK can also take the form of an **Integrated Development Environment (IDE)**.

The advantage of using an SDK to gain information and knowledge is that many of the SDKs provide a combination of supporting material including:

- ▶ sample software
- ▶ technical notes
- ▶ documentation
- ▶ tutorials which clarify points made by the technical notes and documentation.

The main disadvantage of SDKs is that they can be rigid/inflexible, as they may only enable users to add a specific feature to their applications in a certain way. They can also be platform, hardware and operating system specific which could also limit their usefulness.

Key terms

Application programming interface (API): a software interface that provides a service to other software. It is a connection between digital devices or between software.

Integrated Development Environment (IDE): a software application providing a range of functions and facilities for software development. It usually includes a source code editor, automated build tools and a debugger.

Research

Research the different types of hardware developer kits (HDK) available, including the supporting material they come with.

What are the advantages and disadvantages of HDKs?

Supplier literature

Supplier literature can take many forms including instruction manuals, technical details or information about up-coming products.

Manuals and technical details are usually supplied when a product is purchased and can be in hard copy format or available electronically. The information contained within these types of supplier literature can be viewed as reliable and valid. This is because the information they contain has been created by the supplier. One disadvantage of supplier literature is that the technical information can be confusing if the user does not have specialised knowledge.

White papers

There are two different types of white paper. These are:

- ▶ an information document providing details of a solution or product that an organisation sells or plans to sell
- ▶ a document that presents government policies and legislation to gather public reaction.

The information document white paper is probably the most relevant for the digital sector. This document will enable information and knowledge to be gained about an existing or soon to be released product. A white paper will provide factual and technical evidence that a product will solve a problem or challenge. The information contained within this document will be reliable and valid as, just like supplier literature, the information has been created by the organisation linked to the product.

Activity

Find some supplier literature and white papers relating to digital devices and software.

Evaluate the information they contain. How could they be improved?

Test yourself

- 1 Identify two different types of supporting materials in an SDK.
- 2 Identify two forms of supplier literature.
- 3 Identify one disadvantage of supplier literature.
- 4 What is the difference between supplier literature and a white paper?
- 5 Why can the information in a white paper be considered reliable and valid?

Reliability and validity factors

When you have found sources of information and knowledge, it is important to check them to assess their reliability and validity. When checking for reliability and validity there are several factors you should consider.

Author expertise

With the vast amount of information available on the WWW, it is possible to check the expertise of the author. It is possible to find out the qualifications of the author, if they belong to any professional bodies, and reviews of other publications they may have written or contributed to.

Sources of information may have been written by a team of authors. It is possible that the authors may work at the same educational institution or have co-authored before. It is very easy to check the institution, or organisation, the authors work for. If the information source is electronic, it is also possible to identify the owner/author/publisher by checking the URL. If a copyright symbol is shown, this can also be checked.

Depending on the topic it may also be important to check that the author has up-to-date qualifications, experience and expertise in that topic area.

Date of publication is covered in 'academic publications', at the beginning of this section.

Bias

Bias can be defined as

'a specific tendency, inclination, feeling, or opinion, that is preconceived or unreasoned'.

When considering the reliability and validity of an information source there are four main types of bias that you should consider. These are:

- ▶ **Author bias** – which relates to the opinions and views of the author. It's possible they will have no evidence to substantiate these opinions or, where evidence has been provided, it might come from sources which share the same opinions or views.
- ▶ **Confirmation bias** – which relates to the sources which have been used and included in the citations available. The sources will have been selected to share the same opinion or view of the author. There will be little, if any, evidence of sources being used which provide the opposite opinion or view to that expressed by the author.
- ▶ **Selection bias** – which relates to the selection of sources included in the work and included in citations. Sources will have been selected that

agree with, or conform to, the opinions and views expressed by the author. There will be little, if any, evidence of sources which disprove or disagree with the opinions and views of the author.

- **Cultural bias** – which relates to the bias which comes from implied assumptions based on perceptions of different demographic groups. There will be little consideration in the work of a range of demographic groups, including their opinions and views, with the focus on one part of demographics.

While assessing the reliability of an information source for bias, there are three indicators you should consider in conjunction with the types of bias. These indicators are shown by different types of bias as shown in Table 7.1.

Indicator	Type of bias
Partiality	Author
	Confirmation
	Selection
	Cultural
Prejudice	Author
	Selection
	Cultural
Omission	Selection
	Confirmation

▲ Table 7.1 The three indicators and types of bias

Bias is also covered in section 6.1, p. 154 and section 6.3, p. 161.

Subjectivity

Subjective information is information from only one viewpoint. This type of information includes assumptions or interpretations of a topic which is rarely backed up by citations and evidence. Many social media and blog posts contain subjective information as opinions are always subjective. Because subjective information is from one perspective it is not suitable for reliable and valid decision making.

Context

It is usual for a published **work** to have a context. This could be an academic paper about a specific topic area, a textbook about a specific course, or supplier literature about a specific product. It is important to consider this context for the whole of the information source or work. If the work fails to

Key term

Work: in this context, ‘the work’ can be an information source, for example an academic paper, textbook or electronic information source.

fully address the context, or changes the context part way through the work, it can be assumed that the work is unreliable. You should also consider the relevance of the context. If the context is irrelevant to the subject area of the work, then you could also question the reliability and validity.

Intended audience

When you are checking for reliability and validity, you should also consider the intended, or target, audience. The intended audience is the people the author has written the work for. You should consider the level of knowledge of the intended audience. If the work is an academic paper or textbook, it is important that the amount of information provided, the use of technical or non-technical language and the structure is appropriate.

If a source has been found which provides information below the intended audiences level of knowledge, or the technical terms used are not appropriate or correct, it could be unreliable or invalid.

Citations, evidence and corroboration of sources

A citation is the method of informing readers where third-party material in a source of information comes from. The third-party material may be:

- a quote
- an idea that someone else has already expressed
- specific reference to the work of another author
- someone else’s work that has been critical in developing ideas.

The citation should be detailed enough for the reader of the source to locate the third-party material. This may include:

- the author
- the title
- the publisher
- the date of publication
- the page numbers and/or URL if the work is in an electronic format.

By using the citations defined in the work, it is possible to corroborate these sources. Corroboration means comparing information from two sources to find

similarities. When a second source provides the same or very similar information to the first source, this second source is said to corroborate (support/agree with) the original. By corroborating the sources, it is also possible to validate and check the reliability of the evidence included in the work.

Test yourself

- 1 How can the expertise of an author be checked?
- 2 Identify two types of bias.
- 3 What is meant by subjectivity?
- 4 What is a citation?
- 5 What should be included in a citation?

Case study

A primary school is considering introducing an interactive element to their geography lessons. The school is twinned with a school in the Cote D'Ivoire in Africa. It is hoped that children in both schools can take part in the geography lessons together.

The school has heard about the emerging technologies of the IoT, augmented reality and virtual reality. The school would like to integrate these into the geography lessons and, in future, other areas of the curriculum. They have also asked for suggestions about further emerging technologies and how these could be integrated into other areas of the school curriculum.

You have been asked by your team leader to prepare a proposal for the primary school, to include:

- an explanation of the concepts of IoT, AR and VR

- how these can be used to meet the needs of the primary school, including how the IoT, AR and VR would enhance the learning experience of the children and teachers in the two schools
- an explanation of the other emerging technologies that could be implemented by the school and how these would enhance the learning experience of the children and teachers in the two schools
- details of the information sources used and how you assessed these for reliability and validity.

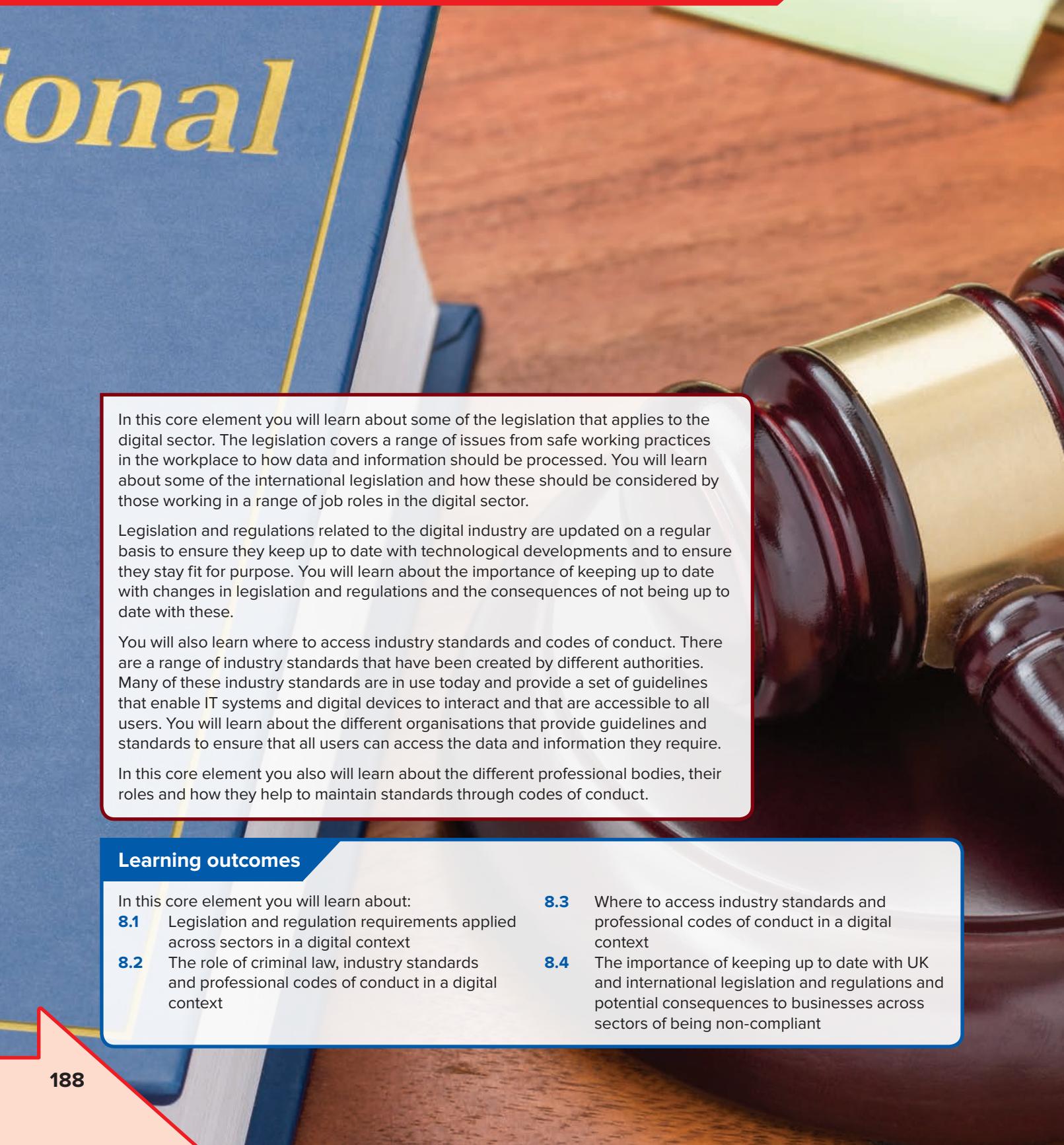
Your team leader has also asked that when you have created the proposal you:

- use one of the reflection techniques to reflect on your experience
- explain the advantages that creating this proposal will have for your professional development.

Assessment practice

- 1 Discuss the advantages for professionals working in the digital sector of regularly completing professional development.
- 2 Identify two possible applications of quantum computers.
- 3 Explain how quantum cryptography differs from normal cryptography.
- 4 Compare AR and XR.
- 5 Explain what is meant by blockchain.
- 6 Explain why a reflective technique should be carried out at the end of a project.
- 7 Describe the advantages of using an SDK.
- 8 Identify and describe one advantage and one disadvantage of using professional networks as an information source.
- 9 What is meant by confirmation bias?
- 10 How can citations assist in assessing the reliability and validity of an information source?

Core element 8: Legislation



In this core element you will learn about some of the legislation that applies to the digital sector. The legislation covers a range of issues from safe working practices in the workplace to how data and information should be processed. You will learn about some of the international legislation and how these should be considered by those working in a range of job roles in the digital sector.

Legislation and regulations related to the digital industry are updated on a regular basis to ensure they keep up to date with technological developments and to ensure they stay fit for purpose. You will learn about the importance of keeping up to date with changes in legislation and regulations and the consequences of not being up to date with these.

You will also learn where to access industry standards and codes of conduct. There are a range of industry standards that have been created by different authorities. Many of these industry standards are in use today and provide a set of guidelines that enable IT systems and digital devices to interact and that are accessible to all users. You will learn about the different organisations that provide guidelines and standards to ensure that all users can access the data and information they require.

In this core element you also will learn about the different professional bodies, their roles and how they help to maintain standards through codes of conduct.

Learning outcomes

In this core element you will learn about:

- 8.1** Legislation and regulation requirements applied across sectors in a digital context
- 8.2** The role of criminal law, industry standards and professional codes of conduct in a digital context

- 8.3** Where to access industry standards and professional codes of conduct in a digital context

- 8.4** The importance of keeping up to date with UK and international legislation and regulations and potential consequences to businesses across sectors of being non-compliant

8.1 Legislation and regulation requirements applied across sectors in a digital context

Industry tip

The details of each piece of legislation/Act/Regulation were correct when this book was published. During your study for this course, you must make sure that you know about and understand the most up-to-date versions of each piece of legislation, Act or regulation. This should also include any changes or additional pieces of legislation, Act or regulation that are relevant to digital support and business systems.

UK requirements

Health and Safety at Work Act 1974

The Health and Safety at Work Act (H&SAWA) came into legislation in October 1974 and has had many additions over the years. These additions include:

- ▶ Work at Height Regulations 2005
- ▶ Manual Handling Operations Regulations 1992
- ▶ Management of Health and Safety at Work Regulations 1999
- ▶ Health and Safety (Display Screen Equipment) Regulations 1992.

The H&SAWA defines the responsibilities of an employer to protect the health, safety and welfare at work of all of their employees, and other people who may be visiting the workplace, including temporary/casual employees, clients and visitors.

Almost everyone, not just employees and employers, has a duty under the Health and Safety at Work Act to work and behave safely. The Act also makes it illegal to act recklessly or to intentionally act in such a way as to endanger yourself or others. Employees must take reasonable care for their own and others' safety and co-operate with their employers in doing so.

Work at Height Regulations 2005

The Work at Height Regulations define what an employer needs to consider and do to protect employees from falls from height. Many network and communication cables in the working environment have been placed in ceiling gaps. So, it is possible that, if cables need routine maintenance or replacing, there

will be some working at height. Work at height means work in any place where, if there were no precautions in place, a person could fall a distance liable to cause personal injury. The regulations require the use of the right type of equipment where the risk of a fall cannot be eliminated. This is likely to be a ladder when dealing with cables in the ceiling gap. It does not mean balancing a chair on a desk.

The regulations mean that employers have a duty of care to:

- ▶ make sure equipment is suitable, stable and strong enough for the job, and that it is maintained and checked regularly
- ▶ make sure employees do not have to overreach when working at height
- ▶ make sure employees take precautions when working on or near fragile surfaces
- ▶ provide protection from falling objects.

In the case of low-risk tasks estimated to last 30 minutes or less then training should be provided on how to safely use the provided equipment. This training can be completed 'on-the-job'.

Manual Handling Operations Regulations 1992

These regulations relate to removing, where possible, the need for employees to carry out manual lifting of heavy boxes. By lifting boxes wrongly employees can damage their backs. Training should be completed to ensure all employees know how to lift boxes correctly. A risk assessment should be carried out and, if required, equipment, such as trolleys, should be provided. This is relevant when new digital equipment is being installed.



▲ Figure 8.1 How not to lift a box – and how to lift it safely

Management of Health and Safety at Work Regulations 1999

These regulations relate to carrying out risk assessments and the day-to-day management of health and safety in the workplace. A designated person has to undertake the role of overseeing health and safety, providing employees with information and training relevant to their job roles, and creating a written health and safety policy.

By creating a health and safety policy and carrying out a risk assessment, many of the possible risks in a workplace will have been identified. However, due to the constant use of equipment, buildings and facilities, risks may occur. It is the responsibility of both employers and employees to keep their working environment safe.

This means that employees have a duty to report to the health and safety officer any issues or accidents as soon as they have occurred. It is then the employer's responsibility to rectify the issue and/or report the accident to the Health and Safety Executive.

If an issue is reported then employers may use signs to warn their employees of the hazard or fence off the area. It is the responsibility of the employees to take note of these signs and restricted areas, and to conform with these restrictions.

Health and Safety (Display Screen Equipment) Regulation 1992

The H&SAWA provides guidance to employers and employees when working with computer systems under the Health and Safety (Display Screen Equipment) Regulation 1992, section 4.1.1. The Act also defines actions that an employer should take to protect employees who work with computers in their job. This is probably the most important health and safety regulation for anyone working in the digital industry with digital devices.

The **DSE** regulations apply to people using computers for their work but not necessarily to those using them at home, unless the employee works at home. The DSE regulations apply to any form of display screen. This means that employees working with PCs, laptops, tablets and smartphones are all covered by these regulations.

Key term

DSE: display screen equipment.

The DSE regulations cover employees who work with DSE for an hour, or more, during the working hours.

These state that employers, for example a business, school/college and so on must complete the four tasks outlined below to ensure the safety of their employees.

1 Analyse workstations and assess and reduce risks

Employers need to check that the computer equipment and the area around it is safe. If any risks are found during the assessment of the workstation and surrounding area, then action needs to be taken to make it safe.

The assessment should also cover the job role being completed and any special requirements of the staff member to carry out their job role.

Employers, and employees working from home, should complete a DSE workstation assessment. A DSE assessment should also be completed when:

- ▶ a new workstation is set up
- ▶ a new employee starts work
- ▶ a change is made to an existing workstation or the way it is used
- ▶ an employee complains of pain or discomfort.

Employers must ensure that workstations meet the minimum requirements including:

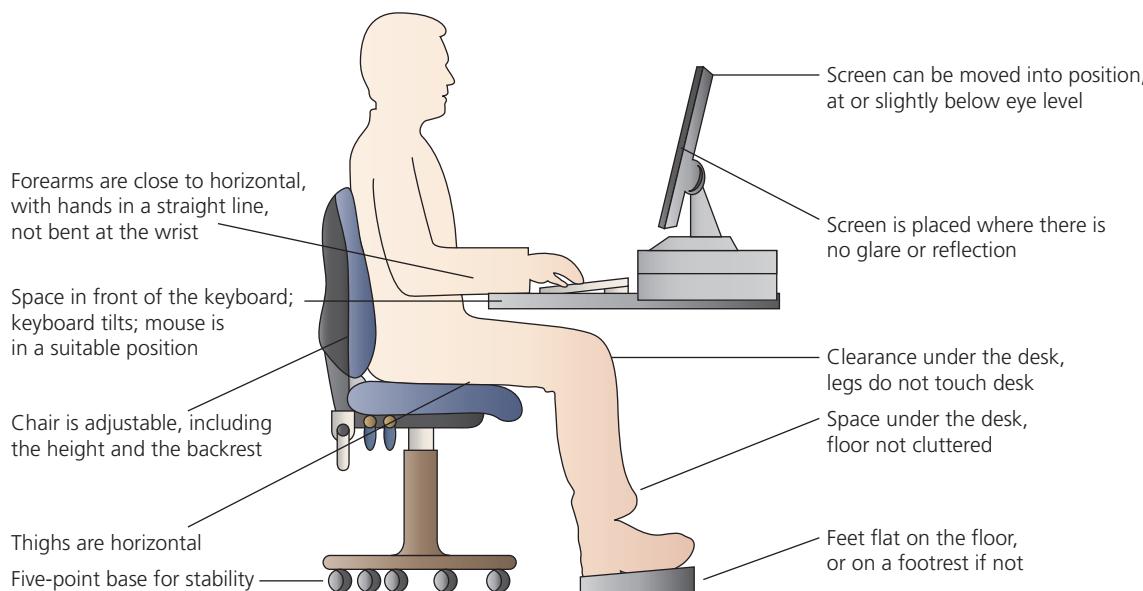
- ▶ providing adjustable chairs and suitable lighting
- ▶ providing tilt and swivel monitors
- ▶ ensuring that the workstation has sufficient space for the keyboard, monitor and any paperwork.

2 Plan work so that there are breaks or changes of activity

Employees should not be expected to work at DSE all day. Regular breaks should be provided or a change in the activity that the employees are carrying out. However, the regulations do not say how long or how frequent the breaks should be. In many workplaces a break from working at DSE may occur naturally, for example meetings in person. However, with the increase in employees working from home, this may not be possible as many meetings are held online.

In this case, employees should take responsibility for planning their own work day. While the regulations do not define when, and for how long, breaks away from DSE should be taken, it is better to have a five-to-ten minute break every hour rather than the traditional tea break of 20 minutes and lunch break of one hour.

During a break, employees should be advised to move around, stretch and focus their eyes on anything except DSE.



▲ Figure 8.2 Correct and safe arrangement of a workstation

3 Arrange and pay for eye tests and glasses (if they are needed for work)

Working with DSE does not cause permanent damage to eyes. But if DSE is used for a long time without a break it can lead to:

- ▶ tired eyes
- ▶ discomfort
- ▶ temporary short-sightedness
- ▶ headaches.

Employees of a business, who work with DSE, can ask for eye tests to be arranged and paid for by their employer. The eye tests can be repeated as advised by the optician – the employer will have to keep paying for these. The business will only have to pay for the glasses if they are required solely for work purposes.

Where employees are using DSE, the **employer** has a responsibility to:

- ▶ provide adjustable chairs and suitable lighting
- ▶ provide tilt and swivel monitors
- ▶ ensure that a workstation has sufficient space for the keyboard, monitor and any paperwork.

When working with DSE it is the responsibility of the **employee** to:

- ▶ check their screen is well positioned and properly adjusted
- ▶ make sure lighting conditions are suitable
- ▶ take regular breaks from screen work.

Health and safety training and information

For all parts of the H&SAWA, employers must provide training to make sure that their employees can use

their equipment correctly. The training they provide could include how employees can use the equipment to minimise risks to their health. The employers should also provide information to their employees about health and safety when, for example, using screen equipment and the steps that have been taken to minimise the risks.

Activity

Investigate the Health and Safety policy which applies to DSE users at your workplace or centre.

Write down the main points of the policy and summarise how the policy affects the DSE users.

General working environment

The general working environment not only covers those employees working with DSE but all job roles within the business. The employer and employee both have responsibility for the working environment. The working environment should:

- ▶ have the appropriate workplace facilities including the right number of toilets and washbasins, drinking water and somewhere to rest and eat meals
- ▶ be a healthy working environment
- ▶ be a safe workplace.

The Health and Safety Executive (HSE) states that a **healthy** working environment is one which has:

- ▶ good ventilation including a supply of fresh, clean air from outside or a well-maintained air-conditioning system

- ▶ a reasonable working temperature so it is comfortable to work (usually at least 16°C, or 13°C for strenuous work, unless other laws require lower temperatures)
- ▶ lighting suitable for the work being carried out
- ▶ enough room space, suitable workstations and seating
- ▶ appropriate waste containers for recyclable and non-recyclable waste.

A **safe** workplace is one which has:

- ▶ maintained buildings and work equipment
- ▶ floors and traffic routes kept free of obstructions
- ▶ windows that can be opened and cleaned safely
- ▶ any glass or transparent doors or walls protected or made of safety material.

Every workplace must have a health and safety policy. This is covered under the Management of Health and Safety at Work Regulations 1999.

The policy should cover areas, depending on the nature of the business, such as:

- ▶ statement of intent – including the management of health and safety
- ▶ responsibilities for health and safety – the names of the responsible people and the specific area they have responsibility for
- ▶ arrangements for health and safety – the practical arrangements including risk assessment, health and safety training based on the employees' job roles and using safety equipment.

Activity

Create a health and safety policy for your workplace or centre. Consider all the job roles that are carried out and the appropriate health and safety procedures.

Test yourself

- 1 Identify two tasks that an employer must complete to ensure the safety of their employees.
- 2 When should a DSE assessment be carried out?
- 3 What is meant by a healthy working environment?
- 4 What health issues could occur when working with DSE?
- 5 Identify two responsibilities of an employee when using DSE.

Investigatory Powers Act 2016

The Investigatory Powers Act (IPA) was brought into legislation in November 2016 and has been nicknamed 'The Snoopers Charter'. The IPA brought together a

range of surveillance powers that were included in different Acts.

These IPA also updated legislation in an attempt to make it more applicable for the increased use of digital devices and communication methods, for example emails, social media and messaging services. A single body was created to oversee the application of this Act – the Investigatory Powers Commission (IPC).

There are three main parts of the IPA. These are:

- ▶ **interception** – this relates to the accessing of communications, including telephone, email and any type of messaging, during transmission
- ▶ **interference** – this relates to the accessing of electronic equipment, including digital devices and smartphones, to obtain communication data
- ▶ **retention** – this means that all internet connection records have to be archived for 12 months.

These activities which are now permissible under the IPA are outlined below.

Interception of communications

Interception of communications relates to the actual content of a communication. This could be listening to a phone conversation or reading a message or email.

Communications can be intercepted if a **warrant** is granted. Intelligence agencies, police forces and HMRC can apply for a warrant to intercept communications.

The Home Secretary can grant a warrant, if the interception is deemed to:

- ▶ be in the interests of national security
- ▶ fight serious crime
- ▶ protect the economy at a national security level.

However, the IPA needs safeguards to be in place to limit the use of intercepted material and related communications data.

Equipment interference (hacking)

The security services can legally hack into digital devices, including computers, networks, mobile devices and servers. This includes downloading data from a mobile phone that is stolen or left unattended or installing key logging software to track every keyboard letter pressed by a user.

Key term

Warrant: a document issued by a legal or government official that authorises the police or other authority to make an arrest, search premises or carry out some other action relating to the administration of justice.

The IPA also provides the ability for complex equipment interference operations to be carried out. This could include the exploitation of existing vulnerabilities in software in order to gain control of devices or networks to remotely extract material or monitor the user of the device.

The power is available to police forces and intelligence services. Permission or warrants must be issued for hacking to be carried out.

The IPA also provides the ability for bulk hacking to be carried out – bulk equipment interference. This can be carried out if someone living outside the UK has come to the attention of the security services. This means that data and information can be accessed from a large number of digital devices in a specified area and is usually carried out where, for example, terrorism is suspected. However, by carrying out bulk hacking it is likely that innocent people's digital devices and data will also be accessed. The power to carry out bulk hacking is available to security and intelligence services.

Permission or warrants must be issued by the Secretary of State for bulk hacking to be carried out.

Retention of web records

The IPA also allows security services and the police to access communications data to help in their investigations. This means that Internet Connection Records (IRC), or the internet history, has to be archived for one year by communication service providers.

Communication service providers include internet service providers, and messenger and social media providers. They have to archive metadata about all communication made through their services. Any encryption should also be removed where it is possible to do so.

This means that who, what, when and where from, is archived for one year. So, every website visited, email sent and messaged posted is stored.

Permission or warrants must be issued for an IRC to be accessed. Authorities that can request a warrant to access IRCS include the Ministry of Defence, GCHQ and the National Crime Agency (NCA).

Research

Find out what is included in an IRC.

Freedom of Information Act 2000

The Freedom of Information (FoI) Act was brought into legislation in November 2000. The Act deals with

Test yourself

- 1 What is the nickname of the IPA?
- 2 Who oversees the application of the IPA?
- 3 What are the three main parts of the IPA?
- 4 How can equipment interference be carried out?
- 5 What does IRC mean?

access to official information and being able to find out any information on any topic from any public authority. This is known as 'a right of access'. The FoI Act is overseen by the **ICO**. Scotland has its own version of the FoI which was passed into Scottish legislation in 2002. This has the same purpose as the UK FoI but relates to Scottish authorities.

The FoI Act applies to all public authorities including government, health trusts, schools and the police. The Act allows anyone to make a request for information. There are no exclusions, including age. The process begins with a request made by letter, email or message to the authority that the information is required from. The name and address of the person wanting the information is needed so the information can be returned. The request should also detail the information required.

There is usually no charge for the information, although a small charge may be made if information has to be scanned or copied if it is not in electronic form. The information may include printed documents, computer files, letters, emails, photographs, and sound or video recordings.

The authority has 20 working days to comply with the request. All requests will be treated equally by the authority. That means every request for the same information must receive the same information as a response to that request.

The main benefit of the FoI Act is that information that was not accessible to anyone outside the authority is now available. This increases accountability as it is no longer possible for decisions to be made and then 'hidden'.

It is possible to request any information. However, this does not mean that the information requested will be supplied. Some information may be withheld to protect interests, or it may fall within one, or more, of the permitted exceptions.

A request must be made under the correct Act. The FoI Act enables access to information about public authorities.

Key term

ICO: Information Commissioner's Office.

If information is required about yourself, then a request needs to be made under the Data Protection Act 2018.

The Data Protection Act is covered later in this section.

The request should be very clear and specific in what information is needed. The authority has to confirm or deny the existence of the information requested. If the request is too vague then either the request will be denied, or the information may not be found.

There are absolute exceptions when actioning a request. These include:

- ▶ information that is already in the public domain
- ▶ information contained in court records.

Research

Investigate the absolute exceptions of the FoI Act. Are there any others that you think should be included?

Discuss your thoughts with the rest of your teaching group.

Under the FoI Act authorities have to publish seven types of information. These are:

- ▶ who we are and what we do – this includes organisational information and structure, locations and contact details
- ▶ policies and procedures
- ▶ what we spend and how we spend it
- ▶ what our priorities are and how we are doing
- ▶ how we make decisions
- ▶ lists and registers
- ▶ the services we offer.

The ICO has published definition documents which are specific to different types of authorities. These show the types of information, including examples, that should be published.

Activity

Select one type of education authority and research the relevant definition document.

Create a digital communication explaining the main points of the FoI Act, the types of information that can be requested and which should be published. The communication should be aimed at 16–18 year olds.

Computer Misuse Act 1990

The Computer Misuse Act (CMA) was brought into UK legislation in 1990 and has seen many amendments over the years. The original focus of the CMA was

Test yourself

- 1 Who oversees the FoI Act?
- 2 What type of information cannot be requested under a FoI access request?
- 3 Identify one absolute exception contained in the FoI Act.
- 4 How many types of information have to be published by authorities?
- 5 Identify one type of information that has to be published by authorities.

to criminalise the act of accessing or modifying data stored on a computer system without appropriate consent or permission. In 1990 the use of computer devices and networks was limited but was increasing. This increased use led to more data being stored on computer devices and networks.

The Act was developed following a high-profile case in 1987: *Regina v Gold and Schifreen*. Gold and Schifreen were hackers who managed to gain remote access to the British Telecom (BT) Prestel Service at a trade show. They used authentic access details of a BT engineer to carry out the remote access attack. They acquired the access details by shoulder surfing.

The definition of access or modification was initially limited as the number of methods by which the Act could be broken was very limited. However, with the increased use of computer devices, networks and the internet, there have been several amendments to the CMA. The increased use and storage of data has led to an ever-increasing range of threats and possible areas for harm. The act of preparation for a cyber attack and a range of methods of attack have now been included.

It is interesting that the CMA does not provide a definition of a computer. This is justified because if definitions were included these, due to the ever-changing innovations in technology, could very quickly become out of date.

The CMA enables the justice system to determine the definition based on the case that is in front of them. However, in the cases of *DPP v McKeown* and *DPP v Jones [1997]* Lord Hoffman defined a computer as:

‘a device for storing, processing and retrieving information’.

Key term

DPP: Director of Public Prosecutions.

The three original sections the CMA covered are shown in Table 8.1.

Section	Offence	Penalty
1	Unauthorised access to computer material	A fine up to a maximum of £5,000 and/or a maximum of six months in prison
2	Unauthorised access to computer materials with intent to commit a further crime	An unlimited fine and/or a maximum of five years in prison
3	Unauthorised modification of data	An unlimited fine and/or a maximum of five years in prison

▲ **Table 8.1** The original sections of the CMA

A further two sections were included in the CMA in the 2000s. The Police and Justice Act of 2006 led to section 3A being included in the CMA. The

introduction of the Serious Crime Act of 2015 led to section 3ZA being added to the CMA.

Section	Offence	Penalty
3A	Making, supplying, or obtaining any articles for use in a malicious act using a computer	An unlimited fine and up to five years in prison
3ZA	Unauthorised acts causing, or creating risk of, serious damage	An unlimited fine and/or up to 14 years in prison Unless the offence caused or created significant risk to human welfare or national security – in which case there is a maximum life sentence in prison

▲ **Table 8.2** Two further sections added to the CMA

Examples of offences

Table 8.3 shows examples of offences for each of the sections of the CMA.

Section	Examples of offences
1	Hacking – without them knowing, you watched your friend put their password into their phone. You then used it to gain access to their phone and download their photos.
2	Obtaining the unauthorised access with the intention of committing theft, such as <ul style="list-style-type: none"> • by diverting funds which are in the course of an electronic funds transfer, to the defendant's own bank account, or to the bank account of an accomplice • or where the defendant gained unauthorised access to sensitive information held on computer with a view to blackmailing the person to whom that information related. Without their permission, you accessed your friend's smartphone, obtaining their bank log-in details, so you could transfer money from their account.
3	You learned from a YouTube video how to use a tool to perform a denial of service attack against a friend, knocking them off an online game. You did this simply intending to win a game.
3A	You downloaded a program which was able to take remote control of a friend's computer without their knowledge. You didn't get a chance to use it before you were caught. This offence covers the possession of 'malware' but also legitimate software for which you had the intent of using to commit an offence.
3ZA	The most serious cyber attacks, for example those on essential systems controlling power supply, communications, food or fuel distribution. Loss of these systems could have a significant impact, resulting in loss of life, serious illness or injury, severe social disruption or serious damage to the economy, the environment or national security.

▲ **Table 8.3** Example offences for the CMA sections

Hacking

It can be seen that section 1 of the CMA refers to hacking.

Hacking means finding out weaknesses in an established system and exploiting them. A computer hacker is a person who finds out weaknesses in a computer system to gain unauthorised access. A hacker may be motivated by a multitude of reasons, such as profit, protest or challenge.

There are three main types of hacking that can take place: white hat, grey hat and black hat.

The different types of hacking are covered in section 1.13, p. 56 and Core element 10, section 10.3, p. 241.

Examples of hacking attacks

There have been many high-profile examples of hacking. Most of these have included some form of data breach. Some examples are detailed below.

Adobe

In October 2013 Adobe reported that their systems had been hacked. It was reported that 38 million usernames and encrypted passwords had been stolen by the hackers. In addition to this data breach, Adobe reported that the hack had exposed an undisclosed number of customer names, IDs, passwords and debit and credit card information.

eBay

In May 2014 eBay reported that a hacking attack had exposed account detail for all its users, reported to be 145 million people. The account details included names, addresses, dates of birth and encrypted passwords. eBay confirmed that hackers had used the credentials of three corporate employees to access its network and had complete access for 229 days.

British Airways

Between 10.58 p.m. on 21 August 2018 and 9.45 p.m. on 5 September 2018, British Airways (BA) suffered a hacking attack which led to a data breach of BA customers' data. The data breach was limited to those customers who had booked flights and holidays during that time through the BA website or mobile app. About 380,000 customers were found to have been affected.

Research

Research some more high-profile hacking attacks on businesses.

Develop a presentation showing the results of your findings. Present your findings to your group.

The data that was stolen related to payment details. BA reported that no travel or passport data was stolen during the attack.

There are many different threats to data and information. Some threats can also be targeted at physical computer equipment.

Cyber security attackers, including hackers, can hijack a computer system which could lead to data and information being stolen. This can have huge impacts on a business or an individual. As more businesses, and people, use the internet for, for example, financial transactions, security of this data has to be increased to ensure that information and data do not fall into 'the wrong hands'.

Hackers use a range of methods and threats to gain information and data. These methods and threats can be split into the following broad categories:

- ▶ malicious spam
- ▶ malware, including viruses
- ▶ threats.

Threats, malware, and malicious spam are covered in section 10.3, p. 241.

Test yourself

- 1 In what year was the first version of the CMA brought into legislation?
- 2 How did Lord Hoffman define a computer?
- 3 Identify two offences defined under the original CMA.
- 4 What is the penalty for a breach of section 3ZA?
- 5 Identify one type of hacking.

Digital Economy Act 2017

The Digital Economy Act (DEA) came into legislation in April 2017. The Act attempts to implement commitments related to the digital economy made in the Conservative party manifesto.

The Act is made up of six parts as outlined below.

1 Access to digital services

The Act details a new broadband Universal Service Obligation (USO) which provides everyone with the right to request a basic level of broadband: a minimum of 10 Mbps download speed. There is no mention of a minimum upload speed. However, the Government will direct **Ofcom** to

Key term

Ofcom: the regulator for communications services.

recommend the USO has minimum download speeds of more than 30 Mbps, if over 75% of premises are already accessing at least 30 Mbps. Ofcom will be responsible for overseeing and regulating the broadband USO, which will be implemented by commercial providers. Ofcom also has the power to increase the speeds defined in the USO.

The Act gives Ofcom the power to make communications' providers streamline and simplify the switching of provider process. This is particularly relevant when consumers have bought a bundle package, for example broadband, mobile and television together. By simplifying the switching process consumers will be able to switch providers and reduce their bills.

The DEA specifies that consumers should be automatically compensated when their broadband services drop service or are below the USO. However, the DEA does not provide a timeframe for this compensation to be received.

2 Digital infrastructure

The DEA includes a new electronic communications code. The aim of this code is to reduce the cost of building mobile and superfast broadband infrastructure. The planning rules for building the infrastructure have also been simplified. This includes the permission for operators to build the infrastructure on public land and grants rights to install equipment on private land.

There are also details about how private landowners will be compensated for the infrastructure being built on their land. It is important, however, that the locations are in keeping with the landscape and natural beauty. For example, the building of large-scale infrastructure in national parks, such as the Lake District, will have to be carefully considered.

The DEA also allows new management of the radio spectrum which will increase the capacity of mobile broadband.

3 Protecting citizens in the digital economy

The DEA includes a new statutory code of practice for direct marketing. This means that the Information Commissioner's Office can enforce sanctions against nuisance callers and spammers. This means that consent now has to be given by the consumers. This is also covered by the Data Protection Act and General Data Protection Regulation.

The DPA and GDPR are covered later in this section.

The other aspect of this part of the DEA is that it aims to protect children from online adult content (pornography). This is to be accomplished by making websites verify the age of someone wanting to access adult content material. Internet service providers also have to provide filters that can block all websites containing adult content. Consumers have the option to opt-out of using these filters.

4 Intellectual property

This part of the DEA supports digital industries by raising the maximum prison sentence to ten years for an internet copyright infringement. This brings it in line with the legislation relating to physical copyright infringement.

A patent can be granted to give the owner of a design a legal right to stop others from making, using or selling it for a specified number of years. Patents can be applied to all areas of technology, as long as they are new, involve an inventive step and can be applied to industry. Patents can be applied to most designs, including software processes and hardware.

A new online registration service called **webmarking** can now be used to protect assets which have a patent. It used to be that a patent number had to be shown to define that the design had been patented. The Intellectual Property Act includes details that allows the patent holder to provide an internet link to a website which provides details of the patent number. As with other details this only applies to designs patented after 1 October 2014.

The Copyright, Designs and Patents Act is covered later in this section.

5 Digital government

This part of the DEA focuses on the UK Government to deliver better public services and produce world leading research and statistics. Public authorities are able to connect, using digital systems, to manage data and information where the objective of connecting is a benefit to the public. Moving this forward, public authorities are able to share data and information to enable them to combat public sector fraud, such as fraudulent claiming of state benefits or tax evasion.

Key term

Webmarking: an internet link to a web page listing patent(s) which cover the product instead of marking the product itself with the actual patent number.

The introduction of tougher safeguards of personal data, which links with the Data Protection Act, has led to the introduction of new offences for unlawful disclosure of data and information (data breaches).

6 Miscellaneous

The most important item in this part of the DEA is that of section 114. The government has made a commitment in this part of the DEA to provide publicly funded basic digital skills training free of charge to adults in England who need it. These courses will be delivered by colleges and adult education providers.

Test yourself

- 1 How many parts does the DEA have?
- 2 What are the basic speeds defined in the USO?
- 3 How does the DEA attempt to protect children from accessing adult-content material on websites?
- 4 What is webmarking?
- 5 What is the focus of section 114 of the DEA?

Public Sector Bodies (Websites and Mobile Applications) (No. 2) Accessibility Regulations 2018

The Public Sector Bodies (Websites and Mobile Applications) (No. 2) Accessibility Regulations 2018 were brought into legislation in September 2018. These regulations require UK **public sector** websites and mobile apps to meet specified accessibility standards.

The regulations apply to the websites and apps of UK public sector bodies (e.g. NHS Trusts) including:

- ▶ the government
- ▶ regional or local authorities
- ▶ bodies governed by public law.

Key terms

Public sector: the sector that provides a range of governmental services, including infrastructure, public transport, state education, healthcare, police, fire and military services.

Non-governmental organisation (NGO): a non-profit organisation that is independent of government, for example an organisation which aims to address a social or political issue.

There are some exceptions to the regulations. These are:

- ▶ **non-governmental organisations (NGOs)** and charities (unless their finance comes from public funds, they provide essential public services, or specifically provide services aimed at people with disabilities)
- ▶ schools or nurseries, except for website content needed to access the services
- ▶ public sector broadcasters and their subsidiaries.

There are also exceptions to content including:

- ▶ office file formats published before 23 September 2018
- ▶ live time-based media
- ▶ online maps and mapping services
- ▶ third-party content
- ▶ the content of extranets and intranets published before September 2019.

If the website and mobile app meets the European accessibility standard EN 301 549 then it is permissible under these regulations. This standard is currently based on the Web Content Accessibility Guidelines (WCAG) 2.0 but may be updated to WCAG 2.1.

Important point

There is a difference between the internet and the World Wide Web (WWW/W3). In this core element/book the term 'the internet' has been used as most people use the internet as a blanket term to include both.

It is, however, important that you understand the difference between the internet and the WWW/W3.

Activity

Watch the video entitled Introduction to Web Accessibility and W3C standards:

www.w3.org/WAI/videos/standards-and-benefits

Answer the following questions:

- ▶ What features are defined for accessibility?
- ▶ What situations are detailed?
- ▶ How can accessibility features be included? Provide some examples.
- ▶ How does each feature work?
- ▶ What are the three sets of guidelines created by W3C?
- ▶ What features does the video include, or that you can access, to conform to the accessibility guidelines?

As a group, discuss your findings.

The main requirement of the regulations is to make a website and mobile app accessible by making it perceivable, operable, understandable and robust. These are the four guiding principles of the WCAG and are explained in Table 8.4. If any of these are not true, then users with disabilities will not be able to access and use websites and apps.

Principle	Definition	Meaning
Perceivable	Information and user interface components must be presentable to users in ways they can perceive	The content and components cannot be invisible to all of the user senses
Operable	User interface components and navigation must be operable	The interface cannot require interaction that a user cannot perform
Understandable	Information and the operation of user interface must be understandable	The content and operation of the user interface cannot be beyond the user's understanding
Robust	Content must be robust enough that it can be interpreted reliably by a wide variety of users, including those using assistive technologies	As technologies evolve, the content should remain accessible

▲ **Table 8.4** The four guiding principles of the WCAG

Contained in WCAG 2.1, there are 13 guidelines split between the four principles. Each guideline has success criteria. The guidelines demonstrate how web and mobile app content can increase accessibility to those with a disability. However, many of the principles and guidelines can also help in making web and mobile app content more accessible to all users.

An accessibility statement must be created, in an accessible format, and kept under regular review. The statements must be shown on the website and for apps a link must be provided to the statement or should be available when the app is downloaded.

The statement must include:

- ▶ an explanation of any content that is not accessible and the reasons why
- ▶ a description of any accessible alternatives provided, where appropriate

- ▶ a description of, and link to, a contact form that enables a person to notify the body of any failure to meet the accessibility requirements, and request details of information excluded.

By conforming to the Public Sector Bodies (Websites and Mobile Applications) (No. 2) Accessibility Regulations 2018, and the WCAG, the accessibility of a website and mobile app will be increased for all users but specifically those with a disability.

Activity

Complete the table below to show the principles and the associated guidelines.

Principle	Guideline(s)
Perceivable	
Operable	
Understandable	
Robust	

Activity

Using your centre's or employer's website or mobile app, apply the regulation and current WCAG.

Create a communication to be presented to the website or mobile app owner detailing compliance to the regulations and WCAG. Make suggestions as to how the website could be improved.

Test yourself

- 1 Identify and describe two principles set down by the WCAG.
- 2 Identify three standards defined by the W3C.
- 3 According to the WCAG, what is web content?
- 4 What are the four principles in WCAG 2.1?
- 5 Identify two areas that must be included in the accessibility statement.

Copyright, Designs and Patents Act 1988

The Copyright, Designs and Patents Act (CD&PA) was brought into UK legislation in November 1988. The CD&PA, and subsequent amendments, establishes copyright and that this copyright lasts:

- ▶ 70 years after the work was created or published
- ▶ 70 years after the death of the author
- ▶ 50 years for computer generated work.

Key term

Intellectual property (IP): creative work which can be treated as an asset or physical property. IP covers four main areas – copyright, trade marks, design rights and patents.

In 1992 The Copyright (Computer Programs) Regulations were amended to include computer programs. The CD&PA protects the creative work of individuals or businesses. The creator of an original piece of work, automatically owns the 'copyright'. The CD&PA aims to protect **intellectual property (IP)** rights.

Among the works that the CD&PA covers are:

- ▶ images
- ▶ software
- ▶ writing
- ▶ music.

The creator can decide what others do with their work. For example, they can decide to sell it or allow it to be used with a credit. The creator may also decide to invoke a Creative Commons licence. This type of licence is public copyright which allows the free distribution of a copyrighted work. The creator gives people the right to share, use and build on their work. Open-source software is an example of a Creative Commons licence.

Activity

There are six Creative Commons licence options. Investigate these six options and create a presentation explaining them, including examples.

Present your findings to the rest of your teaching group.

The CD&PA protects against:

- ▶ illegal downloads of video and audio files
- ▶ software piracy, either by illegal download or illegal distribution
- ▶ theft of intellectual property, for example text/ written work, including on websites
- ▶ use of software without the relevant software licence
- ▶ using/downloading images without permission of the copyright holder.

The CD&PA protects the creator of the work by making it a crime for anyone to download, copy and share their work without first paying for it, or in some cases asking for permission to use it first.

There are three main ways in which the CD&PA is broken, as outlined here.

Using software without the correct software licence

If a software program has been bought by a business with a licence to install it on three digital devices but the business has installed it on four devices, then the CD&PA has been broken. Some applications or programs will only run if a special piece of hardware is plugged into the computer or if a unique code is entered for that specific device.

Activity

In 1984 the Federation Against Software Theft (FAST) was set up.

Research FAST and create a digital communication aimed at business owners detailing the legal use of software.

Downloading files from the internet

If text, images and other files are downloaded and used, then permission from the copyright holder must be obtained. The name of the copyright holder should also be acknowledged (credited). Sometimes a fee may have to be paid to use the work.

Copying music, DVDs, CDs and software

Any copying or sharing of digital files that you have not created yourself is a breach of the CD&PA. This includes copying and sharing of MP3 and MP4 files made from streaming services or from music CDs. Copying and sharing films copied from DVDs or from streaming services is also a breach of the CD&PA. It is also illegal under the CD&PA to make and share copies of software.

Test yourself

- 1 How long does copyright last for on computer generated works?
- 2 What is intellectual property?
- 3 Give one example of work licensed under a Creative Commons licence.
- 4 What does FAST stand for?
- 5 Identify one way the CD&PA can be broken.

Waste Electrical and Electronic Equipment Directive 2012

The Waste Electrical and Electronic Equipment Directive (WEEE Directive) aims to increase the amount of recycling of unwanted electrical and electronic equipment. One of the impacts of the WEEE regulations is that retail businesses have to provide recycling facilities for customers and arrange to get these items collected by

registered waste disposal firms. The 2012 directive lists ten categories of goods that are covered by WEEE. These ten categories are:

- 1 large household appliances, for example fridges, cookers, microwaves, washing machines and dishwashers
- 2 small household appliances, for example vacuum cleaners, irons, toasters
- 3 IT and telecommunications equipment, for example digital devices, copying equipment, telephones
- 4 consumer equipment, for example radios, televisions
- 5 lighting equipment
- 6 electrical and electronic tools, for example drills, sewing machines, electric lawnmowers
- 7 toys, leisure and sports equipment, for example electric trains, games consoles and running machines
- 8 medical devices
- 9 monitoring and control equipment, for example smoke detectors, thermostats and heating regulators
- 10 automatic dispensers, for example hot drinks and money dispensers.

Category 3 is the most relevant to those working in the digital industry. Any device that shows the WEEE symbol, shown in Figure 8.3, has to be disposed of in a safe and environmentally friendly way.



▲ Figure 8.3 The WEEE symbol

This means that when a device has reached the end of its useful life then a WEEE compliant disposal must be carried out. A registered specialised company should be used to dispose of equipment in a WEEE compliant way.

Research

The WEEE Directive 2012 has been updated.

Investigate the up-to-date categories. Are there any more that could be added?

Human Rights Act 1998

The Human Rights Act (HRA) was brought into UK legislation in October 2000. The Act defines the basic

rights and freedoms that everyone in the UK is entitled to. The HRA is linked to the European Convention on Human Rights (ECHR).

The ECHR is covered later in this section.

Human rights are the rights and freedoms that apply to every person from birth until death. It does not matter which country you come from, what you believe in or the life you choose to live.

Human rights cannot be taken away from a person. They can be restricted if a person breaks the law or if a threat is posed to national security.

Human rights are based on values which are defined and protected by law, and include:

- dignity
- fairness
- equality
- respect
- independence.

The HRA defines the human rights in a series of Articles, each dealing with a different right. The Articles are all taken from the ECHR. The Articles are shown in Figure 8.4.

Article	Description
2	Right to life
3	Freedom from torture and inhuman or degrading treatment
4	Freedom from slavery and forced labour
5	Right to liberty and security
6	Right to a fair trial
7	No punishment without law
8	Respect for your private and family life, home and correspondence
9	Freedom of thought, belief and religion
10	Freedom of expression
11	Freedom of assembly and association
12	Right to marry and start a family
14	Protection from discrimination in respect of these rights and freedoms

▲ Figure 8.4 Articles of the Human Rights Act 1998

Public authorities and other public or private bodies must comply with the HRA when carrying out their functions. These authorities include:

- government departments
- local authorities
- hospitals and the NHS

- ▶ educational establishments
- ▶ police and prison officers
- ▶ immigration officials
- ▶ the court and tribunal system.

Article 8 – respect for your private and family life, home and correspondence – is also included in the ECHR and is the most relevant to the digital age. Correspondence includes letters, telephone calls and emails. The Article defines a person's right to privacy.

Under Article 8 a person has the right to live their life privately without government interference. The idea of private life includes the right to decide:

- ▶ sexual orientation
- ▶ lifestyle
- ▶ how to look and dress
- ▶ how to develop a personal identity, including friendships and other relationships.

Personal data and information must be kept securely and not shared without permission. These data and information include official records, photographs, emails and medical records. Article 8 also covers media intrusion and makes it so that others can be prevented from interfering in your life, including surveillance.

There are, however, situations when public authorities can interfere with the right to respect for private and family life, home and correspondence. This when the authority can show that this is lawful, necessary and **proportionate** in order to:

- ▶ protect national security
- ▶ protect public safety
- ▶ protect the economy
- ▶ protect health or morals
- ▶ prevent disorder or crime
- ▶ protect the rights and freedoms of other people.

Activity

In your group, each pick one Article of the HRA – except Article 8.

Research the Article and create a presentation explaining your chosen Article.

Present your findings to your group.

Key term

Proportionate: when it is appropriate, and no more than necessary, related to the problem concerned.

Test yourself

- 1 Identify two categories included in the WEEE 2012.
- 2 What should be used to dispose of WEEE compliant equipment?
- 3 Identify two Articles in the HRA.
- 4 Identify two authorities that have to comply with the HRA.
- 5 Identify two situations when authorities can interfere with the guidance of Article 8 of the HRA.

The Data Protection Act 2018/General Data Protection Regulation

The Data Protection Act (DPA) attempts to control how personal data and information are used by organisations, businesses and the UK Government. The Act also seeks to empower individuals to take control of their personal data and to support organisations with their lawful processing of personal data.

The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR). The DPA does not bring the GDPR into UK law. The GDPR has had a direct impact on EU member states since 25 May 2018, which means the GDPR is already part of UK law. When the UK left the EU, the GDPR was amended and converted into UK law under the European Union (Withdrawal) Act 2018.

The Act provides an update to the DPA 1998 and became law on 25 May 2018. The Information Commissioner at the time, Elizabeth Denham, stated that:

'The previous Data Protection Act, passed a generation ago, failed to account for today's internet and digital technologies, social media and big data. The new Act updates data protection laws in the UK, provides tools and strengthens rights to allow people to take back control of their personal data.'

www.ico.org.uk

The DPA is described by the UK government as:

is a complete data protection system, so as well as governing general data covered by the GDPR, it covers all other general data, law enforcement data and national security data. The DPA includes a number of agreed changes to the GDPR to make it work for the benefit of the UK in areas such as academic research, financial services and child protection.

The principles of the act

The DPA defines several principles. The principles of the DPA can be broadly equated to the principles of the GDPR. These principles are that data and information are:

DPA 2018 principles	GDPR principles
Used fairly, lawfully and transparently	Lawfulness, fairness and transparency
Used for specified, explicit purposes	Purpose limitation
Used in a way that is adequate, relevant and limited to only what is necessary	Data minimisation
Accurate and, where necessary, kept up to date	Accuracy
Kept for no longer than is necessary	Storage limitation
Handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage	Integrity and confidentiality (security) Accountability

▲ Table 8.5 Principles of the DPA 2018 and GDPR

The DPA also provides legal protection for sensitive information and data including:

- ▶ race
- ▶ ethnic background
- ▶ political opinions
- ▶ religious beliefs
- ▶ trade union membership
- ▶ genetics
- ▶ biometrics (where used for identification)
- ▶ health
- ▶ sex life or orientation.

Data subject rights

Under the DPA 2018 the **data subject** has rights. These include being able to find out what data is held or stored about them.

Other rights a data subject has under the DPA include the right to:

- ▶ be informed about how the data is being used
- ▶ access **personal data**
- ▶ have incorrect data updated
- ▶ have data erased
- ▶ stop or restrict the processing of the data
- ▶ data portability (allowing the data subject to get and reuse the data for different services)
- ▶ object to how the data is processed in certain circumstances.

Key terms

Data subject: the person the data is about.

Personal data: any information relating to an identified or identifiable living individual.

A data subject also has rights when an organisation is using personal data for:

- ▶ automated decision-making processes (without human involvement)
- ▶ profiling, for example to predict behaviour or interests.

One of the principles is that

'data and information is handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage'.

This means that the data/information should be protected by some form of security. Effective data protection relies on IT systems being protected from malicious intent. In implementing the GDPR standards, the Act requires organisations that handle personal data to evaluate the risks of processing such data and implement appropriate measures to mitigate those risks. These measures can include cyber security controls.

Security of digital systems, data and information are covered in Core element 10.

Research

Investigate each of the DPA principles.

Create a digital communication providing an explanation of how a UK-based business can comply with each principle.

Marketing consent

Under the DPA and GDPR, consent must be given before, for example, a business, organisation or charity sends a marketing message. The consent must be knowingly and freely given and must be clear and specific. This is also covered under the current version of the Privacy and Electronic Communications Regulations (PECR).

The consent needs to be given for the organisation, and for the type of marketing communication to be used, such as a phone call, automated call, email or text.

Key terms

Opt-in: when a person has to take a specific positive step, for example ticking a box, sending an email or clicking a button or icon, to say they consent to receiving marketing.

Opt-out: when a person must take a positive step to refuse or unsubscribe from marketing.

The consent should be a positive action, for example, ticking a box, clicking an icon or sending an email.

The person must fully understand that they are providing consent. It is not acceptable to only provide information about marketing as part of terms and conditions or a privacy policy as these can be hard to find, difficult to understand or rarely read.

The clearest way to obtain consent is to ask the person to tick a box confirming they are happy to receive your marketing calls, texts or emails. This is called **opt-in**.

It is important that clear records of what has been consented to are kept, including when and how the consent was given. This means that compliance can be proved in case of a complaint.

Consent can be withdrawn at any time, so it must be easy for someone to do this. This is called **opt-out**. For example, a link at the bottom of a marketing email that provides a link to unsubscribe, as shown in Figure 8.5.

Some organisations provide opt-in boxes that are automatically pre-ticked. However, the GDPR is clear that pre-ticked boxes do not give valid consent.

[Unsubscribe](#) | [Forward to a friend](#)

If you'd like to speak to a product specialist, [visit our website](#) to find someone in your area.

▲ **Figure 8.5** An unsubscribe link

Enforcement

Those who break the requirements will face financial penalties or other restrictions. There are two tiers of penalty that can be issued by the ICO – the higher maximum and the standard maximum.

The higher maximum penalty applies to any failure to comply with the core data protection principles or an individual's rights as stated by the DPA. It also applies in the instance of data transfers to third countries.

The penalty is £17.5 million or 4% of the total annual

worldwide turnover in the preceding financial year, whichever is higher.

For all other infringements (for example of the DPA's administrative requirements) the standard maximum penalty applies. This is a penalty of £8.7 million or 2% of the total annual worldwide turnover in the preceding financial year, whichever is higher.

Test yourself

- 1 Identify two principles of the DPA 2018.
- 2 Define the term 'data subject'.
- 3 Identify two rights of a data subject.
- 4 How can people opt-in?
- 5 What is the standard maximum penalty?

International requirements

As has been discussed in this core element, co-operation between digital professionals including those who use digital systems is very important. This means that co-operation across country boundaries must be maintained. There are many pieces of legislation that cross country borders. As the transition period for the UK to leave the EU ended on 1 January 2021, amendments have been made to some of the EU legislation to bring these into UK legislation.

The design and development of digital systems is, in the main, covered by the guidelines provided by organisations such as the ISO, WCAG and IETF. These need to be considered at the design stage, even when they relate specifically to the use of digital systems. When designing digital systems, it is also very important to consider the specific local legislation of the country or area in which a product will be used as these tend to differ.

Further details about the ISO, BSI, IETF and other industry standards and codes of conduct can be found in section 8.3, p. 207.

European Convention on Human Rights – Article 8

Article 8 protects a person's right to respect for their correspondence, family life, home and private life. Correspondence includes emails, letters and phone calls. This basically means that a digital system cannot be used to 'snoop' on anyone.

There are, however, exceptions to this. For example, it is possible for covert surveillance to be carried out if there is a perceived threat to national security, for example a terrorist attack. It is also possible for surveillance to be carried out in the case of the most serious criminal activity.

The increased use of the internet has enabled new types of political activism, cultural exchanges and the exercise of human rights. However, some may argue that restrictions related to access to the internet and digital media, and attempts by governments to monitor online activities or e-communications, for example, email, messaging and social media, interfere with the fundamental rights defined in the European Convention on Human Rights (ECHR) and possibly freedom of religion and belief, or the right to a fair trial.

The internet is largely unpoliced: this was a founding principle for Tim Berners-Lee. However, the increased use of the internet in everyday life has also led to a darker side of human nature. The internet has enabled an increased space for criminal behaviour and activity which crosses country borders, for the dissemination of hate speech and uprisings against authority or, for example, different religions. The internet can also be used for breaches of copyright legislation, fraud, identity theft and money laundering.

The internet has also been used to attack its own features, for example cyber security attacks through malware or distributed denial of service attacks. Cyber crime and cyber security have become major concerns.

Further details about threats to digital systems can be found in section 10.3, p. 241.

However, to carry out surveillance can be seen as contravening the ECHR. So, this then becomes a catch-22 issue, and the question must be asked – who decides what is an acceptable reason to carry out covert surveillance?

General Data Protection Regulation

The GDPR has already been covered in this core element in the section related to the DPA. The principles of the GDPR are:

- ▶ lawfulness, fairness and transparency
- ▶ purpose limitation
- ▶ data minimisation
- ▶ accuracy
- ▶ storage limitation
- ▶ integrity and confidentiality (security)
- ▶ accountability
- ▶ data security.

Electronic Communications Privacy Act 1986 – USA

The Electronic Communications Privacy Act (ECPA) is a piece of US legislation and relates to the use of a digital system relating to electronic communications. The legislation includes the Stored Communications Act (SCA) which covers the content of emails, private Facebook messages, YouTube videos and metadata, including websites visited, sender and recipient, and time/date stamps on emails.

The ECPA protects phone and electronic communications while those communications are being made, are in transit and when they are stored on computers.

However, as with the ECHR, it is possible to apply for permission to carry out covert surveillance if there is a perceived threat to national security or criminal activity.

Controlling the Assault of Non-Solicited Pornography and Marketing Act 2003 – USA

The Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act is another piece of US legislation and relates to the use of a digital system to send unsolicited commercial email.

The Act bans incorrect, deceptive or misleading subject information and lines. The Act requires that unsolicited commercial email is identified as an advertising email. As with the DPA and GDPR, this Act requires that those people who receive advertising email are supplied with the means to opt-out. The Act also establishes the criteria for determining the primary purpose of a commercial email.

In addition, the Act directs the US Federal Trade Commission (FTC) to issue rules about the subject lines of emails containing sexually explicit content.

Test yourself

- 1 What does EHCR stand for?
- 2 What does Article 8 of the EHCR aim to protect?
- 3 Identify one exception to Article 8 of the EHCR.
- 4 What does the ECPA protect?
- 5 Under the CAN-SPAM Act what do advertising emails need to include?

8.2 The role of criminal law, industry standards and professional codes of conduct in a digital context

It is important that any legislation and regulations set in law are complied with. This is to maintain the integrity of the law and to ensure compliance with the requirements of the laws. Each law covered in section 8.1, UK and international, has penalties detailed which can be applied if the law is broken.

Criminal law – national

Criminal offences against the laws can affect society on many levels.

The main reason that laws must be complied with in the UK are outlined here.

Maintains order

If there were no laws, then everyone could just do what they wanted with no punishments. Laws ensure that everyone knows what is legal and illegal. That is not to say that there are not people who break the law but when they are caught, they face penalties. Every law discussed in section 8.1 ensures that order is maintained. The legislation covered also ensures that data and information are kept secure, and that people are safe when working with digital systems.

Resolves disputes

Disputes can arise about many issues. In the digital context this is likely to include, for example, the ownership of a work. This dispute would be covered by the CD&PA as this is the law that deals with ownership. However, the DEA, part 4 – Intellectual property, also covers ownership of works taken from a website.

It may be that to solve a dispute information needs to be acquired. If the information is needed from a public authority, then a request can be made under the FoI Act 2000.

Protects individuals and property

The law is in place to protect individuals and property. This may include breaches leading to leaks of data. For example, the DPA/GDPR protects the security of personal information and data. The penalties for any breaches which lead to data leaks include:

- ▶ **higher maximum** – the equivalent in sterling to 20 million euros or 4% of the total annual worldwide turnover in the preceding financial year, whichever is higher
- ▶ **standard maximum** – the equivalent in sterling of 10 million euros or 2% of the total annual worldwide turnover in the preceding financial year, whichever is higher.

The CD&PA protects the copyright of the creator of a work (property). If a copyright infringement has taken place and is proved, then the penalty is:

- ▶ a maximum fine of £5,000 and/or six months imprisonment, in a magistrates' court
- ▶ an unlimited fine and up to 10 years imprisonment, in the Crown Court.

Research

Research the penalties for breaches of:

- ▶ Health and Safety at Work etc. Act 1974
- ▶ Computer Misuse Act 1990
- ▶ Waste Electrical and Electronic Equipment Directive 2012

Safeguards civil liberty

It is important that people feel safe and are able to live their life in peace and without fear. There are some laws which aim to protect the civil liberties of people including:

- ▶ Investigatory Powers Act 2016
- ▶ Human Rights Act 1998.

The IPA defines circumstances where authorities can use surveillance and interception. It is only in these circumstances that these measures can be used. If the measures are used in any other circumstances and for any other purpose, then this can be seen as an infringement of people's civil liberties. Linked with this is Article 8 of the HRA, where it is written into law that governments and public authorities must maintain

'respect for your private and family life, home and correspondence'.

As already discussed, this means that a person has the right to live their life privately without government

interference. To clarify, this means that the only times a person's civil liberty can be infringed are to:

- ▶ protect national security
- ▶ protect public safety
- ▶ protect the economy
- ▶ protect health or morals
- ▶ prevent disorder or crime
- ▶ protect the rights and freedoms of other people.

Test yourself

- 1 What are the two penalties that can be given under the DPA/GDPR?
- 2 What is the maximum penalty for an infringement of the CD&PA in the magistrates' court?
- 3 Which part of the DEA covers ownership of works taken from a website?
- 4 Which laws relate to civil liberties?
- 5 When can a person's civil liberty be infringed?

Criminal law – international

There are international laws which cover offences committed outside the UK. It is possible for someone to commit an offence outside the UK and be charged with these offences while living in the UK. There is cross border co-operation between security services which means that extraditions can take place.

As the use of the internet has increased it is important that people understand that a crime carried out in a country will be subject to the laws of that country.

For example, works protected in the UK by the CD&PA are also protected under the Berne Convention and Trade-Related Aspects of Intellectual Property Rights (TRIPS).

Industry standards and professional codes of conduct

You will learn about industry standards and codes of conduct in section 8.3, p. 207. The main reasons that industry standards and codes of conduct are in place are:

- ▶ compliance
- ▶ facilitating competition within industry
- ▶ promoting innovation
- ▶ providing interoperability between new and existing systems
- ▶ ensuring security
- ▶ ensuring transparency of sectors.

8.3 Where to access industry standards and professional codes of conduct in a digital context

There are many organisations that aim to provide standards and guidelines focused on a range of issues relating to the use of digital devices, data and information, and cyber security.

Industry standards

The industry standards organisations you need to know about for this course are:

- ▶ International Organization for Standardization (ISO)
- ▶ Internet Engineering Task Force (IETF)
- ▶ Electronic Industries Alliance/Telecommunications Industry Association (EIA/TIA)
- ▶ British Standards Institution (BSI)
- ▶ Institute of Electrical and Electronics Engineers (IEEE)
- ▶ Payment Card Industry Security Standards Council (PCI SSC).

Standards are agreed ways of doing something. They are written down as a set of precise criteria so they can be used as rules, guidelines or definitions.

Industry tip

Many of these organisations have a membership category for students. By joining one, or more, of these organisations you will be able to access resources, attend seminars and conferences and gain access to training courses and accreditations.

International Organization for Standardization

The International Organization for Standardization (ISO) is an independent, international, non-governmental organisation. The ISO currently has in excess of 160 national standards bodies as members, including the BSI. The ISO was formed in 1946 in London and has grown to become one of the most influential organisations in the creation and application of international standards across a range of sectors. The aim of the ISO is to:

'bring together experts to share knowledge and develop voluntary, consensus-based, market-relevant international standards that support innovation and provide solutions to a range of global challenges.'

www.iso.org.uk

The BSI is covered later in this section.

Research

Visit the ISO website (www.iso.org). Look at the timeline about the creation and development of the ISO.

Make a list of all the sectors that are affected by the work of the ISO.

In recent times cyber security has been high on the list of priorities for governments around the world with an increased level of cyber threats. These threats have come about because of the increased use of digital devices and the internet which has made the world appear smaller and more interconnected.

The ISO has developed the 27000 category of standards. The focus of these standards is on the safety of information assets. These assets include personal and organisational data as well as the confidential, national security and government data stored in the cloud.

These standards also assist organisations to manage the security of their assets such as intellectual property, and financial and employee data. This also includes the cloud providers who hold information in trust for third parties.

There are more than 12 standards in the 27000 suite. Some of these and their application areas are shown in Table 8.6.

Activity

Create an information sheet for a new member of staff in an IT support department detailing the ISO standards relating to digital systems and cyber security. You should provide details of each standard and how each can be complied with.

The ISO have developed standards about a range of other areas. These include:

- ▶ health and safety
- ▶ environmental management
- ▶ food safety
- ▶ quality management.

The ISO 9000 suite relates to quality management. This suite aims to help businesses and organisations improve the quality of their goods and services to meet customer expectations. The suite enables a business or organisation to complete an audit of their processes. By doing this, risks, weaknesses and inefficient areas can be identified. These can then be addressed to make the processes more efficient and ensure that relevant legislation is complied with. In some cases, business relationships with other businesses and organisations require ISO 9000 compliance.

Activity

Many business and organisations have ISO 9000 suite accreditations.

Invite a representative from one of these who is responsible for the accreditation to come and talk to your group about how it was achieved, what has to be done to maintain it and what benefits it has brought.

Internet Engineering Task Force

The Internet Engineering Task Force (IETF) is an internet standards organisation. The members are international and are mainly working as network designers, operators, vendors and researchers.

Standard	Application area
ISO/IEC 27000:2018	Provides an overview of information security management systems (ISMS). Terms and definitions commonly used in the ISMS family of standards are also included. This relates to all types and sizes of organisation (e.g. commercial enterprises, government agencies, not-for-profit organisations).
ISO/IEC 27001	Stipulates and defines the specifications for the implementation of an information security management system (ISMS).
ISO/IEC 27002:2013	Provides guidelines for organisational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organisation's information security risk environment(s).
ISO/IEC 27004:2016	Provides guidelines intended to assist organisations in evaluating the information security performance and the effectiveness of an information security management system in order to fulfil the requirements of ISO/IEC 27001:2013, 9.1.

▲ Table 8.6 Some of the standards in the 27000 suite and their application areas

The mission of the IETF is:

'to make the internet work better by producing high quality, relevant technical documents that influence the way people design, use, and manage the internet'.

The main focus of the IETF is the evolution of the internet architecture and the smooth operation of the internet. Earlier in this section you learned that the internet is defined as the hardware on which the WWW presents the information.

The IETF have five guiding principles. These are:

- ▶ open process
- ▶ protocol ownership
- ▶ rough consensus and running code
- ▶ technical competence
- ▶ volunteer core.

The main areas of interest of the IETF change over time as the technological developments change. This means that these areas keep up to date with technological developments. The main areas of interest for the IETF in 2021 were:

- ▶ automated network management
- ▶ the Internet of Things
- ▶ new transport technology
- ▶ security and privacy.

Most of the work of the IETF is carried out by remote working practices. These include virtual conferences, mail lists and forums. The IETF issues **RFCs**. These contain technical and organisational notes about the internet. The IETF has a library of RFCs which can be searched using keywords. Once an RFC has been published in the library it never changes. There are, however, occasions where errors have been identified. If errors are identified, then an erratum is uploaded to the library. Errors and the associated erratum can be categorised into:

- ▶ technical – errors identified in the technical content
- ▶ editorial – errors identified in spelling, grammar or punctuation, or syntax errors that do not affect the technical meaning.

Key term

RFC: Request for Comments.

Test yourself

- 1 How many national standards bodies belong to the ISO?
- 2 Which category of standards is focused on the safety of information assets?
- 3 Identify two of the guiding principles of the Internet Engineering Task Force (IETF).
- 4 What is the main focus of IETF?
- 5 What are the two categories of errors identified by the IETF in their RFCs?

Electronic Industries Alliance/ Telecommunications Industry Association

The Electronic Industries Alliance/Telecommunications Industry Association (EIA/TIA) developed standards focused on cables. The EIA was disbanded in 2011 but the work related to the standardisation that was carried out with the TIA still carries on today.

In the mid-1990s methods for cabling buildings were developed by EIA/TIA. The aim was to develop a standardised cabling system that would support multi-vendor products.

In 1991 the TIA/EIA 568 Commercial Building Telecommunication Cabling standard was released. The ISO standard IEC-11801 Generic Customer Premises Cabling standard is based on this initial standard.

The TIA/EIA 568 structured cabling standard defined how to design, build and manage a structured cabling system. The standards define that the system is developed in blocks – each of which have very specific performance characteristics – and are in a hierarchical structure. By following this standard a unified communication system can be designed and built.

The standard defines the use of fibre-optic cable (single and multimode), shielded twisted pair (STP) cable and unshielded twisted pair (UTP) cable.

Cabling is covered in section 5.2, p. 121.

Since the release of the TIA/EIA 568 standard there have been many updates due to the advancement in digital systems. In 2000 a major update was issued which combined all the amendments since TIA/EIA 568.

The most popular standards are:

- ▶ TIA-942 Telecommunications Infrastructure Standard for Data Centres
- ▶ TIA-568-C Telecommunications cabling standards, used by most voice, video and data networks
- ▶ TIA-569-B Commercial Building Standards for Telecommunications Pathways and Spaces
- ▶ TIA-598-C Fibre-optic colour coding
- ▶ TIA-222-H Structural Standard for Antenna Supporting Structures and Antennas
- ▶ TIA-602-A Data Transmission Systems and Equipment, which standardised the common basic Hayes command set
- ▶ TIA-102 Land Mobile Communications for Public Safety.

The TIA also defines Ethernet cabling quality standards. Each Ethernet UTP standard lists a TIA cabling quality as the minimum that the standard supports. The TIA standards follow an increase in numbers meaning the better the quality.

For example, 10BASE-T allows for Category3 (CAT3) cabling or better. 100BASE-T requires higher-quality CAT5 cabling, and 1000BASE-T requires even higher-quality CAT5 cabling.

Research

Investigate the standards and cabling used on the network in your centre or workplace.

Ask the IT team about how they ensure that standards are complied with when maintaining and upgrading the network.

British Standards Institution (BSI)

British standards are developed by the British Standards Institution (BSI). The Institution is part of the ISO. Many of the standards created by the BSI are included in the ISO standards library.

The BSI is the national standards body (NSB) for the UK. It represents the UK in a range of international standards organisations. The BSI also develops business information solutions for UK-based organisations and businesses.

The BSI provides standards related to a range of sectors including:

- ▶ aerospace
- ▶ information and communications technology including biometrics, data protection and the Internet of Things

- ▶ information management
- ▶ manufacturing and engineering.

The BSI also validates the BSI scheme. By a product being awarded the BSI Kitemark it can be seen to meet high standards of quality and safety.

The Kitemark logo can be found on a range of products where safety is paramount. These products include smoke alarms and crash helmets. However, it is now possible to find a Kitemark on a range of digital services including electrical installations and cable management, for example data cables.

Activity

Select one of the sectors where a BSI Kitemark has been awarded.

Produce a digital communication providing details of products/services including the advantages of being awarded a Kitemark.

Present your findings to your teaching group.

Test yourself

- 1 Which TIA standard relates to fibre-optic colour coding?
- 2 How are TIA Ethernet cabling quality standards categorised?
- 3 Identify one sector that the BSI provides standards to.
- 4 Identify one product where a Kitemark can be found.
- 5 Identify one service where a Kitemark can be found.

Institute of Electrical and Electronics Engineers

The Institute of Electrical and Electronics Engineers (IEEE) was formed in 1963 and is a professional association aimed at professionals who work in the electronic and electrical engineering sectors. It is the world's largest professional association with members in over 160 countries.

The objectives of the IEEE are the educational and technical advancement of electrical and electronic engineering, telecommunications and computer engineering.

The IEEE have developed standards related to computer technology. One of the most commonly known standards created by the IEEE is that of the 802 standards for local area networks (LANs), metropolitan area networks and other area networks, including Ethernet and wireless LAN (Wi-Fi).

Other areas that are covered by the IEEE standards include:

- ▶ blockchain and cryptocurrency
- ▶ portable operating system interfaces
- ▶ software life cycle processes
- ▶ software unit testing.

Many of these standards have been developed in conjunction with the ISO.

Activity

Watch the 'IEEE Overview' and the 'IEEE One Voice' videos on the IEEE website.

What activities do the IEEE carry out? Why is the IEEE important?

Discuss the video with your group focusing on the importance of the IEEE standards.

Activity

Access the PCI SSU website and locate details about the stages where the standards are used.

Create a digital communication aimed at 16–18 year olds explaining the 15 standards and where they are used in the payment process.

Test yourself

- 1 What are the objectives of the Institute of Electrical and Electronics Engineers (IEEE)?
- 2 What do the IEEE 802 standards relate to?
- 3 What is the aim of the Payment Card Industry Security Standards Council (PCI SSC)?
- 4 Who formed the PCI SSC?
- 5 How many standards relate to the payment process?

All of the organisations covered in this section have the same basic aim: to make sure that digital systems are accessible, of a high quality and secure. It is important that every professional working on projects connected to digital systems uses the same basic protocols and standards. By doing this, the functionality of any digital system will be consistent and accessible for all users.

To turn this on its head – what would happen if every professional used a different set of standards and protocols?

Professional codes of conduct

There are many professional bodies for professionals working in the digital industry. For this course you need to know about three of these. These are the:

- ▶ British Computer Society (BCS)
- ▶ Institute of Analysts and Programmers (IAP)
- ▶ Chartered Institute of Information Security (CISSec).

Each of these professional bodies has developed a **code of conduct** for their members. The purpose of the codes of conduct is basically the same – to provide a set of guidelines which members agree to abide by.

Each of the professional bodies is relevant to different job roles within the digital industry. It is, however, possible to belong to more than one professional body.

Key term

Code of conduct: a document which defines rules, values, ethical principles and vision.

Payment Card Industry Security Standards Council

The Payment Card Industry Security Standards Council (PCI SSC) aims to maintain, evolve and promote standards for the safety of payment cardholder data across the globe. The PCI SSC's mission is to enhance global payment account data security by developing standards and supporting services that drive education, awareness and effective implementation by stakeholders.

The PCI SSC was formed by the major payment card issuers, including Visa, Mastercard and Amex. The main focus of the PCI SSC is to help organisations that provide payment cards to implement standards to protect payments systems from data breaches and leaks of cardholder data. Payment card suppliers and processors hold a lot of customer data all of which must be kept secure and confidential.

The PCI SSC currently have 15 standards which are implemented at different stages of the payment card process.

- ▶ The BCS is a professional body that represents those working in information technology (IT) and computer science.
- ▶ The IAP is a professional body that represents those working in the digital sector as an analyst or programmer.
- ▶ The CIISec is a professional body that represents those working in the information and cyber security sector.

Important point

There are generally entry requirements (such as qualifications or experience in the sector) for an individual to meet before they can become a member of a professional body, and they will usually have to pay a fee.

Each of these professional bodies not only acts as a community for those working in digital industries but also provides:

- ▶ training and a range of qualifications to enable members to update their skills
- ▶ updates on advances in digital industries
- ▶ a range of resources that can be used by members to enhance their own knowledge.

Each of the professional bodies has links with education including schools, colleges and universities.

The purpose of a code of conduct is to provide members with a set of guidelines and principles which need to be followed to uphold the philosophy of the professional body. When members join a professional body, they are agreeing to follow the guidelines and principles set down in the code of conduct.

The role of a code of conduct is to provide guidelines for members. These guidelines provide clear details about how members should behave and conduct themselves in their professional lives.

The BCS states on their website that the code of conduct serves as a

'unique and powerful endorsement of your integrity and also serves as a code of ethics for IT professionals'.

www.bcs.org

The IAP clearly states on their website that they need to ensure that their members hit the highest professional standards, are committed to their own development and abide by their duty to serve the public interest in their work.

The CIISec is dedicated to raising the standard of professionalism, integrity and excellence in information and cyber security. The CIISec also aims to develop ethical standards for those working in the information security sector and to promote ethical and professional standards in all parts of the world.

The codes of conduct of each of the professional bodies all include the commitments of the members to work in the public interest and to accept their professional duties. The BCS also includes the statement that by accepting your professional duty, this is the

'foundation of the digital professional which is built upon everyday by the competence, integrity and diversity of their members'.

The codes of conduct of each of the professional bodies also act as a benchmark when assessing the misconduct of their members. Each code of conduct includes statements of responsibility related to the IT and computing digital industry.

The key principles of the code of conduct for the BCS are:

- ▶ 'You make IT for everyone (public interest).
- ▶ Show what you know, learn what you don't (professional competence and integrity).
- ▶ Respect the organisation or individual you work for (duty to relevant authority).
- ▶ Keep IT real, Keep IT professional, Pass IT on (duty to the profession)'.

Research

Investigate the codes of conduct and ethics for the BCS, IAP and CIISec. Compare these codes for the three professional bodies. Evaluate the similarities and differences between each code. Identify any possible omissions.

Create a digital communication to present your findings to a group of students aged 17–19 years old.

Test yourself

- 1 What are the three main professional bodies related to those working in the digital industry?
- 2 What is the purpose of a code of conduct of a professional body?
- 3 What is the role of a code of conduct of a digital professional body?
- 4 Identify two main points of the code of conduct for the BCS.
- 5 What is the aim of the CIISec?

8.4 Keeping up to date with UK and international legislation and regulations and potential consequences of being non-compliant

Importance of keeping up to date

All pieces of legislation and regulations, both UK and international, change over the years. In the case of legislation and regulations relevant to the use of digital systems and the digital context, this is usually to update them in line with technological advances and how they are used.

It is, therefore, important to keep up to date with these updates. The main reasons to keep up to date are:

- ▶ protection for business
- ▶ protection for customer
- ▶ avoiding the consequences of non-compliance.

As legislation and regulations change, any processes and policies must also be updated to meet these changes. This can be important as it will help to avoid penalties for non-compliance. For example, if any changes in health and safety legislation were not implemented, a person could get injured and the business or organisation be fined by the HSE for non-compliance.

If changes to the legislation and regulations about data and information were not implemented then again if a breach happened and there was a data leak, this could result in fines and penalties. By complying with the up-to-date legislation and regulations, customers' interactions will also be protected. This includes secure storage of their data and information. If data is leaked, then fines and other penalties will most probably be issued. This will then have a negative effect on the business or organisation which was storing this data.

Any goods purchased by customers must also be compliant with legislation and regulations. For example, the BSI Kitemark is applied to a range of goods. By keeping up to date with these standards, the

company can assure customers that the goods are safe at the time of purchase.

Potential consequences of non-compliance

The potential consequences of non-compliance include:

- ▶ financial
- ▶ legal
- ▶ reputational
- ▶ professional
- ▶ sector specific.

Much of the legislation and regulations have a financial consequence for non-compliance. This has already been discussed in section 8.2. Non-compliance of the legislation and regulations can lead to prosecution. This can have a financial impact in the form of fines, and can also lead to imprisonment for any responsible people.

Not only can non-compliance lead to fines, it can also lead to a loss of customers and clients. This in turn will lead to a loss of income. If, for example, a data breach happened, then it is possible that the news of this will be reported in the media. This includes posts on social media. This can affect the reputation of the business or organisation as people would not want, for example, their data held insecurely. This could lead to brand damage as the customer perception of the brand will diminish.

When a prosecution occurs as a result of non-compliance with legislation and regulations, it is possible that the responsible person will be imprisoned. If this does not happen, but other penalties are given, the responsible person is likely to either have their contract terminated or they will have their job role and responsibilities re-evaluated. It is also possible that if they were a member of a professional body, for example the BCS, they may have their membership revoked. This will be as a result of failing to meet the standards as set in the code of conduct.

There are some sectors where non-compliance with legislation and regulations can have dire consequences. For example, if food standards are not met in the hospitality sector, then this could lead to an outbreak of food poisoning which could lead to customers being

ill. This would then, in turn, lead to brand damage, and loss of reputation and customers, which could mean a loss in income.

There are many consequences to non-compliance with legislation and regulations to a business, organisation and people. By keeping up to date with the legislation and regulations, the probability of these consequences occurring can be negated.

Research

In a group of two or three, select one sector from health, education, retail or hospitality.

Research cases where non-compliance of legislation and regulations has occurred, and the consequences of this non-compliance.

Create a digital communication and present your findings to the rest of your teaching group.

Project practice

A small start-up company delivers pet food to its customers. Customers order pet food by phoning one of the customer support team.

The pet food is stored in a warehouse. Each order is picked and packed in boxes by the warehouse employees. The boxes are delivered by a courier company.

Business is improving with more customers placing orders. The company is employing new employees to work in their offices and warehouse. The new IT department employees must have membership of at least one professional organisation.

The company are considering creating a website where customers will be able to register and order their pet food. Customers will need to provide their name, address, phone number and an email address when registering. The owner of the business wants the website to be as accessible as possible to all users.

The customer details will be stored by the company. The company wants to send emails to the email address provided on registration to tell their customers about new products and services.

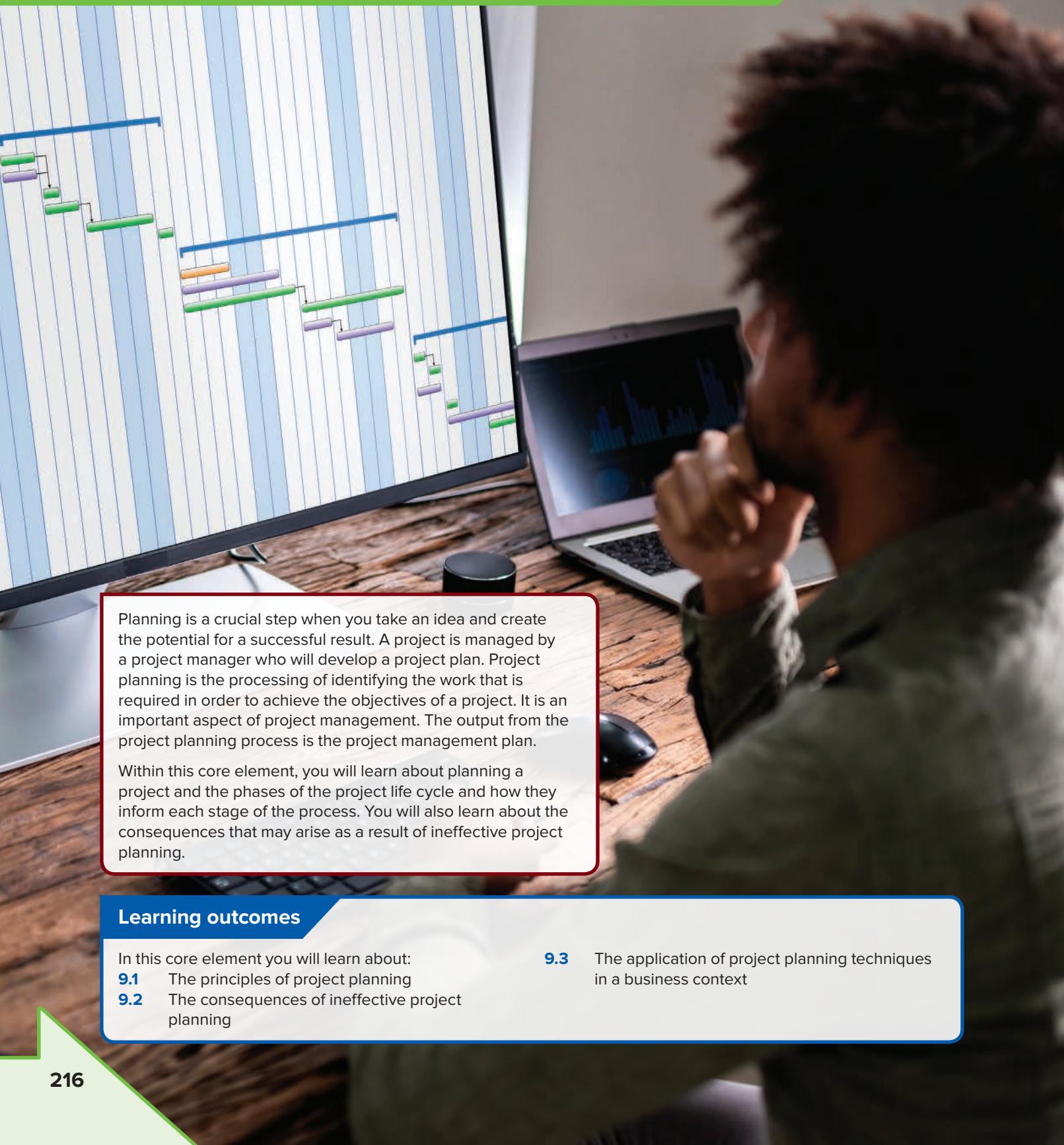
You have been asked to:

- ▶ Provide details of the legislation the business must comply with and the actions needed to comply with them.
- ▶ Explain the importance of following accessibility standards relating to the creation of the website.
- ▶ Identify the industry standards that the business should consider, explaining why these should be followed.
- ▶ Explain why the business should consider becoming accredited with the ISO 9000 suite and the benefits this will bring.
- ▶ Explain the advantages of the IT department having membership of a professional body.

Assessment practice

- 1 Explain, using examples, the importance of the Health and Safety at Work Act (H&SAWA) when working with display screen equipment (DSE).
- 2 Identify and describe two activities which are permissible under the Investigatory Powers Act (IPA) 2016.
- 3 Explain the protection that is given to the creator of a work under the Copyright, Designs and Patents Act (CD&PA) 1988 and the Digital Economy Act (DEA) 2017.
- 4 Discuss the rights of a data subject under the Data Protection Act (DPA) 2018.
- 5 Explain the link between the Human Rights Act (HRA) 1998 and Article 8 of the European Convention on Human Rights (ECHR).
- 6 Discuss the importance, using examples, of standards in the digital context.
- 7 Promoting innovation is one purpose of industry standards and professional codes of conduct. Identify and describe two other purposes.
- 8 Explain why it is important that a card payment process complies with the standards created by the Payment Card Industry Security Standards Council (PCI SSC).
- 9 Why is it important to keep up to date with UK legislation and regulations?
- 10 Identify and describe two reputational consequences of non-compliance with UK legislation.

Core element 9: Planning



Planning is a crucial step when you take an idea and create the potential for a successful result. A project is managed by a project manager who will develop a project plan. Project planning is the processing of identifying the work that is required in order to achieve the objectives of a project. It is an important aspect of project management. The output from the project planning process is the project management plan.

Within this core element, you will learn about planning a project and the phases of the project life cycle and how they inform each stage of the process. You will also learn about the consequences that may arise as a result of ineffective project planning.

Learning outcomes

In this core element you will learn about:

- 9.1** The principles of project planning
- 9.2** The consequences of ineffective project planning

- 9.3** The application of project planning techniques in a business context

9.1 The principles of project planning

A project can be small or large, short term or long term. There are good practice principles that you can follow to help you achieve success with a project. The principles will also help you to reduce the risk of failure by using careful planning and control.

Identification of project aims and objectives

The focus of a project is expressed in terms of aims and objectives. It is important to understand the difference between the two. Below is an overview of what each term means.

- ▶ **Aim** – this is what the intended outcome of the project will be. Sometimes referred to as a statement of intent, it is usually written in broad terms. An example could be:

 - To implement updated digital technology into a manufacturing process

- ▶ **Objectives** – these are more specific statements and define the steps that you need to take to achieve the outcome of the project. These statements define the measurable outcomes. When writing objectives, it is always advisable to use strong positive statements. Use strong verbs such as collect, classify, develop, construct, measure, devise, revise, produce, select and synthesise. Objectives should also be **SMART**:
 - **Specific** – be precise about what is going to be done/carried out.
 - **Measurable** – so it will be clear when the objective has been achieved.
 - **Achievable** – ensure that the objective is not over-ambitious and that it can be easily achieved taking all factors into consideration.
 - **Realistic** – are the resources available in order to achieve the objective? Resources can include time, skills, personnel, finance and so on.
 - **Time constrained** – it is important to identify when each stage needs to be completed. Has time been factored in to allow for potential delays?

Project scope

The project scope is the part of project planning that requires the project manager to determine and document a list of specific project goals, tasks, deliverables, costs and deadlines. It is important to

Key term

Stakeholders: any individual, group or organisation that is impacted by the operations of an organisation. These can include customers, suppliers, employees, communities, government and even the ecosystem.

define the scope of the project as it indicates what the project entails, so that all **stakeholders** can understand what is involved. It provides a roadmap that is used to schedule work, allocate budget and assign tasks. This helps the project team to focus on the objectives of the project. It also helps to ensure that the project does not expand outside the original aim.

User/client requirements

It is important that the requirements of the project are clearly understood and documented. You need to consider not just the client who has hired you to carry out the project, but also anyone who is affected by the outcome of the project. So, this also includes the end users and customers. It is important that all the stakeholders are identified, and their own needs and interests considered when the project plan is created. Information must be gathered about each of their needs and expectations. This informs the baseline for the project scope, the timelines and budget. A scope statement is then created that records the details of the scope of the project.

Business case

A business case analyses how the project will support an organisation's business strategy and maintain any competitive advantage it may have in the market. A business case can include additional information that can develop it into a plan with action steps and major milestones. The business case is an important input into the project management plan and when the project is complete, the project closure stage will measure the success of the project's objectives against those identified in the business case. Business cases can take many formats but here are the common components that should be included:

- ▶ reasons for the project
- ▶ options – brief description of any alternative approaches considered with one option recommended to take forward
- ▶ expected benefits – expressed in measurable terms, for example increase in the number of customers purchasing via the online platform as opposed to visiting the retail outlet

- ▶ risks – this is a summary of any major risks that have been identified
- ▶ costs
- ▶ timescales.

Expected outcomes

Outcomes are the changes that will have happened as a result of the project. What these outcomes are will depend on the type of project. Outcomes should be measurable, for example 25% reduction in time to manufacture a product, 50% increase in the number of customers and so on. Outputs and outcomes are all as a direct result of a project and are similar but there are some key differences, as shown in Table 9.1.

Outputs	Outcomes
<ul style="list-style-type: none"> • These are directly produced by the project; if activities are completed, they will create an output. • They are tangible and measurable. • The outputs are not the reason the project was implemented. 	<ul style="list-style-type: none"> • These are produced from the outputs of the project. Just because a project activity is completed, it does not mean that the outcomes have been achieved. • They are more intangible and harder to measure.

▲ **Table 9.1** The key differences between outputs and outcomes

Expected outcomes have the following features:

- ▶ Within the project proposal, there will be an explanation of how the proposal will meet the needs identified in the requirements.
- ▶ There will be a clear indication and explanation of the benefits that will be achieved if the project proposal is accepted. The proposal may also state what might happen if the proposal is not accepted.
- ▶ Expected outcomes are usually written in the future tense stating that something ‘will’ happen or may be conditional and say that something ‘would happen’.

Stakeholder roadmap

A stakeholder roadmap provides a strategic overview of the main components of the project. It will include the objectives, deliverables, milestones, resources and timelines. A roadmap is used to communicate the strategic objectives of the project to the stakeholders. Stakeholders also use a roadmap to help them keep on track with the progress of the project. In addition, the roadmap should also provide them with the strategic reason for implementing the project.

It is important not to confuse the stakeholder roadmap with the project plan.

- ▶ A **project plan** provides the task-level details of the project that are presented on a timeline. It helps project managers to assign tasks/responsibilities and track all areas of the project at a detailed level. It is an internal document resource for use by the project team to keep an up-to-date view of the progress of the project.
- ▶ The **stakeholder roadmap** presents only the high-level, strategic view of the project and does not include the day-to-day tasks. Nor does it include a detailed view of the roles and responsibilities and who will be working on what part of the project. It is used to help the project team present a quick overview of the project status to other teams which may include investors, executive staff and departments within the organisation. The roadmap is developed first to provide a strategic overview of the project and then used to break down the strategic goals and milestones into the task-level components of the project plan.

Timeline and deadlines

Timeline

The timeline shows what phases of the project are in the past, what the current progress is and what is still left to do to complete the project. It therefore helps to keep projects on track. Different projects may have different key elements; however, there are a few elements that are usually in all timelines:

- ▶ start and due/end date of the tasks
- ▶ the duration of the tasks
- ▶ who the tasks are assigned to
- ▶ task dependencies (where the start of one task is reliant on the completion of another task or tasks).

The **benefits** of using a timeline are as follows:

- ▶ multiple tasks and project management phases are in one location
- ▶ provides a simple, visual presentation of the project to enable all teams to understand and discuss task/project progress
- ▶ provides a realistic view of the project that can assist teams in their recovery from setbacks (unexpected outcomes) or adjust to any major changes that may be required
- ▶ team members can focus on important tasks/activities
- ▶ managers can sequence the events across the project so that team members are not overloaded with work which they would have difficulty in completing
- ▶ helps to promote improved time and resource management.

Deadlines

These are an important component of every project. There can be easy and difficult deadlines and even at times 'we are never going to make this' deadlines when involved in projects. Deadlines can be imposed by the customer, executive management, project manager, the project team members or just due to circumstances beyond the project team's control. Sometimes there is a small degree of flexibility within the deadlines set and sometimes they cannot be changed at all and must be met on time. Many organisations and project managers miss deadlines occasionally and therefore flexibility with respect to the deadlines may have been built in by stating that a task must be completed in advance of when it is necessary.

Linked to organisational strategic objectives

Even though strategic planning and project planning are not the same, they are closely related to each other. A strategic objective is something that is organisation wide, the bigger vision for the organisation. Project planning is used as part of the implementation phase of an overall strategic plan. An organisation's strategic objectives can help an organisation to address the vision, mission and goals, and share them with the teams. Every project should support the overall strategy of the organisation.

When considering the project objectives and how they align with the strategic objectives of the organisation, the following should be considered:

- ▶ **Prioritisation** – a decision must be made on which projects are also organisational priorities. When selected, they should be broken down into actionable steps.
- ▶ **Project management methodologies** – there are many different project management methodologies, and it is important to choose the one that is appropriate for the project and the intended strategy.
- ▶ **The roles of leadership within an organisation** – effective leadership is an important aspect of any organisation and can have a major influence on the culture of the company. It is important that the leadership team understands the organisational strategic objectives and is committed to motivating their teams and supporting them through the project management process.
- ▶ **Completing the work** – any team that has a good leader and follows a strong project management methodology has a better chance of following through on their tasks, which is of paramount importance for the success for the project.

Resource requirements

A resource plan is created during the planning phase of a project. It helps to anticipate all the resources required to complete a project. A good resource plan should be detailed and include several components that are important to the completion of the project. A resource plan can help reduce budgeting and help the accurate forecasting of project expenses. A good resource plan will:

- ▶ reduce (possibly prevent) the overallocation of resources
- ▶ prevent underutilisation of resources
- ▶ assist the planning of resources required
- ▶ minimise task and resource dependencies (this is where one or more tasks are dependent on the completion of another task, and the resources are available for the task). A person is not waiting for resources to become available because they are being used by someone else. Remember, people are also classed as resources.

People and skills

It is important to find the correct people with the relevant skills to become part of the project management team. If the people are involved with other tasks elsewhere within the business, then it is important to take these commitments into account to check on their availability.

Estimates and costings

This is a summarisation of the individual cost elements of a project. It is important to use cost methods and valid data so that an estimate of future costs can be calculated. There are many costs that may arise over the life cycle of a project and accurate estimates and costings can have an impact on the successful completion of a project. Projects always attract risks and those in turn bring in unexpected costs. Cost estimation takes several factors into consideration.

Venues/premises

Considerations for venues/premises depend on the requirements of the project. This can be in relation to where the project review meetings will take place, the locations of where the project activities will take place, and also how meetings and collaboration will take place if the teams are not in the same location.

Facilities

It is also important to plan what facilities are required. These can include toilets, breakout areas, food and

drink facilities, health and safety support such as first aid, fire extinguishers and so on.

Equipment

The equipment that is required will of course depend on the project. The equipment can include computers, whiteboards, smart devices and projectors – basically any equipment that is required to support the development of the project.

Hardware and software

Again, this is very dependent on the project. Hardware can include computers, networks and scanners – any type of technological hardware that is required along with the software to enable the team to use the hardware. Software can be bespoke packages, off-the-shelf packages, software available from the cloud and so on.

Stakeholder engagement

For a project to be successful, it is important that the stakeholders are engaged and that the organisation has a clear vision. This is achieved through a robust strategic planning process, and an effective strategic plan or marketing plan. This can only be achieved through stakeholder engagement. Key stakeholder opinions are very valuable when planning a project. They can provide useful information relating to the operating environment of the business, the marketplace that the business functions in, the needs of the users and the customers and so on. Stakeholders can include the board of directors, business owners, employees, shareholders, customers and suppliers.

Budgeting

It can be difficult to budget for any project. It can be more effective if you follow a simple process during the planning process.

Accurate estimating and forecasting

There are four essential elements to consider to ensure the accuracy of the estimates made:

- ▶ Confirm the project priorities, ensuring that the requirements are clear and in order of priority.
- ▶ Ensure the planning process allows for complete and appropriate estimates. The stakeholders must be informed of what exactly will and will not be provided by the project.
- ▶ Consider lessons learned from other projects. It is important to consider previous projects within the business and the causes of their success or failure, to establish what has been learned.

- ▶ Do not make the plan fit the senior management's wishes for lower costs and reduced time allocation if there is a need for higher estimates and/or time.

Estimating and forecasting is not just about finance but also relates to time and the resources required by the project. Depending on the project, considerations must be given for:

- ▶ the number of people, their skills and their schedules
- ▶ funding required and available
- ▶ resources including equipment, hardware and software
- ▶ requirements for the project.

Financial contingency planning

It is important to develop a financial contingency plan when working on a project. Setbacks and issues can arise suddenly, for example economic downturns, technical failures, losing customers, natural disasters and supplier bankruptcy. Financial contingency planning includes how to respond quickly to such occurrences and ensure that the project gets back on track. It is important to prioritise the actions that will need to be taken and the costs involved should an issue arise. The business needs to remain solvent and operational during this time.

A financial contingency plan will identify the project's 'worst case scenarios', the impact that they will have on the project and potentially the business, and how they can be responded to, to ensure a positive outcome. Financial contingency plans provide the basis for mitigating risks to the project and the business overall.

The following approach can be taken when developing a financial contingency plan:

- ▶ Identify any risks that could cause problems for the project and potentially result in failure of the project or damage to the functioning of the business.
- ▶ Document the understanding of why these risks may occur.
- ▶ Identify any potential signs that a risk may be occurring and how these can be spotted in advance of the risk occurring.
- ▶ Document in detail the strategy to be used to respond to each risk to include prioritisation (more than one risk may occur at the same time), the steps to be taken, how they will be taken, by whom and in what timescale.

Once the risks have been identified, it is then important to consider the financial resources available and how these will be used to respond to the risks.

- ▶ Analyse the financial profile by considering the costs of the various aspects of the project and how the risks can have an impact on the finance available.
- ▶ Ask questions such as how much finance is required in reserve? What resources and assets are critical and therefore required and therefore need to be protected? Are there any areas where the spending can be reduced without creating further risks to the project? Is there easy access to more funds if they are needed?

Reasonable and documented assumptions

As part of the budgeting for a project, it is important to identify any assumptions that were taken when calculating the figures. Some of the assumptions made will become a reality while others may not. It is always important to ensure that the project reflects reality. A timeline should also be included with these assumptions if the budget needs to span a significant period. This ensures that any recurring costs can be clearly identified and that the timing of when the costs will occur is also clear.

Cost–benefit analysis

A cost–benefit analysis is where the costs associated with the project are evaluated against the benefits to the business.

This is achieved through using a systematic approach to calculate the positives and negatives of various paths throughout the project which include transactions, tasks, business requirements and other investments. It provides the options and the best approach to achieve the purpose of the project while saving on any investments. A cost–benefit analysis therefore identifies whether the project is justifiable, feasible and achievable by determining if the benefits outweigh the costs. It also provides a baseline for comparing project options in order to determine which project option provides the greater benefits compared to the costs.

Viability of project

The difference between the cost of the project and the benefits from the successful completion of the project will confirm whether the project should be taken forward or not. Usually, if the cost is 50% or less of the benefits, and the payback timeline is no more than one year, then the project is worth taking forward.

Quantifying the intended deliverables

A list of the project expenses is put together along with what the benefits will be, based on the

Key terms

Return on investment (ROI): a measure used to evaluate how well an investment has performed. It is expressed as a percentage that is calculated by dividing the potential income from the benefits by the cost of the project.

Internal rate of return (IRR): this is the annual growth rate of an investment a business is expected to generate. In the case of a project, it is the annual increase in profits/benefits on completion of the project.

Net present value (NPV): this is used to calculate the total value at the current time of the expected income generated.

deliverables on successful completion of the project. This enables the business to calculate what is called the **return on investment (ROI)**, the **internal rate of return (IRR)**, the **net present value (NPV)** and the period of time of the payback.

Test yourself

- 1 Explain the term ‘viability of a project’.
- 2 Identify two benefits of developing a good resource plan.
- 3 Describe the term ‘financial contingency planning’.
- 4 What does the term ‘return on investment (ROI)’ mean?
- 5 Identify the four elements that should be considered to ensure the accuracy of estimates.

Project life cycle

All projects should follow a defined set of phases. Following these phases increases the potential to produce project deliverables which are fit for purpose and meet client requirements. There are many phases to the project life cycle including:

- ▶ initiation
- ▶ planning
- ▶ execution
- ▶ evaluation.

Initiation phase

During the initiation phase there are questions that must be considered and answered. This will enable the project manager and client (business) to establish

whether the project is feasible. The types of questions could include:

- ▶ What are the deliverables and who are they for?
- ▶ Who are the people involved and what are the resources that are required to complete the project?
- ▶ What is the timescale for the project and is this timescale realistic?

In addition, during this phase, the client (business) will provide a list of the requirements for the deliverables for the project as well as any time constraints or restrictions such as:

- ▶ timescales for completion of project
- ▶ the available budget
- ▶ security requirements
- ▶ legislative requirements
- ▶ hardware/software requirements for the development of the deliverables
- ▶ hardware/software that the deliverables must be compatible with.

At the end of the initiation phase, a review is carried out to confirm the feasibility of the project and that approval has been given to continue. It is also used to identify any issues that may have arisen/been identified and how these were or could be addressed.

Planning phase

During the planning phase the constraints and requirements are used to create a detailed project plan. This project plan will be used by the project manager to monitor the progress of the project. The planning phase is the most important phase of the project life cycle. If the plans are not detailed enough, then the project may not meet the client's requirements or achieve the deadline for completion. In addition, the project could go over budget. A list of constraints will be developed and referred to throughout the duration of the project to ensure that they are being met.

During the development of the project plans, the project manager must define the:

- ▶ tasks to be carried out to complete the project
- ▶ timescales for the completion of each task
- ▶ the workflow/linking of the tasks including prioritisation of tasks and dependencies
- ▶ contingency time should an issue arise
- ▶ milestones, stating what should be completed at certain key points throughout the project
- ▶ end point for the project
- ▶ resources, including specialist staff and equipment to complete each task and their availability.

Key aspects of project planning are considered in more detail below.

Timing and scheduling

A project schedule is a document that organises the project tasks, task timescales, start and end dates, and milestones on a timeline. The schedule will also define the project team members and the resources needed to complete each of the tasks. The project schedule is an important component for the planning and control of the project. All the work required to achieve the deliverables is identified in the schedule along with all associated costs as outlined in the budget.

Project communication plan

A project communication plan is also a key component of the project planning stage. This identifies how important information will be communicated to relevant stakeholders for the duration of the project. It determines who will receive the communication, how the communication will be received by the stakeholders and how often the information is provided. A good communication plan should include:

- ▶ the purpose and goals of the communication plan
- ▶ information about who the stakeholders are and their roles
- ▶ the types of information that will need to be communicated to different stakeholders
- ▶ the method(s) used to communicate the information
- ▶ how often the stakeholders will be provided with information.

Good and regular communication with stakeholders is important as poor communication can result in a project failing which could result in severe financial loss to the client (business). A project communication plan will:

- ▶ provide written documentation that can be used by the project team for reference during the project
- ▶ set the expectations of when stakeholders will receive updated information
- ▶ increase the visibility of the stakeholders in the project and provide updates on the current status of the project during the life cycle
- ▶ provide the opportunity for stakeholders to offer feedback that can help to identify potential issues early which can be addressed and reduce the risk of wasted work, time and money
- ▶ improve the productivity of meetings (and in some cases can eliminate meetings altogether).

Reporting schedules

Reporting schedules determine the reports required so that everyone with an interest in the project knows what to expect, and usually include important project updates. But it is always important to continue the

communication between the scheduled reports. The types of reports created could include:

- ▶ **Team availability** – this indicates the resources available to complete the tasks. It determines how much work each team member has and their availability for additional tasks. This enables the project manager to make smart resourcing decisions for the project.
- ▶ **Risk assessment** – this report will identify and categorise any risks to projects and their severity and possibility of occurring. The issues/risks can then be prioritised and addressed promptly so that the project does not fail.
- ▶ **Timeline tracking** – this provides an overview of how much time the team is taking when working on the various project activities. This can then be compared with the estimated project timelines and highlight any potential budget overspends. This can also be used to help consider appropriate timelines for future projects.
- ▶ **Status report** – this is used to keep the project team members and other relevant stakeholders informed on the progress of the project and to manage their expectations. The status report could include:
 - information relating to completed activities
 - activities that are due to be started
 - issues or risks that have arisen and how these have been addressed or mitigated against
 - overall completion of the project to date and the amount of budget spent
 - actionable items (things that must be carried out to keep the project on track/to budget, etc.).
- ▶ **Project health report** – this provides an overview of the status of the project. It can be shared with the team and stakeholders to indicate at a glance what activities are on schedule, what activities are behind schedule and any activities that are overdue.
- ▶ **Baseline report** – this report is a comparison of the original timelines within the actual project timeline and is useful for showing how changes or delays have affected the overall project timeline. It is also useful when considering timelines for future projects.

Work packages to break down deliverables

All projects create deliverables which are basically the results of the project or the processes in the project. A deliverable can be a product (something that is tangible) and it can be the overall end product after the completion of the project. Deliverables are broken down into small components that are known as work

packages. Each of the work packages must be small enough to enable the project manager to estimate the timescales and costs. They can be scheduled, estimated with respect to cost, monitored and controlled. For example, a deliverable is to create a website: an example of a work package could be the design documentation or creating a prototype to show the client. Here are some of the benefits of work packages:

- ▶ They allow for simultaneous work to be done on different components of a project by different team members. Each team member will follow their respective tasks (as defined in the work package) and complete them by a specific deadline.
- ▶ Costs are initially estimated at an activity level, but these estimates are also considered at work package level and can more easily be measured, managed and controlled.
- ▶ It can help to determine the direct costs for labour, material, equipment and so on as well as any indirect costs associated with each of the work packages.

Milestones

Milestones mark specific points in the project's timeline. They are used to indicate when an activity or group of activities have been completed or when a new activity or phase within the project life cycle is to start. They are important because they confirm the progress in the project plan. Milestones are used to monitor deadlines as well as identify important dates within the project. They provide the key steps and phases of the project.

Milestones usually coincide with the phases of the project life cycle and, as they mark major progress made within the project, they must be acknowledged and reported on when reporting on the progress of the project.

Prioritisation identification

If a task is more important than others, then this is a priority. Prioritising the organisation of tasks with respect to importance compared to each other is an important aspect of project planning. Prioritising tasks helps to determine where time needs to be allocated and which tasks should be assigned to project team members. Below are some steps that can be taken to identify and prioritise tasks and even risks within a project.

- ▶ Create a list of tasks and responsibilities.
- ▶ Evaluate the importance of each task. This is where the tasks are ranked in terms of the value they add to the project. This can also include the identification of priorities based on what and who

- is impacted and the potential consequences to the project and/or the business.
- It is important to prioritise how much time can be dedicated to a task. People can spend too much or too little time on a task and productivity can be affected.
- Once the prioritisation has been carried out and documented, it is important to follow the list of priorities. It is also important to be aware that priorities may need to change for some reason or another. Therefore, it is important to identify a task which is urgent or important. Some unforeseen issue might occur and therefore priorities may need to change.

Identifying dependencies

No task or activity exists in isolation. Every task/activity relies on the output of others and contributes to the input of others and the final project outcome. The relationships between these tasks/activities are called dependencies. Maintaining a record of these linked (dependent) tasks/activities and managing them effectively is an essential part of project planning, scheduling, monitoring and execution.

Below is a list of steps that can be taken to effectively identify and manage dependencies:

- **Identification** – it is important to brainstorm all possible project dependencies. This can be carried out during a team meeting with members of the project team and other relevant stakeholders. The activities will be discussed and how they are related to one another, and how they may be affected by outside influences.
- **Recording** – a dependency log should be created and include:
- an identification reference for each dependency
 - a description of the dependency
 - a date that the dependency must start and end by
 - the activities and/or people that are impacted by the dependency
 - a calculation of the probability of an issue arising with the linked activities
 - an assessment of the impact if the dependency is not delivered as planned
 - nominating the ‘owner’ for each dependency – this will be the person responsible for the progress of the task.
- **Monitoring and control** – the successful delivery of any project relies on the constant monitoring and

control of the dependencies. Regular meetings should be scheduled to discuss how the linked activities (dependencies) are progressing, where there are any changes to the schedule or requirements and what the potential impacts are on the other linked activities.

► **Communication** – it is important that there is effective and efficient communication in place when managing the dependency of activities. This includes ensuring that all team members understand their responsibilities and that these are in line with the dependencies that must be completed. This will help to prevent issues causing problems during the project life cycle. Regular communication with key stakeholders is also important to ensure that they understand how the dependencies can influence the progress of a project and therefore realistic expectations should be set.

A review is carried out at the end of the planning phase. This is to ensure that all areas have been covered and that the project is still in line with the customer requirements as well as any issues that may have arisen.

Execution phase

This is the longest phase of any project life cycle. During this phase, the final product (deliverable product) is created and tested. The overall project plan that was developed during the planning phase is used by the project manager and the project team to carry out the tasks and monitor the progress of the project. In addition, it will help to identify and address any issues in relation to time, budget and resources, including specialist staff.

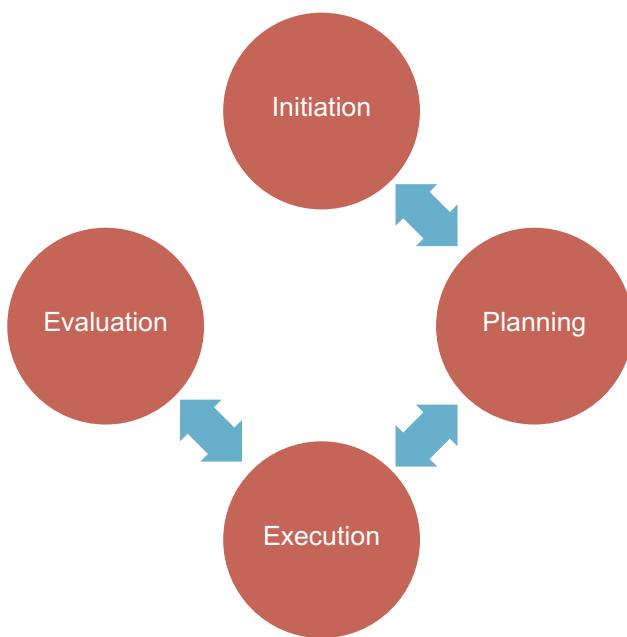
The plan will also be used to monitor and mitigate against other risks that may arise such as changes to legislation and security. At the end of the execution phase a review is carried out to discuss progress/completion and any issues that arose.

Evaluation phase

This is the final phase of the project life cycle and the stage within the project when the deliverable product is released to the client/business. It is also the stage where user documentation is created (if required). The user documentation created may include installation instructions as well as user guides. The review carried out during this phase focuses on the overall project including the deliverables required by the client/business. The review includes:

- ▶ the success of the project measured against success criteria and user requirements which were defined during the initiation phase
- ▶ any deviations from the original project plans
- ▶ the effect of processes and resources on the creation of the deliverables
- ▶ maintainability, which includes any future development of the deliverables or adapting to any changes in the client's business/organisation.

Once the review has been carried out, the deliverables and user documentation are passed to the client.



▲ **Figure 9.1** The interaction between the phases of the project life cycle

Test yourself

- 1 Explain the term 'milestones' in relation to project management.
- 2 Identify the phase of the project life cycle that occurs after the planning phase.
- 3 Discuss the term 'dependencies', and the steps that can be taken to effectively identify and manage them.
- 4 Explain the purpose of the project communication plan.
- 5 Explain the role of the execution phase within the project life cycle.

Risk and issues management

Unexpected problems and queries can arise within the life cycle of any project. When these problems/queries appear, then the project manager must be able to deal with them as they can have an impact on the outcome of the project. It is therefore important that there is an issue resolution process in place before the project is started. This will ensure that the project remains on schedule and that the objectives are met. Unexpected outcomes could include:

- ▶ staff shortages due to sickness among project team members
- ▶ a failure in a system that was not anticipated and requires rectifying before the project can continue
- ▶ a delay in the receipt of materials from suppliers.

Issue management involves the process for identifying and resolving issues. If the issue is unresolved, there is a risk of unnecessary delays or even failure of the entire project.

Project risk and issue management can be overlooked easily but it is critical for the success of any project.

Risks and issues that arise can have a severe impact on project plans and divert attention away from the project activities that must be carried out.

The **risks** associated with a project have several attributes as follows:

- ▶ They are usually identified at the start of the project.
- ▶ They can exist through the life of the project or at specific points within the project.
- ▶ They can impact on the outcome of the project if the risk actually happens.
- ▶ There is a possibility that the risks may happen.

Issues are problems that actually occur during a project that require action in order to resolve them. If an issue is not addressed promptly and appropriately, it can have an impact on the successful completion of the project.

Issues must not be confused with risks. An issue does not usually exist throughout the life of the project and may not be identified at the start of the project. The list of issues will open and close as they are identified and resolved, unlike the list of risks associated with the project.

It is important to recognise the differences between risks and issues:

- ▶ **Risks** are things that have the potential to occur or go wrong. It is very important that risks are

considered at the beginning of a project. This is to ensure that all interested stakeholders are aware of the things that could have an impact on the success of the project's outcome. Risks are the anticipation of something happening. They may happen or be unlikely to happen, but even the smallest possibility of there being any impact on the project must be considered as a risk.

- ▶ **Issues** are events that happen and have an impact on the project while it is in progress. The project manager is responsible for responding to these events and ensuring that any impact on the successful outcome of the project is minimised. Issues require immediate attention and may be a consequence of risks previously identified. Issues invariably arise in the vast majority of projects and they must be dealt with efficiently.

Identification

The first thing the project team must establish is what could go wrong.

Are there any factors which could have an impact on any part of the project being completed?

When identifying risks to a project it is important to think about the potential impact the risks could have on the project and what ways these impacts can affect the project. Considerations need to be made as whether these will delay the project or increase its costs. Consideration should also be given as to whether there will be any effect on the quality of the deliverables of the project.

It is important to quantify the effects, for example:

- ▶ For how many days or weeks will the project be delayed?
- ▶ How much will the original budget be increased by?

By quantifying the effects, it shows that these are real threats to the project with real consequences.

As previously stated, issues occur during the life of the project and are identified as they arise.

Probability

Risk probability is determining the likelihood of a risk occurring. This can be based on historical project information, for example does this risk occur frequently? It can also be determined through interviewing people or having meetings with relevant stakeholders. When determining the probability of risks, they are usually given a score, for example 3 = high, 2 = medium and 1 = low. One of the most common scales used is 0–5.

Impact

It is important to evaluate the impact of the risk if it were to occur.

Would the risk have a major or possibly severe impact on the project or is it just a minor inconvenience?

Impact assessment is usually carried out during meetings or interviews with relevant stakeholders. Once the evaluation has taken place, the impact of a risk is also given a score, for example 3 = high, 2 = medium, 1 = low.

Prioritisation

It is easier to prioritise risks through a visual representation. This is referred to as a probability and impact matrix. Imagine a three-by-three squared grid. The probability will be shown on the left with high probability at the top, medium probability in the middle and the lower probability on the bottom. The impact will be shown across the bottom with the high on the left, medium in the middle and the low on the right.

If the scores are used as previously described, then the risks can be prioritised. For example, a risk has a high probability of 3 and a high impact of 3. Therefore, it has an overall score of $3 \times 3 = 9$. So, it will be placed in the upper left-hand column of the matrix. If the risk has a low probability of 1 and the impact has a low score of 1, then the overall score of $1 \times 1 = 1$ and it will be placed in the lower right corner of the matrix.

		IMPACT		
		High	Medium	Low
PROBABILITY	High	Risk 1 $3 \times 3 = 9$ (High)	Risk 6 $3 \times 2 = 6$ (High)	$3 \times 1 = 3$ (Medium)
	Medium	Risk 2 $2 \times 3 = 6$ (High)	Risk 5 $2 \times 2 = 4$ (Medium)	Risk 8 $2 \times 1 = 2$ (Low)
	Low	Risk 3 $1 \times 3 = 3$ (Medium)	Risk 4 $1 \times 2 = 2$ (Low)	Risk 7 $1 \times 1 = 1$ (Low)

▲ **Figure 9.2** An example of a simple probability and impact matrix

Analysis

This is the process of determining how likely it is that a risk will happen in a project. It is a study of the uncertainty and how this would impact the project with respect to the schedule, costs and quality. There are two ways that risks are analysed, and these are qualitative and quantitative. There are several benefits to risk analysis as follows:

- ▶ to address regulatory issues
- ▶ to comply with new legislation
- ▶ to minimise the impact
- ▶ to reduce exposure
- ▶ to reduce any negative or harmful effects if the risk should occur
- ▶ to avoid any legal action.

While the evaluation of the risks to a project begins in the planning stage, it must continue throughout every stage of the project. But in order to look into the risks in depth, qualitative and quantitative risk analysis must take place.

Qualitative risk analysis

This is the process of prioritising risks for further analysis and/or action. The probability of each risk occurring is determined and rated with respect to its impact on the project. The scale commonly used to rank a risk is 0–5. For example, if the scale of the likelihood that the risk will occur is 0.5, then there is a 50% possibility that it will occur. The impact scale is also measured as discussed previously with 3 being the most impact on a project. The risks can then be categorised as source-based (the risk itself) or effect-based (the impact of the risk).

Qualitative risk analysis reduces the uncertainty in the project and encourages the focus to be on high-impact risks, which can then be mitigated against as part of the planning process.

Quantitative risk analysis

This is a statistical analysis of the effect of identified risks on the project. Decisions can then be made to reduce uncertainty and support the process of controlling the risks. Quantitative risk analysis counts the potential outcomes of the project and ascertains the probability that the project objectives will still be met. This helps with the decision making when there is uncertainty and creates targets for costs, schedule or scope that are realistic.

Contingency planning

A contingency plan is a defined and actionable plan that is to be carried out should an identified risk occur. Think of it as a 'Plan B' when things happen differently to what was originally planned. The Project Management Institute defines contingency planning as

'involving defining action steps to be taken if an identified risk event should occur'.

Contingency plans in project management are a component of the overall risk management and should be part of the risk management plan.

Contingency plans are only used where risks have been identified. They cannot be used for unidentified/unknown risks because if you do not know what the risk is you cannot plan for it. Contingency plans can also be implemented for strategic advantage. For example, a new piece of software and/or hardware is to be released during the project life cycle; the contingency plan could include how to incorporate the new software or technology into the project.

Contingency plans should not be confused with mitigation plans. A mitigation plan is used to reduce (hopefully) the chance of a risk occurring or to reduce the impact of the risk should it occur. A mitigation plan is implemented in advance. The contingency plan identifies the steps to be taken after the identified risk occurs in order to reduce the impact.

The following guidelines can be used to help develop a contingency plan.

- ▶ Identify what event or events need to occur to trigger the implementation of the contingency identified in the plan.
- ▶ Ensure the plan identifies who will be involved, what their roles and responsibilities are, where it will take place and how the plan will be carried out.
- ▶ Ensure there are clear guidelines for reporting and communication during the execution of the plan. This should include how relevant stakeholders are notified, who will prepare the information for the stakeholders, and the timescale for the notification to be sent. How often will updates be provided on progress with the contingency?
- ▶ The plan should be monitored on a regular basis to ensure that it is up to date.

Quality management

There are processes and activities that are undertaken to ensure the quality of the deliverables of a project. With respect to quality management, quality is what the client/business/stakeholder needs from the project deliverables.

Monitoring of project deliverables

If the project deliverables are not up to standard, it does not matter whether you have used the best specialist skills, software and/or hardware, achieved every milestone and completed the project on or under budget. Therefore, the monitoring of deliverables is an important component of quality management. Defining, tracking and managing project deliverables is one of the key responsibilities of the project manager. The following points provide guidance on what should be implemented in order to monitor project deliverables.

- ▶ Deliverables should be defined before the project starts. This provides a clear indication of what the project should entail and how it will be completed. A method often used for defining and planning the deliverables within a project is a Gantt chart. This provides a visual representation of the breakdown of each phase of the project. It is used in conjunction with the deliverables in order to set the project milestones.
- ▶ It is important to understand the requirements of the deliverables. There are two components to project deliverables: the deliverable itself and the acceptance criteria for the deliverable. Prior to a deliverable being accepted, it must meet the requirements of the client/business/stakeholder.
- ▶ Invite input from stakeholders at the start of the project. This is important to understand the criteria for acceptance of the deliverables. It provides a guide to the expectations and helps to define the scope of the project.
- ▶ Break down the deliverables into work packages (referred to as the work breakdown structure (WBS)). This allows different aspects of the deliverables to be delegated and tracked more easily. Stakeholders can provide feedback on these specific work packages and the deliverables as a whole throughout the project life cycle to ensure that the expectations of the client/business/stakeholder meet expectations.
- ▶ Identify whether a deliverable is internal or external. Internal deliverables do not involve external stakeholders and can include tasks such as

creating documentation. The internal deliverables do not necessarily provide income for the business. External deliverables are the outcomes that meet the requirements of the client/business/stakeholder. External deliverables are very important as these relate to the client/business/stakeholder requirements.

- ▶ Identify the process and product deliverables. Process deliverables are the steps taken to help create the project deliverables. Process deliverables will include creating a project plan and the work breakdown structure. Although process deliverables are not the focus of the project, they nonetheless support the managing of the project process.
- ▶ Clear deadlines should be set for each deliverable. They ensure that each deadline is integrated into the project milestones for every step of the project and allow it to be tracked easily.
- ▶ Milestones must be set by breaking down the deliverables into phases. This allows for more effective tracking of progress of the deliverable. Milestones are the checkpoints during the life cycle of the project and do not have hard deadlines. They are used to check progress and ensure that the project remains on track.

It is essential to create a carefully planned strategy for tracking project deliverables. This helps to keep a project within budget, within scope and on track, and assist in keeping key stakeholders up to date with the progress of the project.

Quality assurance

Quality assurance should not be confused with quality control.

- ▶ **Quality assurance** relates to the monitoring and co-ordinating of the quality used within the project management life cycle by evaluating the processes and procedures that are in place.
- ▶ **Quality control** is where the deliverables are compared to the specification or plan, with its focus on detecting and addressing errors or anomalies.

Quality assurance, therefore, is a critical component to ensure the success of the overall project by focusing on key quality functions.

Quality control

This involves the activities used to evaluate whether the deliverables meet quality requirements as specified for the project. Quality control is an important aspect of project management as it ensures that everything is within the scope of the project planning. The quality

control process includes the inspection and verification of the deliverables. It also includes the monitoring and recording of the results obtained from the execution of quality activities, which in turn support the assessment of the performance of the project. The results of quality control are required to put forward any recommendations for potential changes. Quality control provides the following benefits:

- ▶ validation of the deliverables
- ▶ confirmation of meeting the requirements specified by the client/business/stakeholder
- ▶ identification of causes for poor product quality
- ▶ support for recommendations for actions to be taken to eliminate issues relating to quality.

Review and audit

A project quality review helps to identify the causes of problems for a failing project and provides guidance on how it can get back on track. When undertaken at the end of a project, it provides insight into the lessons learned for working on future projects. The process for carrying out a project audit or project quality review is similar regardless of when it is carried out, for example mid-way through a project or at the end with conclusions formed.

There are three key phases to a project quality review as outlined below.

Phase 1

Planning the project quality review and audit. The review and audit are usually planned during the planning phase of the project and they will include the audit process and dates to be undertaken. It is important to make clear the expectations of the project quality and audit reviews.

Phase 2

Project analysis. This is a comprehensive phase and involves the review of the entire project. Information is gathered to assess the issues, challenges and concerns within the project and to ascertain the causes of any problems that have arisen.

Phase 3

Report and recommendations. A detailed report is produced that includes recommendations which are presented to senior management. There will be specific recommendations and actions to improve the overall performance of the project. The report incorporates the findings from all of the information collected; that may include interviewing key stakeholders, attending meetings and reviewing project documentation. All project issues, concerns and challenges are

identified and support is provided for the detailed recommendations and actions to get a project back on track and improve the overall project performance.

For quality reviews carried out at the end of a project, the report and recommendations will provide outline recommendations for future projects. They will also validate whether resources were used effectively and efficiently on the project.

Test yourself

- 1 Explain the importance of monitoring project deliverables.
- 2 Describe the difference between a project aim and a project objective.
- 3 Describe the term 'cost–benefit analysis'.
- 4 Explain the difference between a risk and an issue.
- 5 Discuss the project planning phase and the different aspects of the process that must be included and documented.

9.2 The consequences of ineffective project planning

The project planning phase is an extremely important aspect of any project. Poor project planning invariably means that a project will fail. Although a project may be completed, it does not necessarily mean that it is successful if it results in overdue deadlines, overspend on budgets and dissatisfied stakeholders.

Under-resourced

There are many reasons why there may be a shortage of resources including:

- ▶ not adhering to the initial project estimates
- ▶ organisational changes resulting in budget cuts
- ▶ an urgent increase in the need for the project deliverables
- ▶ availability of project team members (e.g. functional managers not ensuring that their staff are available for the project or not providing staff with sufficient experience or any experience at all).

Without sufficient resources (or having improper resources), the project is at risk of failing the project deliverables on time and within budget. Also, project team members may experience additional pressure in order to achieve unrealistic goals with a lack of resources.

It is important that the project manager communicates with the stakeholders to ensure that sufficient resources are available and incorporated into the project plan.

Escalating costs

There may be occasions when the original estimated costs for a project are completely out of line with reality. This can be due to the need for additional resources, or just the price of resources increasing. If there is a lack of resources due to a lack of available funds, then the project will stop and fail.

An inaccurate estimate of the costs is one of the biggest factors behind project failures. It is always a good planning strategy to obtain a higher budget than you might initially think is required. It is also important to identify any lack of resources that will require more funds as early as possible. Stakeholders can then be approached, and if possible, more funds secured.

Exceeding timeframes

Missed or exceeded timeframes cost money and break the trust of the stakeholders. There are many reasons that timeframes can be missed including:

- ▶ A client/business/stakeholder can insist on very tight timescales for finishing a project and there is little choice but to try and comply with their requests.
- ▶ Timeframes may not have been calculated accurately as it can be difficult to track and manage resources through the duration of the project.
- ▶ Project team members may be given too much work to do and cannot complete the work in sufficient time.

The consequences for exceeding timelines can include:

- ▶ loss of confidence by the project team, management and other relevant stakeholders
- ▶ loss of existing clients/businesses
- ▶ loss of business growth opportunities
- ▶ overspend of budgets, for example due to project team members working additional hours to try and get the project completed
- ▶ loss of team members through over-work, for example leaving the organisation due to a stressful working environment, and absence due to sickness and stress
- ▶ low morale and lack of motivation and engagement from team members due to being under pressure and over-worked.

Projects meet deadlines when they are well-planned and have realistic timelines, including planning for uncertainty and the unexpected. Careful planning provides the opportunity for renegotiation of timelines during the project and the identification of potential issues.

Unable to deliver outcomes

It is important to understand that project outcomes are different to project deliverables.

- ▶ **Project deliverables** are outputs such as project plans, project reports and minutes of meetings. However, they can also be hardware, software, mobile applications, contracts or even test results. The final deliverables are the products that the clients/business stakeholders expect on completion of the project.
- ▶ **Project outcomes** are the changes that have been caused due to the project. They will be written as if the project has been completed. For example, customers will have regular access to their accounts, there will be a 25% increase in customers and so on. Outcomes need to be measurable.

If the outcomes cannot be delivered, then the project has not been successful regardless of whether the deliverables have been achieved on target and to budget. For example, a business wants a social media marketing campaign. The marketing resources are developed and uploaded onto the various social media platforms for the business. These are the deliverables from the project. Unfortunately, there has been a limited increased in customers and it is way below the required 25%. Therefore, the outcome has not been delivered and an evaluation of this will need to take place. Part of the planning process for all projects is consideration of realistic expectations for the outcomes, how they can be measured and the timescales for the measures to be taken to confirm that the outcomes have provided a positive result.

The consequences of not being able to deliver outcomes can include:

- ▶ loss of confidence by the project team, management and other relevant stakeholders (what is the point of the project if the outcomes are not met?)
- ▶ loss of existing clients/businesses
- ▶ loss of business growth opportunities
- ▶ low morale and lack of motivation and engagement from team members (who wants to work on a project where the outcomes are not being delivered?).

Negative environmental impact

The overall purpose of project management is to plan and complete projects within specified timelines and to budget. Projects, however, also need resources, which can include land, money, people, materials (raw materials and/or finished products), energy and communication. It is within this context that environmental issues, for example natural, physical and social, have to be considered as part of the project planning process. Often the environmental and social costs are neglected or only given minimal consideration during the project planning stage. A failure to understand adverse or negative impacts on the environment during the life cycle of a project can lead to several consequences which can hinder and/or prevent the growth and development objectives for which the project was proposed. Some examples of environmental impacts with negative consequences are provided below:

- ▶ **Access to capital** – the majority of projects require access to capital (money for tools, equipment, raw materials, wages, etc.) in order to move a project forward and ensure successful completion. Access to capital can be an environmental factor because any changes to the environment can include access to or the pricing of materials needed to complete the project. If these possible factors are not considered during the planning phase of the project, it can result in a project running out of money, going over budget or even not being able to have access to important materials or specialist staff.
- ▶ **Access to technology** – it may be limited, or the technology required may be expensive or not compatible with the existing technology or equipment. There is also the additional issue that training may be required on how to use the technology. This in turn can create delays and add further expense to the project.
- ▶ **Access to people** – all projects require people, some highly skilled and others with lesser (but nonetheless still important) skills. People are not always readily available and therefore there is the possibility of insufficient team members to complete the project. There could be a situation where there are insufficient people with appropriate skills that are critical to the success of the project. There is also the consideration of where the skilled specialists are situated (from a geographical point of view) compared to where the project is taking place. All of these factors must be taken into consideration when planning a project in order for it to succeed. Not

Key term

Economic shifts: this is a change in the structure of an economic system resulting in changes to societies, cultures and everyday life both on a national and a global level.

enough correct project team members can lead to the failure of a project or a delay in its completion.

- ▶ **Environmental changes** – these can include natural disasters or **economic shifts**. It is important during the planning phase that contingency plans are in place to mitigate against any negative impact on the project's success. Any of these issues can delay a project (meaning timelines are not kept), resulting in insufficient budgets or causing total failure of a project.

Research

Research examples of where environmental changes have led to the failure of projects. They can be any type of project.

Prepare a report to present the results of your research.

Health and safety risks

The planning of health and safety includes all aspects of health and safety conditions for the workplace and location where the project is taking place. Careful health and safety planning decreases the chance of project delays and the possibility of injuries. It also increases the potential success of the project and the confidence of the project team members. The plan should:

- ▶ protect the project team members (and any other employees that may be affected by the project taking place)
- ▶ anticipate any potentially dangerous situations and bypass any hazards
- ▶ provide guidance on the evaluation of the safety conditions of the project environment
- ▶ define the minimum requirements, equipment and/or tools needed to perform specific activities
- ▶ adhere to legal obligations as laid down in current health and safety legislation and regulation.

Scope creep

This is how the original project's requirements increase over the project life cycle. For example, a project could start with the development of a system, which was

required to have three main features and then the number of features is increased to five when the project is halfway through. The needs of the client/business/stakeholder change, and the project requirements must be reassessed. Scope creep can be caused by key project stakeholders changing the requirements, internal miscommunication and disagreements. Scope creep can result in delays to the projects, problems for which there are no planned contingencies, and overspend in the budget.

Test yourself

- 1 Explain the difference between project deliverables and project outcomes.
- 2 Describe how access to people can create a negative environmental impact on a project.
- 3 Identify three reasons why a project may be under-resourced.
- 4 Explain the consequences of exceeding timeframes in a project.
- 5 Describe the term 'scope creep' and explain the impact it can have on a project.

9.3 The application of project planning techniques in a business context

During the planning phase of the project, the project manager will use a variety of planning tools and techniques to create the documentation. Some plans will be used to monitor the progress of the project, other plans may be used during the reviews conducted at the end of every phase of the project life cycle. There are also plans that are used to show the tasks/

activities, process, resources and staff for each aspect of the project. There are many types of planning tools and techniques that can be used, and they are selected depending on the type of project and its complexity. Below are examples of planning techniques used in project management.

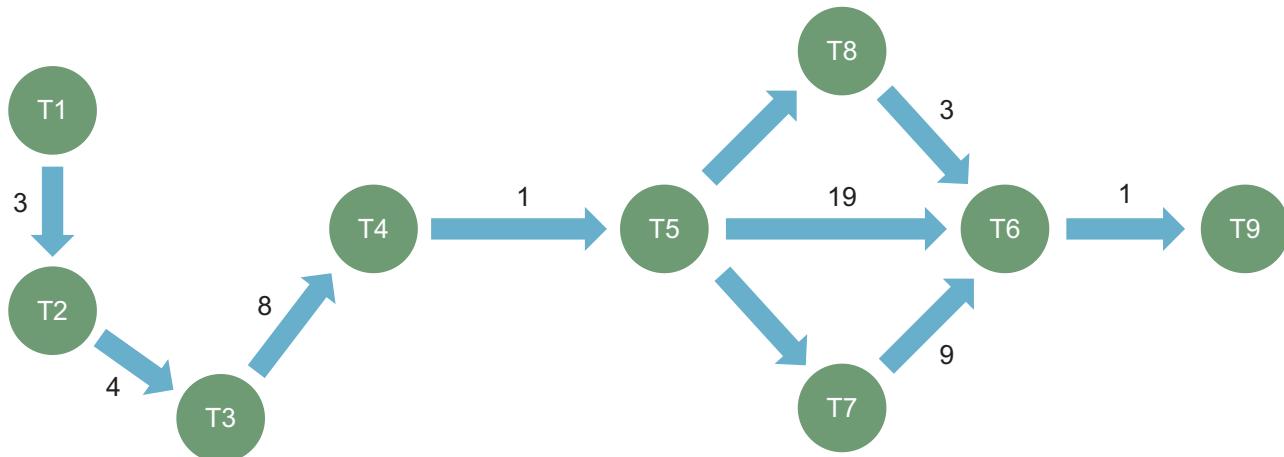
Programme evaluation review technique

A programme evaluation review technique (PERT) chart looks very similar to a railway map and consists of circles or rectangles (sometimes referred to as nodes). These represent tasks/activities or milestones. Lines are drawn between the circles or rectangles to represent dependent tasks/activities and the timescales allocated to them. These lines can come from any event to represent the tasks that can be carried out concurrently. PERT charts can also be used to show the critical path of the project.

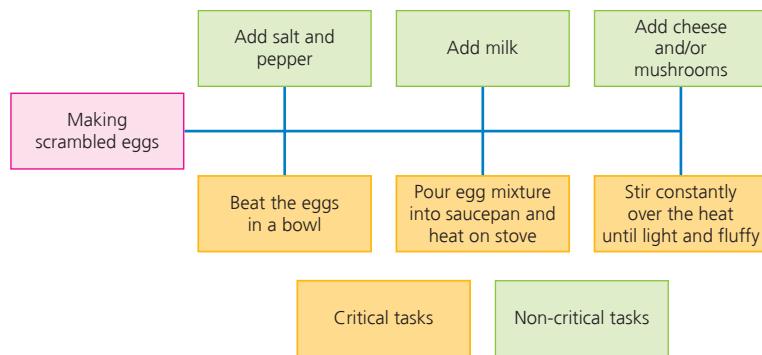
Critical path analysis

The critical path is the path that the project should take to be completed. It shows the dependent tasks and analyses them to calculate the total time to complete the project. This path then shows the shortest time that a project will take to complete (if everything goes according to plan). In addition, the critical path will show the tasks that are critical to the project and those that are not. For example, assume you are making scrambled eggs. A recipe could have the following:

- 1 Beat two eggs in a bowl.
- 2 Put beaten eggs into a saucepan and place over heat.
- 3 Stirring constantly, cook the egg mix until the scrambled eggs are soft and fluffy.



▲ Figure 9.3 A PERT chart



▲ Figure 9.4 An example of a simple critical path

These are not the only tasks you would perform to make good scrambled eggs. You would add seasoning such as salt and pepper, and you could add some milk, cheese and/or mushrooms. However, these tasks are in addition to the three main steps indicated above. If you do not perform these additional tasks, you will still have scrambled eggs, it just may not be as tasty. But if you do not beat the eggs, or cook them in the saucepan, you will only have a cold saucepan and two eggs. So, the three steps in the recipe above are the **critical** tasks required to ensure that the scrambled egg making project is successful.

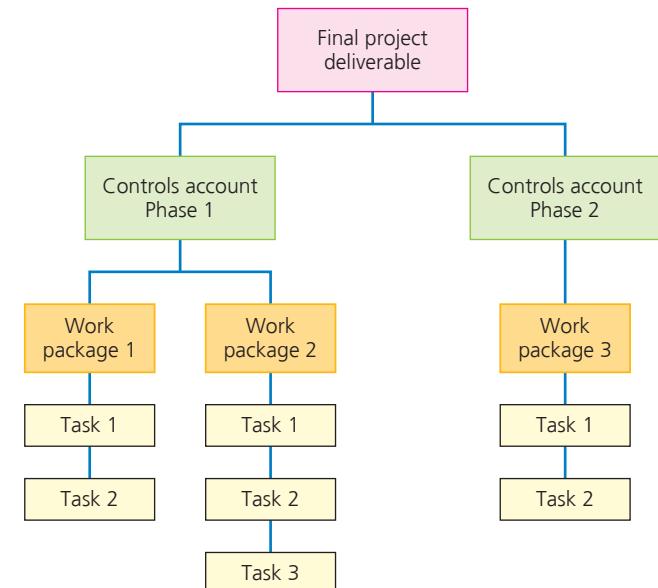
Work breakdown structure

This is a visual, hierarchical and deliverable-orientated deconstruction of a project. It allows project managers to work backwards from the final deliverable of a project and identify all the activities that are required in order to achieve a successful project.

The steps of the project are outlined in an organisational chart of the work breakdown structure (WBS), which is extremely useful for planning and scheduling. The final deliverable of the project is on the top of the diagram and the levels underneath are subdivided into the project scope. This indicates the phases, tasks and deliverables that are required.

There are four levels to a work breakdown structure as follows:

- ▶ top level – the final project deliverable
- ▶ controls account – the main phases of the project and associated deliverables
- ▶ work packages – the group of tasks that feed into the controls account level
- ▶ activities – the activities needed to complete the work package.



▲ Figure 9.5 A work breakdown structure

Step	Project initiation	Project executive	Project manager	Business developer	Technical architect	Website developer
1	Task 1	Consulted	Accountable and responsible	Consulted	Informed	Informed
2	Task 2	Accountable	Informed	Responsible	Consulted	Informed
3	Task 3	Accountable	Informed	Responsible	Consulted	Informed
4	Task 4	Consulted	Accountable	Informed	Responsible	Informed

▲ Figure 9.6 Simple example of a RCAI chart

Responsible, accountable, consulted or informed

A responsible, accountable, consulted or informed (RACI) chart is a responsibility assignment chart that is used to map out every task, milestone or key decision that is required to complete a project. Roles are assigned which are responsible for each of the actions. Accountable personnel are also identified along with who needs to be consulted and informed.

Must have, should have, could have, won't have

You may also see MoSCoW defined as ‘must have, should have, could have, would have’. It is important that you know which format you are using based on the ‘won’t have or would have’ option.

Many projects start with a limited list of requirements, only to discover that the requirements of the client/business/stakeholder have not been fully understood. Once the full set of requirements have been identified, they should be ranked. This helps everyone involved to understand which are the most important requirements and in what order they should be developed. It also indicates what are not so important if there is a restriction, for example with resources or budget, skilled specialists and so on.

So, the requirements are ranked using must have, should have, could have, won’t have (MoSCoW) as follows:

- ▶ **M** = must have this requirement to meet the business needs
- ▶ **S** = should have this requirement if possible but the project is not reliant on it being achieved to be classified as a successful project
- ▶ **C** = could have this requirement if it does not impact on anything else in the project
- ▶ **W** = depending on the format you use it could be ‘won’t have’ this requirement due to constraints, restrictions and so on or ‘would have’ the requirements if all aspects of the project are successfully achieved.

So basically, MoSCoW is a prioritisation method to establish which requirement must be completed first, which must come next, which are desirables if possible and what to exclude. Must requirements are non-negotiable and must be achieved. Failure to deliver the must requirements will result in the project failing. As many of the should requirements as possible should be delivered whereas the could or won’t (or would) requirements are the first to be dropped if the project timeline and budget are restricted.

Test yourself

- 1 Explain the purpose of a PERT chart.
- 2 Describe the term ‘work breakdown structure’.
- 3 What does the ‘A’ stand for in RACI?
- 4 Describe the MoSCoW prioritisation method.
- 5 Explain the purpose of the critical path analysis.

Project practice

You have been asked to project manage the trip of the company’s director to attend a conference in Lucerne in Switzerland. The director has informed you that

- ▶ he wants to fly from Manchester Airport
- ▶ he wants to leave as early as possible in the morning and arrive in Lucerne on the same day
- ▶ he would like to have the shortest flight time (if possible) without having to wait too long at any airports where he may have to change flights
- ▶ he will be staying in Lucerne for seven days and wants a hotel which has spa facilities and is situated in the centre of Lucerne

- ▶ he needs to catch a train from Nuneaton to Manchester which will get him to the airport in time for the flight, which means he needs to arrive at the airport at least three hours before the flight
- ▶ he will also be catching a train back from Manchester to Nuneaton when he returns.

There is a budget of £1500.

You are required to prepare a MoSCoW prioritisation document and justify your reasons for the priorities that you have given for the different aspects of the trip.

Assessment practice

- 1 Discuss the consequences of poor project planning.
- 2 What is placed at the top level of a work breakdown structure?
- 3 Explain the difference between quality assurance and quality control.
- 4 Describe what is meant by the viability of a project.
- 5 Identify two possible reasons for scope creep.
- 6 Explain the purpose of a critical path analysis.
- 7 Identify the four phases of the project life cycle.
- 8 Discuss the consequences of not being able to deliver project outcomes.
- 9 Explain why health and safety must be considered during the project planning phase of the project life cycle.
- 10 Describe the term 'financial contingency planning'.

Core element 10: Security



In this core element you will learn about the potential risks and threats to the digital systems used by organisations. You will apply your understanding of the implications of these to digital systems themselves, as well as to organisations and their stakeholders. You will also learn about the relationships between the different aspects of the data and information that an organisation stores and uses, including confidentiality, integrity and availability.

Each of these risks or threats can be mitigated against to limit its impact and to reduce the threat of it happening again. You will learn about a range of measures that can be used to do this. You will learn about several types of security. Cyber security is the most important type in relation to digital systems, data and information. Physical security can also be used to protect digital systems, data and information, including closed-circuit television and access badges.

Learning outcomes

In this core element you will learn about:

- 10.1** Types of confidential company, customer and colleague information
- 10.2** The importance of maintaining and the consequences of not maintaining confidentiality, integrity and availability
- 10.3** The technical and non-technical threats that may cause damage to an organisation
- 10.4** The technical and non-technical vulnerabilities that exist within an organisation

- 10.5** The potential impacts of threats and vulnerabilities on an organisation
- 10.6** Risk mitigation controls to prevent threats to digital systems
- 10.7** The process and protocols of internet security assurance
- 10.8** The interrelationship of components required for an effective computer security system

10.1 Types of confidential company, customer and colleague information

Important point

All businesses and organisations will have data and information that need to be kept secure, classified and confidential, which should be covered by the confidentiality, integrity and availability (CIA) triad. What data and information are stored will depend on the function of the organisation and will differ from sector to sector.

Confidentiality relates to data, while privacy relates to the individual. In this context an 'individual' can be a single person, a business or an organisation.

The General Data Protection Regulation is covered in section 8.1, p. 202.

The CIA triad is covered in section 10.2, p. 239.

Typically, an organisation will store information about:

- ▶ human resources
- ▶ commercially sensitive information
- ▶ access information.

It is important that this information is kept confidential. Any breaches relating to the information can have a serious impact, leading to the possible loss of clients or business. This in turn can lead to a downturn in the health of the organisation which may, ultimately, lead to the organisation's failure.

Human resources

Human resources (HR) will store and update any data and information held about everyone who works in a business or organisation, irrespective of their job role.

The main data and information held include:

- ▶ employee salaries
- ▶ employee perks
- ▶ employment data
- ▶ medical information.

The data held by HR is confidential, personal and should be stored following legislation guidelines related to the storing and processing of data.

Employee salaries and perks

Salaries should only be known by the employee and the HR department. It is important that this information is kept confidential as different employees carrying out the same task may be paid different salaries based on the number of years they have worked for the organisation, their experience and other factors such as qualifications and training courses attended. It is illegal to pay different salaries on the basis of gender as this would contravene the Equality Act. (Protected characteristics are covered in section 6.1, p. 156.) Data held by HR about salaries will also include National Insurance number and tax codes.

Many employers provide perks. Workplace perks can range from retailer discounts to free tea and coffee. Individual employee perks can include extra days holidays for long service or discounts on health insurance. Which employee gets which perk should, as with salaries, only be known by the employee and the HR department.

Employment data and medical information

Employment data will typically include start date, qualifications, contact details and emergency contact details. This data may also include any warnings about a breach of policy and disciplinary action. Medical data will be stored as an employer has a duty of care to provide, where required, adapted equipment and reasonable adaptations to enable their staff to carry out their job role. This is covered under the Equality Act. Staff may also require time off to attend medical appointments related to any medical condition.

Legislation is covered in section 8.1, p. 189.

Commercially sensitive information

Any business or organisation will store information which can be classed as commercially sensitive. This means that if the information was leaked, competitors could use it to gain a commercial advantage.

Commercially sensitive information includes:

- ▶ sales revenue
- ▶ trade secrets
- ▶ profit margins
- ▶ client/customer details
- ▶ stakeholder details
- ▶ contracts
- ▶ intellectual property.

Client and customer details

All organisations interact with people – clients and customers. Client lists and customer information are business-sensitive information that result from these interactions.

Client details may include individuals, but may also include named representatives from different organisations or businesses. Client details include anyone who interacts with the organisation and they should not be accessed by employees unless absolutely necessary. Clients may interact with the organisation by using the services provided. For example, a client may use the services of an organisation that provides cloud-based storage facilities. Many organisations will have a client relationship team that looks after clients so this team will need access to this information.

Customer details usually relate to those who buy goods or services. The information held about customers will typically include personal details such as name and contact details but may also include order history.

If the privacy and confidentiality of client and customer details are not maintained, the organisation could lose clients and customers. People expect that any organisation storing their personal data will keep it safe and secure to limit any breaches. A breach of personal data can impact the organisation and also the people whose data has been leaked.

Activity

Select an online retailer. Define the data that would be held about the customers. What would the impact on the retailer and customers be, including the consideration of relevant legislation (see Core element 8), if there was a data breach leading to the loss of this data?

Create a digital communication detailing your findings. Present your findings to your group.

Stakeholders and sales revenue

Most organisations have **stakeholders**. Depending on the size and type of the organisation these may be shareholders – **external stakeholders**. Employees can also be classed as **internal stakeholders**. Some organisations may have a policy of keeping stakeholders informed about sales numbers as this may have a financial impact. Some organisations provide a financial bonus to employees or a dividend to investors

or shareholders based on the previous year's sales numbers and revenues. Sales numbers can also be used to determine the goods that are bought and sold by the organisation. For example, goods that have low sales numbers may be reduced in price and not stocked again while those goods with high sales numbers will be restocked to continue the sale of them to customers.

Profit margins

The profit margin set on any goods supplied should also be kept confidential. The profit margin is the difference between the price paid for the goods and the selling price. Where the price of the goods is reduced, the profit margin will also reduce.

Contracts

A contract will be in place where goods are bought from a third party. The contract will usually include the delivery time, quantity required and the price to be paid. These details will be negotiated and should be kept confidential between the two parties. Any breach in this could lead to other companies having a stronger negotiating power.

Trade secrets and intellectual property

Where an organisation sells specific goods, these could be classed as a trade secret. Trade secrets often apply to a patent.

The Copyright, Designs and Patents Act is covered in section 8.1, p. 199.

The Intellectual Property Act (IPA) also covers software processes in addition to patents for tangible items. This means that if the function of the organisation is to provide cloud-based services then the software processes used by the organisation could be covered by the IPA.

Key terms

Stakeholders: anyone with an interest in a business or organisation. Stakeholders can be individuals, groups or other organisations, or businesses that are affected by the organisation's activity.

External stakeholders: groups outside an organisation, for example shareholders.

Internal stakeholders: groups within an organisation, for example owners and employees.

Activity

Using the same online retailer as in the previous exercise, define the data that could be held about the goods that are sold. What would the impact on the retailer and stakeholders be if the data was breached?

Create a digital communication detailing your findings. Present your findings to your group.

Access information

It is important that any access information provided to staff, at all levels, is kept confidential. This is to maintain the security of the workplace and the digital devices on which data and information are stored. The access information stored will include:

- ▶ passwords
- ▶ multi-factor authentication
- ▶ email accounts
- ▶ phone numbers
- ▶ access codes.

Passwords, multi-factor authentication and access codes are covered in section 10.6, p. 253.

How a threat can be carried out using email accounts and phone numbers is covered in section 10.3, p. 244 about malicious spam.

Test yourself

- 1 What is meant by privacy?
- 2 What are the two different types of stakeholders?
- 3 How do clients interact with an organisation?
- 4 Who should access employee salaries?
- 5 What is meant by profit margin?

10.2 The importance of maintaining and the consequences of not maintaining confidentiality, integrity and availability

Security, in particular cyber security, aims to protect digital systems, data and information. **Cyber security** attempts to:

- ▶ act as a deterrent against attackers and hackers
- ▶ prevent an attack from happening

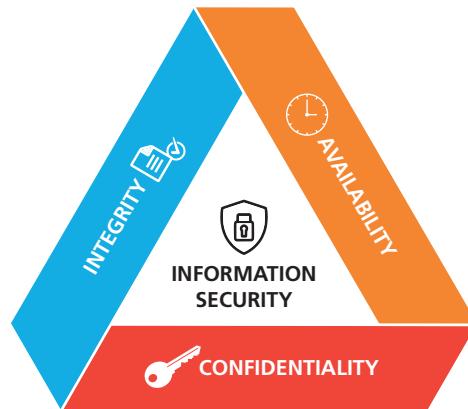
Key terms

Cyber security: the practice of defending computers, servers, mobile devices, electronic systems, networks and data from malicious attacks.

Confidentiality, integrity and availability (CIA): also known as the CIA triad.

- ▶ detect and warn users of the digital systems that an attack is happening.

The main purpose of cyber security is to maintain the **confidentiality, integrity and availability (CIA)** of digital systems, data and information.



▲ **Figure 10.1** The CIA triad

Figure 10.1 shows the CIA triad, viewed here as a triangle with security in the centre. The CIA triad is a security model developed to define the important parts of cyber security and how they are interlinked.

- ▶ **Confidentiality** means that the digital systems, data and information resources are protected from unauthorised viewing and access (hacking).
- ▶ **Integrity** means that data is protected from unauthorised changes to ensure that it is reliable and correct.
- ▶ **Availability** means that authorised users have access to the digital systems, data and information they require.

The CIA triad shows the clear relationship between these three parts of cyber security. Looking at these in a triangle we can see that they overlap, but they can also work against each other when deciding which types of mitigation to use. Visualising things in this way enables an organisation to plan and prioritise the implementation of new security policies and processes.

A good example of how confidentiality, integrity and availability interact can be found in online banking:

- ▶ **Confidentiality** – it is important to a customer that their financial details are kept confidential between them and the bank. One strategy that can be used to maintain the confidentiality of the financial data is through access-level login. When a customer logs into the bank website their log-in details provide access only to their bank account (and no one else's).
- ▶ **Integrity** – the financial data of the customer must demonstrate integrity. This means that the customer can expect their financial data to be correct. For example, their recent transactions using their debit or credit cards should be true and accurate. The financial data should also be reliable, which is linked to its accuracy.
- ▶ **Availability** – customers should be able to access both the bank website and their financial records when they want and need to. If the website or personal financial data is not available, then this part of the CIA triad has been broken.

The importance of maintaining confidentiality, integrity and availability

It is important that any business or organisation maintains CIA. By maintaining CIA:

- ▶ compliance with legislation and regulations associated with data can be maintained
- ▶ internal and external stakeholders can trust the business or organisation to keep data safe
- ▶ the business or organisation will have a positive brand image which may lead to an increased customer base so leading to more profit
- ▶ security risks and unauthorised access to data can be minimised.

Stakeholders are covered in section 1.1, p. 2.

Legislation is covered in section 8.1, p. 189.

The consequences of not maintaining confidentiality, integrity and availability

If CIA is not maintained, then the business or organisation may suffer consequences. These consequences include:

- ▶ financial
- ▶ legal
- ▶ reputational.

Financial consequences

The financial consequences can have a devastating effect. If data is breached, then fines can be issued under legislation relating to data. For example, the Data

Protection Act 2018 (DPA) and Computer Misuse Act (CMA) both have the provision to fine data holders where a breach has occurred.

In addition to the fine issued under the legislation, compensation will also have to be paid to the customers whose data has been part of the breach. The DPA requires data to be kept secure, usually by following the CIA triad. This means that measures must be put in place to prevent unauthorised or unlawful processing of data. Data must also be protected against accidental loss, destruction or damage. If a breach occurs, then those whose data is involved can make a claim for compensation. Refunds of any extra costs may also need to be paid. For example, if airline tickets need to be changed, then the cost of doing this can be claimed back.

When a data breach occurs, it is possible that the reputation of the business or organisation will be damaged. Customers need to be assured that their data is safe. After a breach it is probable that customers will move away as they feel their data is unsafe. This reduction in customers will cause a decrease in trading, leading to a reduction in revenue or earnings.

Legal consequences

The legal consequences of not maintaining the CIA triad can also have dire consequences. After a data breach, those whose data has been affected can take legal action. This can, as already discussed, have financial consequences in terms of paying compensation and refunds, as well as any legal action taken under the DPA and CMA. Suppliers or customers can also terminate their contacts if a data breach occurs. This will have an operational impact. If suppliers refuse to allow their data, which is often business sensitive, to be stored and processed, then they may withdraw from supplying goods and/or services – terminate their contract. Customers may also terminate contracts as they do not trust the security of their data.

Reputational consequences

The damage to reputation after a data breach can also have dire consequences. The main issue will be that customers/clients may refuse to deal with a business or organisation that cannot maintain the security of their data. This decrease in customers will also have a negative effect on the brand. As data breaches have to be reported to the ICO it is highly likely that, with the increased use of websites including social media, news of the breach will travel very quickly.

Research

Three high profile businesses – Adobe, eBay and British Airways – have been victims of data breaches.

Investigate one of these data breaches for each business. For each breach, explain how the CIA triad was broken. Consider the impact on the customers of, and consequences to, these businesses.

Create a presentation showing the results of your findings. Present your findings to your group.

Test yourself

- 1 What does the I in CIA stand for?
- 2 How is the CIA security model represented graphically?
- 3 Define confidentiality.
- 4 Describe one reason why CIA should be maintained.
- 5 Identify one Act that can be used to issue fines following a data breach.

10.3 The technical and non-technical threats that may cause damage to an organisation

There are many technical and non-technical threats that can have an impact on systems, data and information. It is important that cyber security is considered by everyone who uses a digital system. This covers large multinational organisations, governments and individuals. Digital systems store and use a wide range of data and information, all of which are important and, if lost or stolen, can have far reaching impacts.

Every industry, business, organisation and individual can be the target of technical threats. Every digital system, irrespective of where and why it is used, can also suffer vulnerabilities. The technical threats will vary depending on the nature of the data and information held and the motivation of the attacker.

Technical threats

There are many technical threats that can affect systems, data and information. These include:

- botnets
- denial of service (DoS)
- distributed denial-of-service (DDoS)

- hacking
- malware
- malicious spam.

Bots/botnets

The aim of a bot/botnet is to take control of a digital system. A bot is a type of malware that allows a cyber security attacker to take control of a digital system that has been infected without the user's knowledge. It can result in a botnet which is an interconnected network of infected computer systems.

Denial-of-service

This is an attempt to make a digital or network system unavailable to its users. The result of a DoS attack is that users are unable to access the digital or network system. The attack is usually focused on, for example, email, websites and online accounts (e.g. banking). The DoS attack floods the digital system under attack with network traffic until the digital system can no longer either respond to the requests, or crashes, preventing access for users. A DoS attack uses only one digital system to carry out the attack.

Distributed denial-of-service

This is another type of attempt to make a digital or network system unavailable to its users by flooding it with network traffic. A DDoS attack has the same aim as a DoS attack, but a DDoS attack uses many digital systems to carry out the attack. A DDoS is usually focused on preventing a website or internet service from either functioning efficiently, or at all, either temporarily or indefinitely. DDoS attacks usually target websites or services hosted on high-profile web servers, such as banks, payment websites, for example, Google Pay or PayPal, and mobile phone companies.

Test yourself

- 1 What is a botnet?
- 2 What is the aim of a DoS threat?
- 3 What is the difference between a DoS and a DDoS?
- 4 What type of websites are usually targeted by a DDoS threat?

Hacking

Hacking can take many forms. These include using techniques such as:

- cross-site scripting (XSS)
- password-cracking software
- SQL injection (SQLI).

Cross site scripting

XSS is a threat to the users of, usually, a website. The threat works by a hacker inserting malicious code into a legitimate website or web-based application. This type of threat is known as a client-side code injection threat.

The threat has two steps:

- 1 Malicious code is inserted into a website or web-based application. This can only be achieved if the website requires user input on the web pages. The malicious code will then be considered part of the source code by a web browser.
- 2 A user visits the website or web pages. The visit may be as a result of malicious spam or **social engineering**.

Password-cracking software

Password-cracking software is used by hackers to steal passwords to give access to data. Password-cracking software exploits the tendency of most users to reuse passwords or have passwords that can be guessed easily. This type of software uses two different types of techniques:

- dictionary
- brute force.

A dictionary attack uses a list of predefined passwords. This can include a list of the most commonly used passwords or words from a dictionary. A brute force attack uses every combination of letters, digits and special symbols to find the password. Simple passwords will be found very quickly by a brute force attack. Longer passwords, over eight characters including upper and lower case letters, numbers and special characters, will take more time to find. This is why the minimum number of recommended characters in a password is usually eight.

Research

Research the rules that should be followed when choosing a password.

Create an infographic showing these rules.

Key term

Social engineering: the art of manipulating people so that confidential information can be found out.

SQL injection

An SQLI threat exploits a weakness in a website or a web-based application. The main purpose of this type of threat is to enable hackers to exploit software vulnerabilities in websites or web-based applications for the purpose of stealing or editing data, or to gain administrative privileges of the digital systems hosting the affected applications. An SQLI puts malicious code in SQL statements, via web page input.

An SQLI threat is one of the most predictable and easiest to protect against. Hackers are able to find websites or web-based applications that have weaknesses using web-based searches. When a website or web-based application is identified as having a weakness, then automated programs can be used to carry out the attack. The only input from the hacker is the URL of the identified target. The weakness will be exploited and the hacker will have access to the data.

The type of websites and web-based applications most at risk of threat from an SQLI are social media sites, online retailers and educational establishments.

Test yourself

- 1 Identify one type of password-cracking technique.
- 2 What does the brute force technique use to find a password?
- 3 What is the minimum number of characters that should be used in a password?
- 4 What is the main purpose of an SQLI threat?
- 5 What is the only input from a hacker in an SQLI threat?

Malware (malicious software)

This is installed on a digital system. Some malware collect information about users without their knowledge whilst other will disrupt the digital system it has infected. There are many types of malware but the main types are adware, key logger, remote access Trojan, ransomware, spyware, Trojan, virus and worm.

Table 10.1 shows different types of malware, why they are used and how they work.

Type of malware	Why it is used	How it works
Adware	Adware generates revenue for its author.	Adware is also known as advertising-supported software. This is any software package which automatically shows adverts, such as pop-ups. It may also be in the user interface of a software package or on an installation screen. Adware, by itself, is harmless; however, some adware may include spyware such as key loggers.
Key logger	Key loggers can take two forms. They can be legitimately installed to monitor users or can be installed maliciously.	Key loggers collect information and send it back to a third party. Algorithms are used to monitor keyboard use through, for example, pattern recognition. Some key loggers will only collect keyboard strokes into one website or application. Others record every keyboard stroke including any information/data that is cut and pasted.
Remote access Trojan (RAT)	RATs access and infect digital systems, usually through the internet.	RATs are typically installed without user consent and remain hidden to avoid detection, allowing a hacker to control your device remotely. When a RAT is connected to a digital system, the hacker can access and use the files and folders, login and personal details or use the connection to download viruses that could infect other digital systems.
Ransomware	Ransomware holds a digital system captive and demands a ransom, usually money, to release it.	Ransomware can restrict user access to the computer system by encrypting files or locking down the computer system. A message is usually displayed to force the user to pay so that the restrictions can be lifted and the user has access to the data/computer system. It is spread like a worm and can be started by downloading an infected file or by a vulnerability on the computer system.
Spyware	Spyware can collect data from an infected digital system, including personal information like websites visited, user logins and financial information.	Spyware is usually hidden from a user and can be difficult to detect. It is often secretly installed on a user's personal computer without their knowledge. However, some spyware such as key loggers may be installed to intentionally monitor users. Spyware can also install additional software or redirect web browsers to different websites. Some spyware can change computer settings which could lead to slow internet connection speeds or changes in web browser settings.
Trojan	A Trojan is a standalone malicious program designed to give full control of a digital system to another digital system.	Trojans often appear to be something which is wanted or needed by the user of a digital system. They can be hidden in valid programs and software. Trojans can make copies of themselves, steal information or harm their host digital system.
Virus	A virus attempts to make a digital system unreliable.	A computer program that replicates itself and spreads from computer to computer. Viruses can increase their chances of spreading to other computers by infecting files on a network file system or a file system that is accessed by other computers.
Worm	A standalone program that replicates itself so it can spread to other digital systems.	A worm can use a network to spread. Unlike a virus, it does not need to attach itself to an existing program. Worms almost always cause some harm to a network, even if only by consuming bandwidth.

▲ Table 10.1 Different types of malware, why they are used and how they work

Test yourself

- 1 What is the purpose of adware?
- 2 What does RAT stand for?
- 3 How does ransomware work?
- 4 Identify one example of how spyware can change settings on a digital system.
- 5 What does a worm do to bandwidth?

Malicious spam

Spam is junk email. But, unlike the physical junk mail that arrives through snail mail, spam can be malicious and attempt to trick users into providing details such as personal or financial information. Malicious spam can take many forms including email, phone calls and text messages.

Table 10.2 shows different types of malicious spam, why they are used and how they work. Many victims of malicious spam are people who are not tech-savvy.

Malicious spam	Why it is used	How it works
Pharming	Pharming is malicious spam that tries to redirect users from a genuine website to a fake one. This is done without the knowledge of the user.	Pharming is very similar to phishing in that both use fraudulent websites. The main difference is that a phishing attack will use fake or hoax emails while pharming attacks very rarely use this type of tactic.
Phishing	Phishing tries to get users to input, for example, their credit or debit card numbers and security details, or login details into a fake website.	Phishing uses a fake website which looks identical to the real one. The most common targets for phishing are bank, building society and insurance websites. The attackers send out emails or text message which pretend to be from, for example, your bank. A link is contained in the email which you are asked to click on. This link takes the user to a fake website.
Smishing	Smishing is a form of phishing and is the fraudulent practice of sending text messages.	Smishing is when someone tries to trick you into giving them your private information, such as passwords or credit card numbers, via a text or SMS message which pretends to be from a reputable company.
Spear phishing	Spear phishing is a form of phishing. The emails are sent to specific and well-researched targets alleging to be from someone they know and trust.	An email is sent alleging to be from a trustworthy source and redirects the user to a bogus website full of malware.
Vishing	Vishing is making phone calls or leaving voice messages pretending to be someone they know and trust.	The calls and messages pretend to be from reputable companies to try and trick people into revealing personal information, such as bank details and credit card numbers.

▲ Table 10.2 Different types of spam, why they are used and how they work

Buffer overflow

A **buffer** overflow threat is probably the most common threat to software. The threat occurs when data is being written to a buffer which overruns the buffer capacity. The data then exceeds the buffer boundary and overflows into other buffers. When this happens the data in the other buffers is corrupted or the data is overwritten. The threat can overwrite executable code with malicious code or can selectively overwrite code which can lead to the normal function of the program being changed.

Legacy programming languages, for example C and C++, are more vulnerable to a buffer overflow attack. This is because these languages have no built-in checking or protections. Languages such as Python and Java do have built-in features to minimise the possibility of a buffer overflow but do not totally reduce the possibility of this type of threat.

A buffer overflow threat can lead to a change in the program's execution path and expose data. New code can be inserted into the program code to enable unauthorised access.

Research

The WannaCry ransomware attack used the buffer overflow technique.

Investigate how the WannaCry attack began, how it spread so quickly and how it was stopped.

Discuss your findings with the rest of your teaching group.

Key term

Buffer: contains data stored in random access memory for a short amount of time before it is used.

Non-technical threats

There are also non-technical threats which can occur and have an impact on a business, organisation or individuals. These threats include:

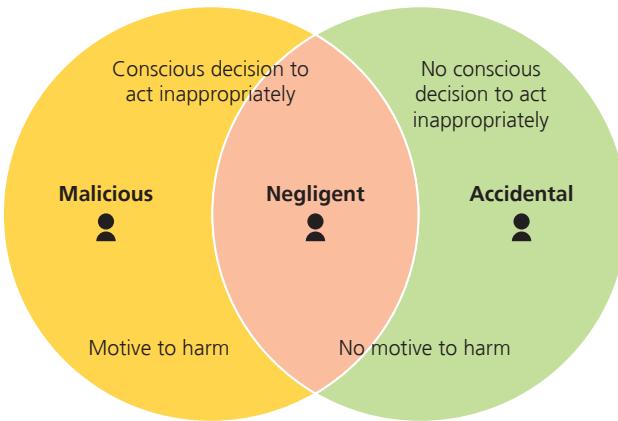
- ▶ human error
- ▶ malicious employees
- ▶ disguised criminals
- ▶ natural disasters.

Human error were the cause of approximately 90% of data breaches in 2019 according to statistics from the Information Commissioner's Office (ICO) (www.cybsafe.com).

Activity

In 2008 Facebook made public the dates of birth of 80 million users. How did this happen? What are the possible impacts of this breach on Facebook users?

Figure 10.2 shows the differences between malicious, negligent and accidental human threats to digital systems, data and information.



▲ **Figure 10.2** Malicious, negligent and accidental behaviour are all considered to be risky

Human error

Human error can lead to an accidental loss of data. This is a loss of the data itself rather than a loss of a copy or backup version of the data. For example, the loss of a hard copy of the data would not result in the loss of the source of that data if it is saved digitally.

Human error can include:

- ▶ accidentally deleting a file containing the data, or shredding the final hard copy of a data file
- ▶ saving files and folders to a different location

- ▶ sending emails to the wrong recipients with attachments containing data
- ▶ accidentally making changes in documents.

While every person is capable of making an error, businesses and organisations should attempt to minimise the likelihood of these errors happening. This may be through the use of regular employee training, high-profile reminders to employees, for example on splash screens on digital devices, and ensuring that all policies and procedures are read and understood by all employees.

Malicious employees

Malicious employees can be another threat to digital systems, data and information. Malicious employees are also known as turncloaks. They typically use their access details in a malicious and deliberate way to steal information and data for financial or personal reasons. An individual may become a turncloak as a result of a social engineering attack.

While many employees take no further action if they are disciplined or sacked, a turncloak employee may hold a grudge against their employer. This type of threat is often difficult to trace as they are familiar with the security procedures of the business as well as any vulnerabilities.

Disguised criminals

Disguised criminals use social engineering techniques to gain access to buildings. There are two main types of social engineering that can be used to achieve this. These are:

- ▶ tailgating/piggybacking
- ▶ shoulder surfing.

Tailgating/piggybacking is used to try to gain access to a secure building or room. This type of attacker takes the form of someone who does not have authority to enter a building or room, following someone who does through the doors. The most common type is that the attacker pretends to be a delivery driver and asks an authorised person to hold the door.

Shoulder surfing aims to steal data and information. This happens when someone's private and confidential information is seen. For example, when using this method the attacker may stand very close to someone using a cash machine to see their PIN. This method is very effective in crowded places when a person uses a smartphone or mobile device and log-in details can be seen. This method can also be used to find out access codes which will then allow the disguised criminal to access buildings and rooms.

Research

In 2015 a US health insurance company, Anthem, suffered a data breach. Social engineering was thought to have provided the access codes to the customer database.

Identify the different types of social engineering and describe how each type could have been used to gather the required access codes.

Natural disasters

With the increase in the use of digital devices and the cloud, there are external threats, also known as environmental or natural disasters, that can affect data, information and digital systems.

If a natural disaster occurs, for example an earthquake, then it is probable that internet access could be lost. This could mean that any data and information stored in the cloud could be inaccessible. The impact of inaccessible data and information could affect the recovery from a natural disaster.

It would also be possible that digital devices could be destroyed during a natural disaster. If a tsunami or flood happened, the water coming onto the land could destroy or wash away buildings. If digital devices were in these buildings, then they would be destroyed or lost. The cabling infrastructure or any internet service equipment could also be affected. Even if buildings could be made safe, the tremors that can happen with a natural disaster, such as an earthquake, could damage any hard drive surfaces causing the data and information stored on them to be unreadable.

Even if physical backups were available, there is a probability that these would also be affected by the same natural disaster. If the backups were stored in the cloud, then these may also be inaccessible as there may be no internet access.

Power failure is one of the potential after-effects of a natural disaster. As digital systems need electricity to either charge or operate, this will also mean very limited accessibility of data and information, and the digital devices these are stored on. One method that can be used to keep digital systems operating is to use batteries or a power generator as backup power sources. However, the batteries must be kept fully charged and fuel must be available to run the generator.

Lightning strikes are another natural disaster that can affect computer systems and devices. A lightning strike can cause a surge or spike in the electricity supply. These surges can affect how hard drives and other storage devices operate.

Research

Investigate the different devices that can be used to protect against power surges. Identify where each device could be used.

Test yourself

- 1 What is a turncloak?
- 2 What are the two steps involved in cross site scripting (XSS)?
- 3 Why is phishing used?
- 4 Which type of programming language is most at risk from buffer overload?
- 5 Identify two types of natural disaster (environmental) threat.

10.4 The technical and non-technical vulnerabilities that exist within an organisation

Technical and non-technical vulnerabilities can increase the chances of a threat occurring to an organisation.

You will learn about the ways to mitigate against these vulnerabilities in section 10.6, p. 249.

Technical vulnerabilities

Weak or outdated encryption

There are two different types of encryption and a stronger method of encrypting data called hashing. What is important is that, whether encryption or hashing is used to secure data, the software used is updated to the latest versions as released by the vendor. Checking for updates to encryption software should form part of scheduled, routine maintenance tasks.

Out-of-date software, hardware and firmware

All the components of a digital system will, eventually, become out of date. Vendors and manufacturers will

Key term

Firmware: code, added at the time of manufacturing, written to a hardware device's non-volatile memory. It is the software that allows the hardware to run.

release patches for updates to software and **firmware** but eventually these components will need to be updated. This may also be as a result of incompatibility between newer software programs and hardware or because, in the case of hardware, general failure to operate as intended. Again, checking for out-of-date software, hardware and firmware should form part of routine maintenance tasks.

Software no longer supported by vendor/supplier

Eventually a software vendor will issue an end of life (EoL) notice to all those who use the software. For example, Microsoft ended support for Office 2010 in October 2020.

Compatibility of legacy systems

As new hardware and software is purchased, there is a probability that it will not be compatible with the existing, legacy, hardware and software. This can cause issues. For example, with software, data and information stored on legacy systems, software and data may have to be converted to be used on the new software. This can sometimes lead to data becoming corrupted or not being in a useful format. This is called forward compatibility. If data is entered and processed on new software but is then exported to legacy software this, again, can lead to data being corrupted or unable to be exported. This is called backward compatibility. This lack of compatibility can also occur in hardware. For example, if new printers have been purchased, it may be difficult, or not possible, to make them communicate with the network workstations or other digital systems that need to use them.

You will learn more about EoL and compatibility of legacy systems in the section 10.6, p. 259.

Fail-open electronic locks

This type of software lock will keep the software, and the system, open if an error is detected. This means that traffic and processes still flow into the system.

This type of lock is used when access to the system is perceived to be more important than authenticating the traffic. This can cause a vulnerability because there is an increased probability that an attack can happen.

Weak passwords

Many software applications and networked components have default passwords. These are usually 0000 or 1234. It is easy for users to simply carry on using these default passwords but they are known to attackers and so can be breached very quickly by password-cracking software. If a password is changed, as required by an IT policy, then users tend to use their name, a pet or family member's name, or a sequence of numbers. These are weak passwords. Users also have a tendency to reuse passwords across a range of applications, for example email or network login. This means that when one password has been cracked it will be very easy for an attacker to gain access to other applications and the data they store. Users of a digital system should be encouraged to use strong passwords or passphrases.

You learned about password-cracking software in section 10.3, p. 242.

You will learn about passphrases in section 10.6, p. 255.

Missing authentication and authorisation

If users do not have to be authenticated or authorised to use a digital system, then the system is very vulnerable to attacks. By having no authentication or authorisation, any user can gain access to the digital system and the data stored on it. It is, therefore, very important that this vulnerability is closed with all users having credentials that authenticate and authorise them to be able to use the digital system.

Exploitable bugs/zero-day bugs

This type of bug refers to a software or hardware vulnerability which has just been discovered. As the bug has only just been discovered it means that a patch has not yet been released to close the vulnerability. So, the term zero-day means that the vendor has zero days to fix the vulnerability. A race between the attackers, who may already be aware of the vulnerability and could already be exploiting it, and the vendor, who needs to release a patch, begins.

Non-technical vulnerabilities

Employees

As already discussed, people are the weakest link in any security procedure or process.

All businesses and organisations will have policies and procedures which must be followed to maintain a high level of security. It is important that employees read, understand and act on the policies and procedures.

Training and continuing professional development should be carried out on a regular basis to maintain awareness of the contents of the security policies and procedures and to increase the competency of staff. If staff are not competent then they may be unable to follow the contents of policies and procedures because they do not have the necessary skills. When staff are being recruited, questions about the skills and competencies of the applicant may need to be included on the application document. This information could be verified through the use of practical assessments prior to an offer of employment. This is called recruitment screening.

Poor data/cyber hygiene

It is important that the data and information stored continue to be useful and up to date. This is also one of the requirements of the Data Protection Act. A vulnerability could occur if an employee has left, but their account and log-in credentials are still 'live'. This means if the employee was disgruntled about the termination of their employment, they could still access the digital systems and the stored data. Ex-employees who hold a grudge are also susceptible to social engineering attacks. To close this vulnerability, data about clients, customers and suppliers should be reviewed and cleaned on a regular basis but data related to employees who have left should be archived as soon as they leave employment.

Malicious employees and turncloaks are covered in section 10.3, p. 245.

The Data Protection Act is covered in section 8.1, p. 202

User access, policies and procedures, and user access restrictions, are covered in section 10.6, p. 253.

Physical access controls

While it is important that data is kept secure with authenticated and authorised users having access, the physical environment should also be protected. While physical access controls can be implemented, it is how they are used that could cause the vulnerabilities.

Many physical environments have door access codes which must be input before access to the room is granted. Like many other security procedures, these codes should be regularly changed, with only staff who need access to those rooms being provided with the updated codes.

It is not good practice to reuse access codes. The practice of using the same code for multiple doors and using weak, or easily guessed, codes, for example 1234, can also cause a vulnerability. For example, if an intruder manages to crack one access code, then they will have access to all other areas with that code. This will increase the potential damage that could be caused.

Limiting knowledge of access codes can ensure that only staff who need access to secure areas, for example server rooms, can gain access. It can, however, be difficult to monitor who has access to areas if simple key code locks are used. Access codes could be shared by staff which would lead to an increase in people who know the codes.

Security procedures should be put in place and reviewed at regular intervals. If security procedures are not adequate enough or are outdated, then the chance of an attack on the physical environment will increase.

Test yourself

- 1 What is backward compatibility?
- 2 Give an example of a weak password.
- 3 What is a fail-open software lock?
- 4 Why should users be authenticated and authorised?
- 5 What is a zero-day bug?

10.5 The potential impacts of threats and vulnerabilities on an organisation

Threats and vulnerabilities can have an impact on an organisation. Many of these impacts have already been covered in this core element when the threats and vulnerabilities have been described.

As a recap, the most common potential impacts are:

- loss of sensitive information
- unauthorised access to the system or service
- overload of the system to affect a service
- corruption of a system or data
- damage to system operations
- disclosure of private information and credentials

- ▶ unauthorised access to restricted physical environment
- ▶ essential security updates not installed.

10.6 Risk mitigation controls to prevent threats to digital systems

Digital systems and the data and information stored on them are very valuable assets, not only to the businesses and organisations that collect, store, process and use them, but also to each individual.

Data and information such as customer shopping records, financial data, and health data and information, are used for a variety of purposes. What is important is that all data and information are kept secure and protected from the large range of threats that could occur.

Activity

Find and watch the video called 'What is penetration testing' at www.cisco.com.

What are the main points related to the importance of cyber security raised in the video?

Make notes about your findings.

National Cyber Security Centre Cyber Essentials

The UK-based National Cyber Security Centre (NCSC) has developed guidance for businesses, organisations and individuals about cyber security. Cyber Essentials is a UK Government-backed scheme to help people learn about how to protect themselves against an attack.

Some of the guidance relates to:

- ▶ using a firewall to secure an internet connection
- ▶ selecting, and using, the most secure settings for hardware devices and software
- ▶ how to protect against viruses and malware
- ▶ how to control access to software and hardware devices
- ▶ how to keep hardware devices and software up to date.

Activity

Find the NCSC website. Investigate the guidelines and advice provided.

Select one area and create a digital communication to provide these details to the owner of a business.

Anti-virus and anti-malware

Anti-virus and anti-malware programs are security software designed to prevent, detect and remove viruses and other malware, including adware, Trojans and worms. It is essential that any digital system connected to the internet has some form of security protection. If security software is not installed then it is possible that within minutes of connection to the internet the system will be infected.

Security software performs several tasks including:

- ▶ scanning files or directories for any viruses, malware or known malicious patterns
- ▶ automatic real-time scanning
- ▶ performing a manual scan of a digital device
- ▶ removing any malicious code detected – sometimes you will be notified of an infection and asked if you want to clean the file; other programs will automatically do this behind the scenes
- ▶ blocking unsafe websites or alerting a user about infected emails.

When security software finds a malicious program on a digital system, the user is usually offered two options:

- ▶ to quarantine it so the software cannot infect the digital system – this option gives the vendor the opportunity to analyse the program so that they can offer an update to users
- ▶ to delete it – this option clears the digital system of the infection.

Automatic versus manual updates

Some security and application software updates automatically. This process is usually completed in real time. This means that when the computer system is connected to the internet the software will automatically be checking all the time for new updates. If an update is found, then the security software will automatically update it. This happens because new viruses and other security threats are being released all the time. These updates are known as **patches**.

Key term

Patch: software code that can be downloaded and installed, after the software program is originally installed, to correct an issue with that program.

This means that the user does not have to remember to manually check for updates and so the digital system is always protected from any threats.

If a business uses automatic updates of software then they do not have to remember to manually check for updates and can be sure that their digital system is as up to date as possible. This also means that any vulnerabilities identified by the vendor are solved before an attack can take place.

Manually updating security software can be dangerous to the digital system and the data and information held on it. Employees can forget to carry out manual updates and this can leave the digital system vulnerable to threats.

A manual update for security software could be completed on an ad hoc basis or can be set to check at a specified time (scheduled) by a user.

One of the problems with manual updating of security software is the time it can take to download the patch. There may also be a time delay between the patch being released by the software vendor and the time when the manual update takes place.

Another problem with manually scheduling an update is that the digital system must be switched on and connected to the internet for the update to be downloaded. If the manual update has been scheduled for a time when the business system is switched off, then the business will never get updates or download patches. This can leave the digital system open to attacks and threats and could result in data being lost or stolen.

Some users, however, may prefer to update their software manually because they want to look at the updates to decide whether or not to download them. Some users may consider the updates to be intrusive or not appropriate.

Activity

Choose any two of the different providers of anti-virus software – look on the internet to see the different providers available.

Copy and complete this table to show the features which are available (two features have been given for you). You may need to add more rows to the table.

Feature	Provider 1	Provider 2
Internet links scanner		
Live support		

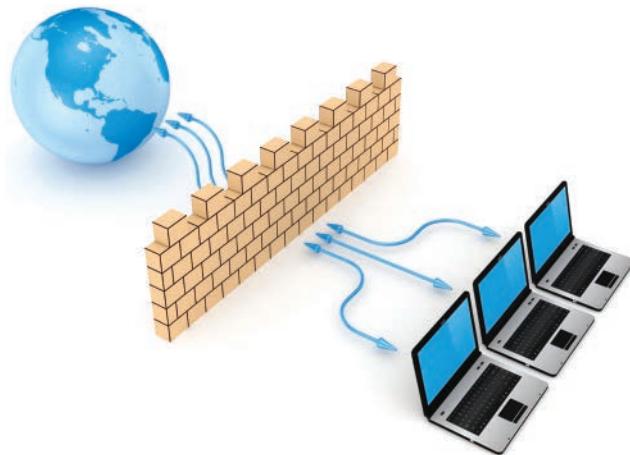
Test yourself

- Identify two tasks carried out by security software.
- Manual updating can be carried out. Identify the other method of updating.
- Describe one disadvantage of manual updating.

Firewalls

A firewall is a security device that mitigates against threats by examining **data packets**. A firewall can be either hardware or software or both, but hardware and software firewalls work in the same way.

The purpose of a firewall is to establish a barrier between a digital device and/or a network and incoming traffic from external sources (such as the internet). Firewalls monitor the traffic that flows into a digital device and/or a network through an internet connection. The firewall blocks malicious traffic, like viruses and hackers, based on security rules.



▲ Figure 10.3 A firewall acts as a barrier against threats to a system's security

There are two formats of firewall:

- A **software** firewall is a program that monitors traffic through port numbers and applications.
- A **physical** firewall is a piece of hardware installed between the network and the gateway.

Key term

Data packets: small units of data which are sent and received when accessing the internet or any other type of network.

It is advisable to use both software and hardware firewalls in tandem, in order to increase their efficiency. Both monitor incoming traffic and analyse it against set security rules. Any traffic that breaks those rules is blocked.

Firewalls monitor the traffic at the entry point – called ports. This is because ports are where the information is exchanged with the external devices.

There are three main types of firewalls:

- **Packet filtering firewalls** mitigate against threats by analysing the data packets and block any packets that do not meet the predefined security rules.
- **Proxy firewalls** mitigate against threats by taking on the role of the intended recipient. They monitor traffic at the application level. Proxy firewalls monitor traffic for seven-layer protocols, including HTTP and FTP.
- **Inspection firewalls** mitigate against threats by marking the key features of any outgoing requests for information, checking for the same key features in the data coming into the system and deciding if the incoming traffic is relevant.

Activity

Research NGFW, NAT and SMLI firewalls.

Create a digital communication aimed at 17 to 18 years olds to explain how each of the firewalls works.

Test yourself

- 1 What is the purpose of a firewall?
- 2 What is the purpose of a port?
- 3 How do packet filtering firewalls work?
- 4 Packet filtering is one type of firewall. Identify two other types.
- 5 What is a data packet?

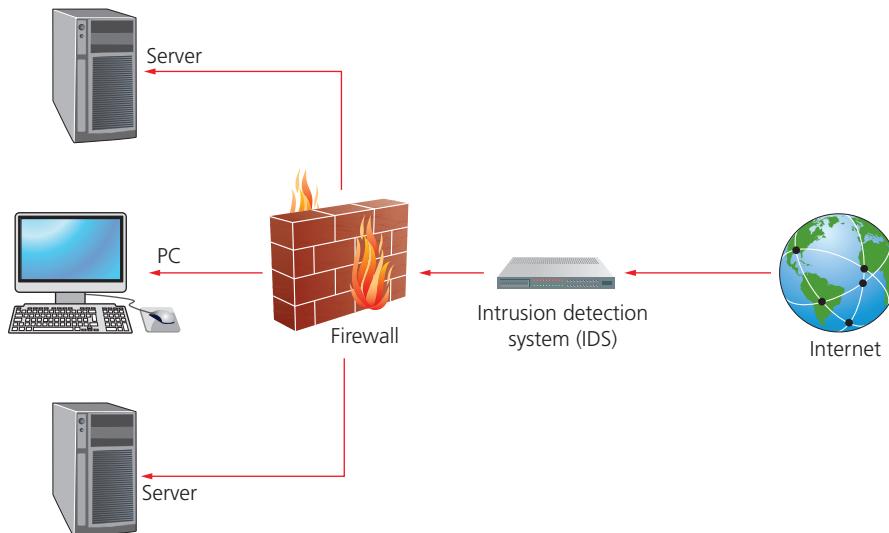
Intrusion detection and prevention systems

Intrusion detection systems (IDS) are designed to expose any attempts by attackers to overcome security controls to compromise data or other resources. There are different types of IDS including:

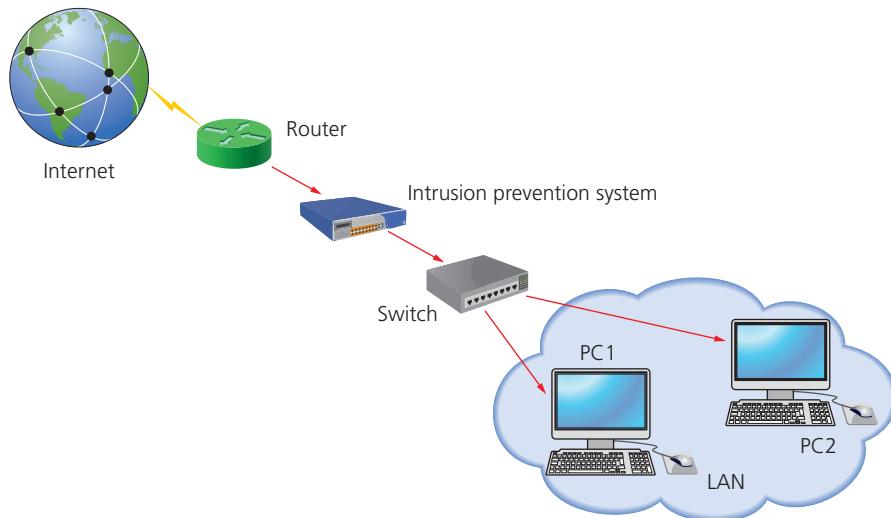
- **network based (NIDS)** which monitor traffic on a network by intercepting network packets, processing the data and identifying suspicious traffic
- **host based (HIDS)** which detect unusual, unauthorised or illegal activities on a specific device.

All IDS collect and log suspected intrusions and alert the designated people.

Intrusion prevention systems (IPSs) are devices or programs that detect attempts at intrusion and take action to prevent them. An IPS can be a hardware device or software running on servers or virtual environments. Unlike an IDS the IPS is connected just like any other part of the system and all traffic flows



▲ Figure 10.4 Intrusion detection system



▲ Figure 10.5 Intrusion prevention system

through it. It creates alerts and logs events, but most importantly it can block attacks. As with an IDS, an IPS can be network or host based.

Encryption

As has already been discussed, the most valuable assets to a business, organisation or individuals are data and information.

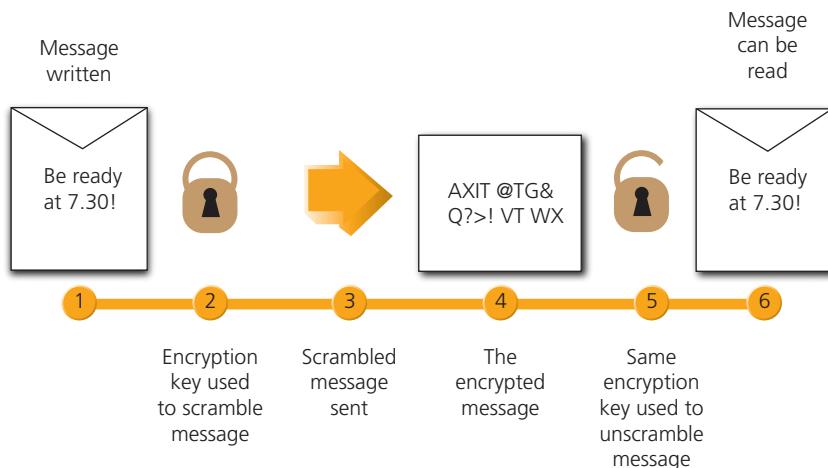
Encryption can help to prevent data being accessed and used by unauthorised people (attackers). Data can be scrambled using encryption software when it is stored or transmitted between digital devices over networks.

Data encryption software uses an **encryption code or key** to scramble (encrypt) the contents of data files.

The proper code is needed to unscramble the file (decrypt it) so it can be read and used. If the encrypted file is accessed by anyone without the proper code to unscramble it, the data is meaningless.

Data can be encrypted at rest and/or in transit. It is common practice, especially where the data is sensitive, for example financial or personal data, to encrypt the **data at rest**. This can help to mitigate the loss of the data against an attack.

It is also good practice to encrypt the **data in transit**. By doing this the encryption can mitigate against the loss of the data while it is being transmitted by, for example, email or being uploaded to a cloud storage area.



▲ Figure 10.6 Using an encryption key to encrypt and decrypt a message

Key terms

Data encryption software: software that is used to encrypt a file or data.

Encryption code/key: a set of characters, a phrase or numbers that are used when encrypting or decrypting data or a file.

Data at rest: data stored on a digital device or storage medium.

Data in transit: data being sent to one or more authorised users.

Hash: a number generated from a string of text.

Asymmetric and symmetric encryption

There are two main types of encryption: asymmetric and symmetric.

Asymmetric encryption is also known as public key encryption. This is when the encryption key is available to anyone to use and encrypt data but only the person who receives the data receives the decryption key.

Figure 10.6 shows the process of **symmetric encryption**. This is when the encryption and decryption keys are the same.

Encryption can also be used on websites. When customers buy goods online, book cinema tickets online or enter personal details into any website, the data should be encrypted before being transmitted. This will keep the details from being read or used by others even if they are intercepted. Everyone should check that the website they are using to enter personal details uses encryption.

A secure website using encryption will use https instead of http in the URL and will show a small padlock. Different web browsers will show the use of https in different ways.

Figure 10.7 shows a web address beginning with https and also shows the padlock to confirm that the website uses encryption.



▲ Figure 10.7 A website using encryption

Encryption is, as already discussed, a two-way process: what is encrypted can be decrypted with the proper key. So, this means that encryption is reversible.

Another method of encrypting data is to use hashing. There is a difference between encryption and hashing.

Hashing

Hashing uses an algorithm to map, or scramble, data of any size to a fixed length. This is called a hash value. Hashing verifies that a file or piece of data is authentic and has not been altered.

Hashing can be particularly useful for storing passwords. Hashing can also be used for searching, for example to find specific data in a very large database, or for cryptographic applications in digital certificates.

Unlike encryption, hashing is only one way and is not reversible. However, technically it is possible to reverse **hash**, but this would take vast amounts of processing power and so it is generally considered to be unfeasible.

Research

There are many different types of hashing algorithms. Investigate the different types and how they work.

In your group, discuss your findings and try to make a decision as to which one is best.

Test yourself

- 1 What is the difference between IDS and IPS?
- 2 What is the purpose of a NIDS?
- 3 What is asymmetric encryption?
- 4 How do websites show they are encrypted?
- 5 What does hashing demonstrate?
- 6 Identify two uses of hashing.

User access, policies and procedures

It is important that any access and permission procedures are communicated to employees. These are usually contained in IT policies. The employees should read these policies and any updates. It may be that new employees are asked to read the policies during their induction and asked to sign a document to confirm they have read, understood and agree to abide by these policies.

Research

Investigate the IT policies that are in place at your centre or workplace. Identify the key points and any omissions.

Discuss your findings with the rest of your teaching group.

Software-based user access controls aim to mitigate against threats by predefining access by authorised employees, that is which areas of the building each employee can and cannot go into. Most workplaces will need to implement a networked access control system.

This type of system is used where control is required at a central point, for example the reception area. The system will enable access control for employees through a number of doors. Each employee can be provided with a specific access control so that they are able to gain access to the areas that are needed for them to perform their job functions. This control will restrict access to other areas that they do not need access to. Having an access control system can go some way to avoid the threat of unauthorised access which could lead to theft, malicious damage and threats to personal safety.

The most up-to-date control systems will enable reports to be run to, for example, identify which employees have used a door. These systems can also be integrated with other security controls such as closed-circuit television (CCTV) and alarms.

Employees can gain access through doors by inputting a unique token which can be:

- ▶ a numeric code/PIN input using a keypad
- ▶ an access badge using **radio frequency identification (RFID)**
- ▶ possession-based authentication.

Key term

Radio frequency identification (RFID): tiny chips that contain information which is transmitted when near a receiver.

Door access control instructions are completed centrally using a digital device and are then sent to each of the doors.

A unique token can be stopped from having access to all doors instantly. This could be very helpful if an employee is sacked. A network access control

system should enable different access permissions for employees and, possibly, at different times of the day.

For example, only those employees who need access to the HR department will be granted the unique token to access this department during working hours. Night security employees might be able to access all doors between specified areas.

Flexible control allows for different access permissions to be granted for individuals or groups of users and at specified times of the day.

As stated, some access control systems will log which employees have accessed which doors. This could be very valuable in the case of a fire leading to an evacuation of the workplace. The log will enable employers to find out quickly if any employees have not left the building. This information can be given to the Fire Service who can then enter the building to find the missing employee(s) and save lives.

User access restrictions

User access restrictions can be used to mitigate against threats by limiting access to data and information, and physical rooms, based on job roles. There are many different types of user access restrictions that can be used. These include:

- ▶ logical
 - usernames
 - passwords and passphrases
 - data access levels and permissions
- ▶ physical
 - physical access control and restrictions.

Usernames

Usernames are part of the log-in credentials provided to employees by their employers. The username, when linked with a correct password or passphrase, is used to provide access to digital systems, data and information. Usernames can also be known as a log-in ID or user ID. Usernames are unique within a workplace. If two users had the same username then this could cause issues when setting access rights and permissions.

Usernames allow lots of users to use the same digital system. The username will enable a user's personal settings and files to be shown.

Passwords and passphrase

Passwords and passphrases are linked with usernames and complete the log-in credentials. The

log-in credentials provide protection on two levels. In a workplace the username allows access/gives permission for the user to access specific software such as financial or HR.

The password, or passphrase, can allow the user **access rights** and **permissions** to the digital system and software such as internet and email access, and standard office applications.

If the data is extremely sensitive then further passwords, or passphrases, may be needed.

It is also good practice for external storage devices, files and folders to be password protected. This is only effective if the password is strong and not easily guessed.

Activity

Many businesses and organisations have rules about passwords in their security policies. Create a digital communication for new employees to show the rules that should be followed when creating a password.

Passphrases

Passphrases are very similar to passwords but are usually a string of words – a phrase. An example of a passphrase could be ‘BrightFunCamp’. There are some advantages to using a passphrase rather than a password.

Passphrases are:

- ▶ usually longer than a password, meaning they are more difficult to be guessed by an attacker (most password-cracking software used by attackers has a limit on the number of characters they can be used on)
- ▶ random words rather than a standard well-known phrase
- ▶ more memorable to the user because a passphrase can be easily remembered, so limiting the number of ‘forgotten passphrase’ requests by users.

Key terms

Access rights: control over what a user has access to in a digital system, for example folders, files and data/information.

Permissions: a list of attributes that determine what a user can do with files and folders, for example read, write, edit or delete.

As with passwords, it is good practice not to use the same passphrase over multiple logins.

Data access levels/permissions

Log-in credentials can be used, as already discussed, to provide access levels and permissions. Digital systems, software, files and folders can have access rights and permissions set. This means that only those users who have the correct log-in credentials can have access.

The access rights can inform what a user can do with a file and folder. These are called permissions. A user can have permission to read, write, edit or delete data and information.

You have already learned that data is the most valuable asset of any business or organisation. It is important that data is protected against any unauthorised access or editing. Permissions can be set to limit what a user can do with data. Permissions are also known as **privileges**.

In addition, rules can be set. These rules can be part of the permissions and privileges to attempt to increase the data security. Examples of rules that can be set include access to all files, and access to specific files and folders. In an organisation these rules are likely to be based on the job role.

Examples of rules that can be set include access to all files, and access to specific files and folders. In an organisation these rules are likely to be based on the job role.

If the use of data is not kept secure and access rules set, there is a possibility that data can be leaked or edited. The impacts of the loss or unauthorised editing of data can include:

- ▶ data bias
- ▶ inaccurate data leading to incorrect processing and analysis, and uninformed decision being made
- ▶ a data breach/leak leading to possible financial and/or reputational impact.

Physical access control/restrictions

There are many different types of physical access control/restrictions. The ones that are implemented will depend on the function of the business or organisation and the physical workplaces.

There are many different types of access controls that can be implemented including:

- ▶ access badges
- ▶ alarm systems
- ▶ barriers
- ▶ external security lights
- ▶ CCTV
- ▶ door sensors
- ▶ locks and keypads.

The physical security measures used will depend on the physical layout of the workplace. If attackers gain access to a workplace then they could steal physical digital devices and could also infect digital systems with malware. How successful this would be will depend on the logical security measures that have been implemented.

Alarm systems

These can be installed to alert people to an unlawful attempt to access the workplace. Different types of alarm systems can be used including motion sensors and glass break detection. Alarms can either be silent or have an audio signal that the alarm has been tripped.

However, an alarm is only fully effective if there is a quick response to the alarm as this will increase the chance of catching the attackers.

Barriers

Barriers can be used to control access to any car parks or distribution areas in a workplace. They can be controlled manually. Barriers can be used to limit access until a code or verbal authorisation has been given. If authorisation is provided, then the barrier is lifted and access is granted.

External security lights

These are a relatively inexpensive and quick method of increasing security effectively. Lighting is often a deterrent for attackers as the mere threat of potentially being seen is more than enough to stop them attempting to gain access to a workplace. If the external security lights are automatic/motion sensing, they will turn on automatically if any motion within the range of the lights is detected.

CCTV

CCTV can be a very strong deterrent against any unlawful activity. As with external security lighting,

CCTV is quick to install and can be inexpensive. CCTV cameras can provide video footage of criminal activity but, as with security lights, just the sight of them can be a deterrent to attackers. Signs stating that CCTV is being used must also be installed.

Research

Research the physical protection methods of access badges, door sensors, and locks and keypads.

Discuss your findings with the rest of your group.

Activity

Carry out a physical security analysis of your centre or workplace. Create a digital communication detailing any potentially insecure areas and recommending how the physical security could be improved. The digital communication should be aimed at a senior management team.

Test yourself

- 1 Identify two types of physical security methods.
- 2 What is the main disadvantage of alarm systems?
- 3 How can barriers limit access to a workplace?
- 4 What has to be in place if CCTV is installed?
- 5 How do automatic security lights work?

Multi-factor authentication

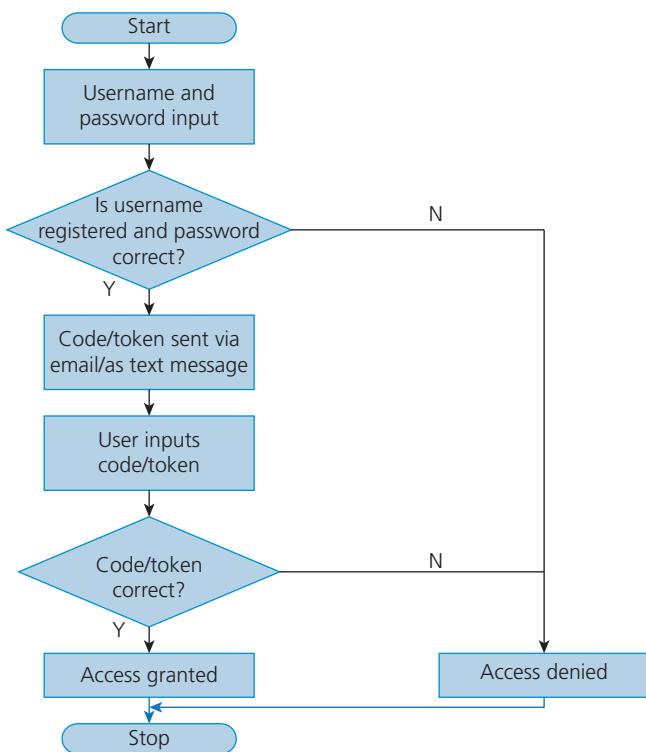
It is also possible to implement multi-factor authentication to increase security and mitigate against threats. Multi-factor authentication can take many forms including:

- ▶ possession-based
- ▶ biometric
- ▶ knowledge
- ▶ location-based.

Multi-factor authentication is also known as two factor authentication (2FA) or three factor authentication (3FA).

Possession-based

Possession-based multi-factor authentication is also known as token authentication. This method is based on a possession that a user typically has with them at all times, for example a mobile phone.



▲ Figure 10.8 Two-step authentication

Figure 10.8 shows the process used during possession-based multi-factor authentication. When a user needs to enter a secure area of a digital system, the log-in credentials are input. When the log-in credentials have been submitted, they are checked by the digital system. A token code, usually numeric, is sent to either the email address or by text to the mobile phone number that are linked to the log-in credentials. The email address and mobile phone number will be stored on the digital system. The user receives the token code and, to access the secure area, inputs this code.

Log-in credentials are covered earlier in this section.

Biometric

Biometric multi-factor authentication uses a person's physical characteristics, for example a fingerprint, retina scan or voice.

It is common for laptops, smartphones and tablets to need a biometric measure to be positive before these devices can be accessed. The owner of these devices will have stored their characteristic as part of the security settings on these devices. When, for example, the fingerprint is used to access the device, it is checked against the stored fingerprint characteristics and if there is a match then access is granted. This

means that only people whose characteristic is stored and recognised can access the device. If anyone else tries to access the device, the characteristic will not be recognised and so access will be denied.

Large businesses can use biometric protection measures to protect, for example, server rooms. When someone tries to access this room, they will scan their characteristic, for example their fingerprint. This is then checked against the database of authorised personnel fingerprints and, if there is a match, then access will be granted. This means that access to areas or rooms of a workplace can be limited.

There are some disadvantages to using biometric protection measures. For example, a person's voice can change if they have a cold. This can cause problems if the device they are trying to access does not recognise the voice pattern. People can have an injury to their fingers, for example a burn or cut. If the injury is severe, this can change the pattern of the fingerprint and may result in access being denied. Another example may be if someone has been swimming and their fingers get wet and wrinkly. This will change the pattern of the fingerprint and will result in the scanner not recognising the fingerprint.

Knowledge

Knowledge multi-factor authentication (KBA) authenticates a user by using questions and answers which have already been agreed. KBA relies on the user having to prove their identity by sharing information about themselves through answers to questions. The most commonly used KBA in the UK is static.

Static KBA is commonly known as secret questions. If, for example, a user forgets their password or passphrase of their log-in credentials, then the secret question can be used to verify the identity of the user. Answers to secret questions are usually provided when an account is set up – often the user can select the security question from a list of options. The answer to the security question is linked to the log-in credentials and stored in a file with a high level of security.

Activity

Create a list of secret questions that could be offered to users of a cloud storage area.

Discuss your questions with the rest of your group.

Location-based

Location-based multi-factor authentication authenticates a user through their physical location. If a user wants to log into a digital device which is wired into a network, then a specific PIN could be used.

This is because, as the device is wired into a network, the location of the user can be verified. Another factor could be that access to the workplace is controlled by physical security such as access badges.

If, however, a user wants to use the network remotely, then log-in credentials and a token code would be required.

Another method of location multi-factor authentication is that of verifying a user's location via Internet Protocol addresses. For example, many web-based services use geolocation security checks.

When an account is set up, an address is usually required. The address will include the county and country. If an attacker attempts to log into the account from a different location, then the registered account holder will be notified.

Test yourself

- 1 What does the abbreviation 2FA mean?
- 2 How can a token code be sent using possession-based authentication?
- 3 What would be required if a user was logging into a network using a wired connection?
- 4 Identify two features that could be used for biometric authentication.
- 5 What is meant by static KBA?

Staff training and continuous professional development

It is important that staff (employees) are kept up to date with methods used to mitigate against threats. Training should be carried out on a regular basis and should form part of the continuous professional development (CPD) offered to employees.

Research

Investigate the CPD that is carried out in your centre or workplace relating to security.

Discuss your findings with the rest of your teaching group.

As staff are trained, they will become more aware of threats and will form part of the human firewall for their employer. It is generally agreed that people are the weakest link in any security.

A human firewall is based on staff understanding digital security and becoming alert to any threats or suspicious activity.

Activity

Investigate how a human firewall can be implemented.

Create a digital communication to advise employers how staff can become a human firewall.

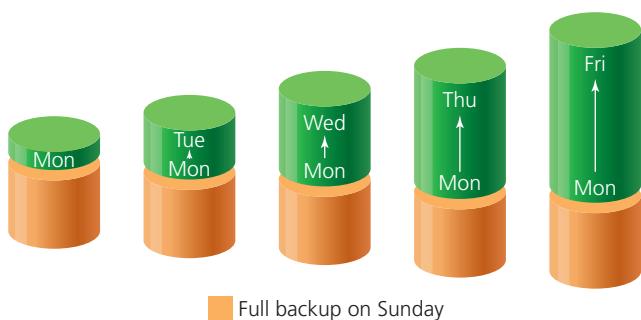
Backups

Backing up data does not protect the data from attack but mitigates the effect as a copy is available. However, backups only provide data from the time the backup was taken. Any data that has been edited after the backup was taken will be lost. Every business or organisation that stores data should have a backup policy based on the need to protect vital data and information. The policy should also define the type of backup and when the backup should take place.

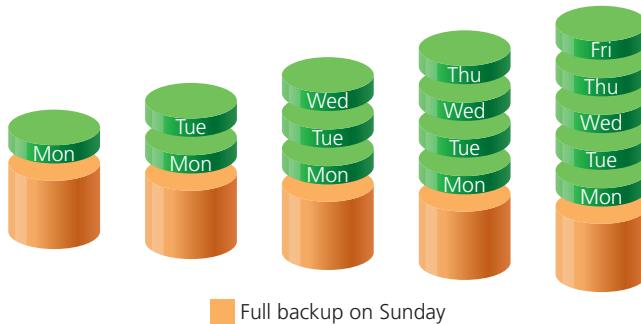
There are three main types of backup:

- **Full** – every single file and folder in the system is backed up. This type of backup takes the longest and needs the most storage space. But, restoring lost data from this type of backup is the quickest.
- **Incremental** – the first backup in this process is a full one. Any backup after the first one only stores edits made to the data that have occurred since the previous backup. The process is quick as the amount of data being backed up is smaller but restoring the data takes longer.
- **Differential** – this is very similar to the incremental backup. With both, the first backup is full. With differential backups, every backup after that stores all changes made since the full backup. This needs more storage space than an incremental backup, but the restore time is faster.

Figures 10.9 and 10.10 show the difference between a differential and an incremental backup over a week.



▲ Figure 10.9 Differential backup



▲ Figure 10.10 Incremental backup

Research

Adobe issued an end of life notice for Adobe Flash Player and stopped supporting it in January 2021.

Research the impact that running an unsupported Flash Player may have on a business's digital system.

This may also cause a problem with legacy software. For example, over the life of a database program, the vendor will issue updates to ensure the database software will still perform as required. However, over time the database will need to interact with more up-to-date software. This is when the database becomes a legacy system. At this point a decision has to be made about replacing the database with an up-to-date version which will interact with newer software. However, this decision has an impact on the business. For example, will the stored data be transferred to the new database with a guarantee of no loss of data?

Hardware can also become obsolete and will need replacing. This may be linked with the firmware being run on the hardware components or may be as a result of a reduction in performance. It is very common to have updates to firmware issued for devices and components, for example mice and printers, but there comes a time, as with software, when manufacturers and vendors will stop supporting any given device or component.

Updating using patches is part of the scheduled maintenance that should be carried out on any digital system. Maintenance should be routinely carried out to, for example, archive or delete any files and folders which are not currently required. Another maintenance task could be to, for example, scan hard drives with a disk defragmenter to free up continuous memory space.

While it is important that maintenance is carried out, the timing of the routine maintenance must be considered to minimise disruption to users. For example, routine maintenance should not be scheduled during working hours as this would mean any users of the system may be unable to carry out their job roles.

What should be remembered is that it is not possible to schedule any emergency maintenance, for example, network servers crashing. The time taken to carry out any emergency maintenance should be limited with users kept up to date with the expected time when systems will be reinstated.

Test yourself

- 1 What is the weakest link in security?
- 2 What is the human firewall based on?
- 3 Why should data be backed up?
- 4 What is a full backup?
- 5 What is one benefit of using an incremental backup?

Software and system maintenance

Over time, digital devices and software will need to be maintained to ensure they run at optimal performance.

Earlier in this core element you learned about the importance of software updates and how these should and can be downloaded and installed. This can also be applied to the hardware of a digital system.

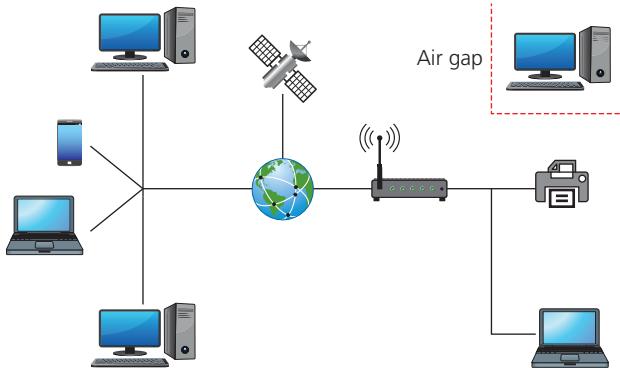
When a digital system is installed, it can be assumed that the hardware and installed software is up to date and can, therefore, be classed as robust. Over the life of a digital system, routine maintenance should be completed on a regular basis. However, eventually software becomes obsolete. This may be because new versions of the software have been released and the patches that enable older versions to run on newer versions are no longer available. It may also be that the software vendor has decided to retire the software.

Activity

Invite a member of the IT Department to talk to your group about the routine maintenance carried out in your centre or workplace. Ask about the tasks carried out, the schedule, how maintenance is documented, what the procedures are for emergency maintenance, and how users are advised about any system downtime.

Air gaps/gapping

Air gapping is creating a digital system that is physically isolated from potentially dangerous networks, such as the internet. Air gapping is having a digital system that works offline.



▲ Figure 10.11 An air-gapped digital system

As shown in Figure 10.11, an air-gapped digital system is one that is not connected, either physically or wirelessly, to other systems or networks. It is usually a standalone system or a network of digital systems that has no external links to any other system.

The name air gap refers to the concept that there is air between the digital system and any other system or network, including the internet. This means that the air-gapped system cannot be the victim of a threat or attack through another network. To carry out an attack on an air-gapped system would require the attacker to be physically sitting at the system.

There are still threats to an air-gapped system. The main threat is the use of removable storage devices. For example, a user downloads an infected file from a network onto a USB memory stick. This memory stick is then used to upload the infected file to the air-gapped

system. This means that the air-gapped system is now infected and has been the victim of a threat.

However, to some businesses and organisations, using the air-gapping technique to mitigate against threats is not always feasible. The reason digital systems are used in business is because users can share information and data, and access these data and information, from a centralised storage area.

But air gapping, if done properly, can provide complete protection to the air-gapped digital system. The other main advantage to using an air-gapped digital system is that, once the air gapping has been carried out, there are no ongoing, recurring costs.

Research

Investigate the types of industries, businesses and organisations that use air-gapped networks and the reasons why.

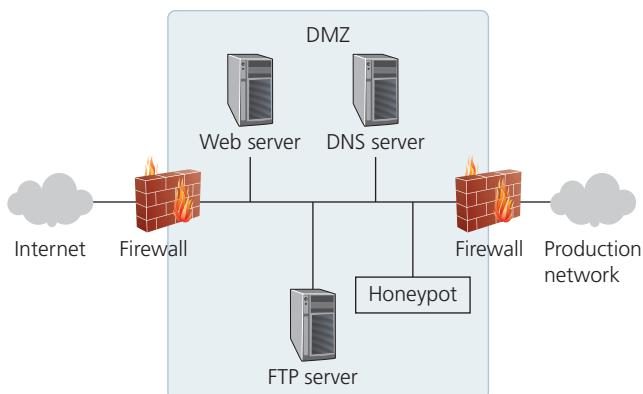
Test yourself

- 1 What is meant by an air-gapped digital device?
- 2 Describe one method of preparing an air-gapped digital device.
- 3 Describe how an air-gapped digital device could be compromised.
- 4 Identify one advantage of using air gapping as a way to mitigate against threats.

Honeypot

A honeypot is a digital system intended to behave like and copy a possible target including applications and data. It can be used to detect or deter attacks from a legitimate target. By using a honeypot it is also possible to gather intelligence about how attacks occur on digital systems.

By monitoring traffic to a honeypot system it is possible to identify which security procedures are strong and those which are weak. The weak procedures are those which will be exploited by attackers. By identifying the weak procedures it will be possible to improve security on the real digital systems that are being copied by the honeypot.



▲ Figure 10.12 Where a honeypot sits in the network

The honeypot will appear to be part of a network – but it is isolated and closely monitored. Any interaction with the honeypot will be as a result of a possible threat as no authorised users will have access to it.

Research

There are three types of honeypot: pure, high interaction or low interaction.

Research each type, including examples of where they could be used.

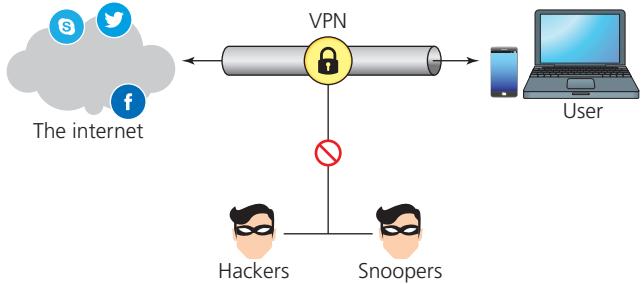
Discuss your findings with the rest of your teaching group.

Virtual private networks

Virtual private networks (VPNs) mitigate against threats by creating a secure connection to another network over the internet. This makes it possible to establish a private, safer and more secure network from a public internet connection.

VPNs were created as a method of connecting business networks together securely over the internet or to allow employees to access a business network remotely. VPNs also mask the **Internet Protocol (IP)** address, which means that online actions are virtually untraceable.

When a digital device is connected to a VPN the device appears to be in the same local network as the VPN. For example, if the VPN is based in Australia then it will appear that the connection is coming from Australia.



▲ Figure 10.13 A VPN works to protect a user from threats by creating a secure connection to another network over the internet

Figure 10.13 shows how a VPN connection works. All traffic is sent from the digital device over a secure connection to the VPN private server. So, when the internet is browsed the digital device the website requested is contacted through the VPN. The VPN hides the device IP address, protecting the identity of both the device and the user. The VPN forwards the request and sends the response from the website back through the VPN secure connection to the device. A VPN creates a private tunnel from a device to the internet and hides data through encryption. It is also possible to set access controls on a VPN if it is being used by a business or organisation. By doing this, access to data stored on, for example, the cloud, can be limited to those who need access for their job role.

As can be seen in Figure 10.13, using a VPN makes it more difficult for attackers to access the information and data being transmitted. This is because if the data is intercepted then it will be unreadable until the final destination is reached.

Activity

Investigate available VPN providers.

Produce a presentation, including speaker notes, comparing the features they offer. Your presentation should help a business to compare different providers before selecting which one to use.

Key term

Internet Protocol (IP): the string of numbers an internet service provider assigns a device, for example 192.158.1.38.

Test yourself

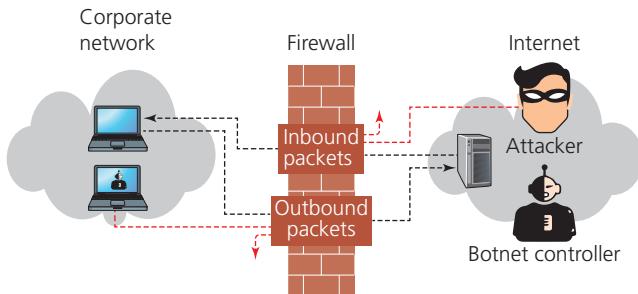
- 1 What is the purpose of a honeypot?
- 2 Identify the three different types of honeypot.
- 3 How does a VPN mitigate against threats?
- 4 What do VPNs aim to mask?
- 5 Why is it difficult for attackers to access data that is being transmitted?

Firewalls are covered earlier in this core element, in section 10.6, p. 250.

Weak/default passwords are covered earlier in this core element, in section 10.4, p. 247.

Passphrases are covered earlier in this core element, in section 10.6, p. 255.

Inbound and outbound rules



▲ Figure 10.14 Differences between an inbound and an outbound firewall

Firewalls can be set to monitor **inbound** or **outbound traffic** or both. The inbound and/or outbound rules the firewall will work to will need to be set. The rules will be used to inspect the data packets and determine if they should be blocked or allowed to continue on their journey. There are three rules that will need to be set:

- ▶ traffic type
- ▶ application
- ▶ destination and source.

Research

Research the different rules that need to be set up on a firewall.

Create a digital communication to explain these rules to a business owner.

Key terms

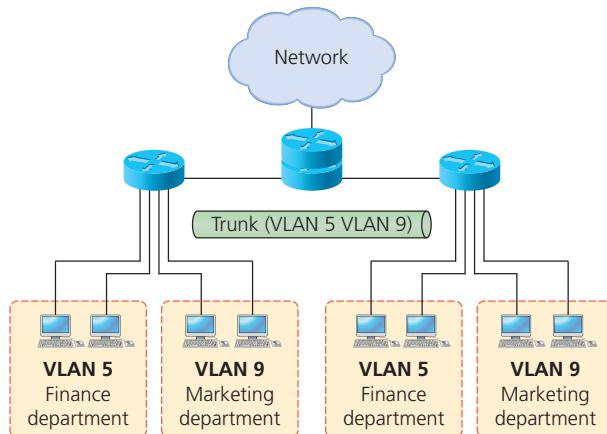
Inbound traffic: comes from outside the network through the firewall into the network.

Outbound traffic: comes from inside the network through the firewall out of the network.

Network segregation

Network **segregation**, also known as network **segmentation**, ensures that if an attack happens then not all of the network will be compromised.

Virtual local area network



▲ Figure 10.15 A virtual local area network (VLAN)

A virtual local area network (VLAN) is the method used to logically separate out networks. Imagine a LAN for a business with multiple departments or even multiple geographical areas. A VLAN is used to separate each department's area on the network into a virtual network. It helps to increase the efficiency of what would be a very large LAN and saves on network resources. It also helps to reduce the time taken for the transmission of data packets (this is more commonly referred to as latency).

Advantages

- ▶ Provides more security control as each VLAN is a simulated/virtual separate network within a larger overall network. Therefore, sensitive information is not accessible by areas of the larger LAN/WAN.
- ▶ Latency is decreased (the data packets are transmitted around a smaller network area).
- ▶ Easier to scale upwards or downwards as each area can be addressed in isolation and not impact other areas on the main network
- ▶ It is easier to troubleshoot problems on a smaller network than a larger one.

Key term

Segregation/segmentation: dividing a computer network into smaller parts.

Disadvantages

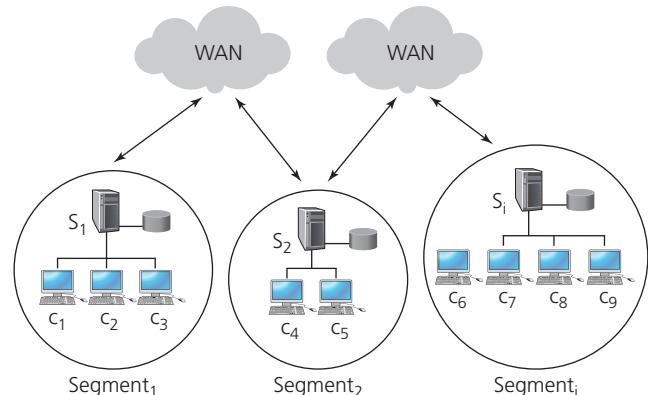
- ▶ It can be more expensive to implement as additional routers may be required to control the traffic of a very large network.
- ▶ Maintenance, including the addition of extra equipment, needs to be carried out using a logical and structured process to maintain existing VLAN segmentation.
- ▶ This means that implementation planning can take longer than other, simpler set-ups.

Physical network separation, or segmentation

This is when a large network is broken down into smaller physical components. Extra hardware may be needed like switches, routers and access points.

Switches, routers and access points are covered in section 5.2, p. 120.

One disadvantage of using physical segmentation is that it is financially expensive as extra hardware may need to be bought and installed, and there are the ongoing maintenance costs. Conflicts between the hardware can also occur. For example if two Wi-Fi access points (WAPs) are located in the same area then each will broadcast a different SSID.



▲ Figure 10.16 Physical network separation

Research

Investigate the advantages and disadvantages (in addition to those given above) of physically separating (segmenting) a network.

Discuss your findings with the rest of your teaching group.

Offline networks

An offline network is one that is not connected to the internet. An air-gapped system is an example of an offline network.

Air-gapped systems are covered in section 10.6, p. 260.

Network monitoring

Network monitoring is running a system that constantly monitors a network to check performance. The system can detect slow or failing components and provide detailed feedback to the network management team.

Network monitoring is very similar to an intrusion detection system (IDS) in that the monitoring is constant and happens, once installed and set up, automatically. An IDS monitors threats and problems from traffic coming into the network, while network monitoring is working within the network.

Intrusion detection systems, intrusion prevention systems and network-based intrusion detection systems are covered in section 10.6, p. 251.

Problems caused by overloaded or crashed servers and network connections can be identified by network monitoring.

Another monitoring tool is a ping test. A ping test checks the response time of any request to a host on an Internet Protocol (IP) network. A ping test measures the time taken for the round trip of a message from a host to a destination system and back again. A ping test works by sending an **ICMP** echo request packet to the target host and waiting for the ICMP echo reply.

The results of a ping test show any errors, if packets were lost and a summary of the results which include:

- ▶ minimum round trip time
- ▶ maximum round trip time
- ▶ mean round trip time
- ▶ standard deviation of the mean round trip time.

Research

Investigate the ping tests used at your centre or workplace. Talk to the technicians about the results expected from the network. Investigate the results of ping tests carried out on the network.

What are considered good, acceptable and poor ping test results?

Key term

ICMP: Internet Control Message Protocol.

To maintain security of a network, monitoring of websites visited, or attempted to be visited, by users should be carried out. For example, many network managers have put social media websites on a blocked list as well as, in some cases, shopping websites.

One reason for this is that many social media websites allow users to download files, which could have viruses or other malware attached. Network technicians will also monitor, in real time, all website requests which originate from inside the network. This will enable them to pre-empt a possible attack as they will be aware of all traffic on the network.

Removable media controls

Removable media includes portable devices such as USB sticks, SD cards and external hard drives. Typically these enable people to copy and transfer data, take it off site and work away from the physical environment.

As the use of these devices has increased, so have the threats. Because the devices are portable and removable and can be connected to a range of digital systems, the risk of network security breaches has increased.

If the use of removable devices is not controlled, then there may be:

- ▶ **loss of data and information** – removable devices can easily be lost resulting in the compromise of large volumes of sensitive information
- ▶ **introduction of malware** – if removable devices are connected to home or public devices they can become infected and transport the malware to the company's network
- ▶ **reputational damage** – if sensitive data is lost then the reputation of the business or organisation can decrease
- ▶ **financial loss** – if sensitive information is lost or compromised the business or organisation could incur financial penalties as legislation relating to the storage and processing of data will have been broken.

Legislation relating to data and information is covered in section 8.1, p. 189.

Research

Using the BBC News and other websites, investigate cases where removable digital devices have been found by members of the public.

Many businesses, organisations, schools and colleges have implemented a 'no removable device' policy. There are, however, some occasions when removable media need to be used. To make sure these devices are used in the most security conscious way possible, guidelines should be created for staff to follow. One guideline may be:

All removable devices should be password protected. The passwords should be strong as this will increase the security of the data and information stored on the device.

Activity

Create an infographic aimed at 16–18-year-old students showing guidelines for the use of removable storage devices.

Anti-virus software is covered in section 10.6, p. 249.

Managing user privileges

User access restrictions/privileges are covered in section 10.6, p. 253.

What privileges are given to users should be carefully considered. Giving all users full privileges means that there is an increased security risk of a user's account being hacked or attacked. The privileges given to users should be based on their job role and what they need to do with the data.

By providing appropriate user privileges, risks can be reduced. Risks can include:

- ▶ misuse of privileges – this could be accidental or deliberate and can lead to a user gaining access to data and information which should be kept secure
- ▶ increased vulnerability – user accounts need to be deleted as soon as they are no longer required. Attackers can use old accounts to carry out an attack as the account will still have the privileges attached to it. If these privileges were linked to sensitive data, for example financial, then this access can be exploited.

Research

Investigate the user privileges set at your school or workplace. Are the privileges appropriate to job roles?

Discuss your findings with the rest of your teaching group.

Key term

Ethical hacking: an alternative term for penetration testing.

Penetration/vulnerability testing

All businesses and organisations that use digital systems should carry out security testing on a regular basis. By doing this, they can identify vulnerabilities and rectify them before an attacker exploits them.

Penetration testing (also known as **ethical hacking**) can be carried out by white or grey hat hackers. The NCSC defines penetration testing as:

'A method for gaining assurance in the security of an IT system by attempting to breach some or all of that system's security, using the same tools and techniques as an adversary might.'

There are many different types of penetration testing that can be carried out.

Network penetration testing

This can be carried out to look for internet and/or external openings to identify how vulnerabilities could be exploited by internal and/or external attackers.

A network attack is the most common type of penetration test. Network attack tests may include analysing network traffic, testing routers, and identifying legacy devices and third-party appliances where updates have not been implemented.

Social engineering penetration testing

This can be carried out to look for human vulnerability. These tests try to convince employees to part with, for example, log-in details/credentials or sensitive data and information. This type of test evaluates the success or failure of the security policies, procedures and processes which have been implemented to protect against a social engineering attack. This type of test can uncover any weaknesses in employees' understanding of the security policies and procedures and may act as a catalyst for staff training.

Physical penetration testing

This attempts to test the physical security in place. This type of penetration testing aims to test access to rooms or buildings (in an attempt to steal and/or remove digital devices, hard drives or recycling containers) to assess the effectiveness of the current physical security measures. As with social engineering, this type of test

can reveal weaknesses in employees' understanding of the security policies and procedures and may trigger staff training.

Activity

Two other types of security testing that can be carried out are web application and wireless.

Research these types and create an infographic detailing how and why these are carried out.

White box testing

This is when the people carrying out the penetration tests are provided with full and complete information about the digital system to be tested. White box testing aims to identify any existing vulnerabilities in the software and any incorrect configurations within the digital system.

Black box testing

This is when the people carrying out the penetration tests are provided with no information except the name of the business or organisation. Black box testing is carried out from an external perspective with the aim of identifying ways that the digital systems could be accessed by attackers. The main disadvantage of using black box testing is that, because full and complete details have not been provided, vulnerabilities within the digital system may not be identified.

Port scanning

Port scanning is a technique that identifies open ports and services available on a network host. Network technicians can use this technique when carrying out a vulnerability audit by sending packets to specific ports on a host and analysing the results. But, the technique is also used by attackers to target vulnerable networks.

The technique identifies which ports on a network are open and ready to receive or send data. A list of active hosts is created with their IP addresses. This is done by carrying out a network scan. This activity provides the organisation of IP addresses, hosts and ports. By doing this, open or vulnerable server locations can be identified which will help to determine the security level. The scanning can also identify the existing security measures, for example a firewall.

Ports are covered in section 5.2, p. 120.

Attackers use port scanning to identify open ports which can be used to enter the network to carry out an attack on the network. By carrying out a port scan the technicians

can identify any open ports which provide an exploitable vulnerability and close them as soon as possible.

SQL injecting testing

SQLI is covered earlier in this core element, in section 10.3, p. 242.

A successful SQLI attack can:

- ▶ read data from a database
- ▶ edit/insert/update/delete data in a database
- ▶ carry out administrative tasks on a database, for example closing it.

SQLI testing is the process of injecting, in a safe environment, code into a database to check for vulnerabilities.

Secure Sockets Layer/Transport Layer Security scanning

Web servers need to secure incoming and outgoing traffic, including user credentials and payment details. Transport Layer Security (TLS) is a newer protocol than Secure Sockets Layer (SSL) and provides better protection against attacks.

TLS and SSL certificates are used to provide data encryption. This is shown by the use of 'https' at the start of the website URL. Https means that the data is encrypted and is only decrypted when it arrives at the destination.

Encryption is covered in section 10.6, p. 252

Firewalls are covered in section 10.6, p. 250

A TLS and SLL content scanner can be used to decrypt, scan and re-encrypt data to check for trustworthiness. The scanner is usually part of a firewall. The certificate is sent, with the public key, to the client. The client should trust the certificate as this is known by client browsers. A secure connection has been set up between the client and the gateway. The destination website is connected to with a secure connection created using the destination server's certification and the public key.

The gateway can now decrypt, scan and re-encrypt content from and to a client as it has the associated private key of the client's public key.

TLS and SSL content scanners can apply exceptions, such as specific URLs' categories, for example banking sites. This would mean that every other website not on the exception list would be scanned by the SSL scanner.

Protocols of internet security assurance

Protocols are a set of rules that determine how data is transmitted between different devices in the same network. A protocol enables communication between connected devices, regardless of any differences in their internal processes, structure or design.

Protocols are also used to communicate on the internet. When a client requests access this is granted by the server, and protocols are agreed between the client and the server – this is called handshaking. When this process is complete the data transfer can begin.

The common protocols, and their purposes, are shown in Table 10.3.

Virtual private networks are covered in section 10.6, p. 261.

Protocol	Meaning	Description
IPSec VPN	Internet protocol security	This protocol operates at the network level. It can be used on its own but can also be used with other VPN protocols like L2TP to provide encryption. IPSec VPN is commonly used for site-to-site VPNs. Many iOS VPN apps also use IPSec.
SSL VPN SSL/TLS	SSL – Secure Socket Layer TLS – Transport Security Layer	These are the most commonly used protocols. TLS is a newer protocol than SSL and provides better protection against attacks. SSL uses the application layer. It works in conjunction with HTTPS to provide a secure encrypted connection using the internet. It is used in some VPN protocols but is not in itself a VPN protocol. SSL is also used to create HTTPS proxies.
SFTP	Secure File Transfer Protocol	A protocol for transferring large files over the internet. It is a more secure method than the File Transfer Protocol (FTP) and includes Secure Shell (SSH) security components. It is also known as Secure Shell File Transfer Protocol.
SSH	Secure Shell Protocol	This protocol provides a secure connection to devices. It is a cryptographic network protocol which is used to provide network services securely over an unsecured network. This is used for remote access command line logins, and execution. Any network service can be secured using SSH.
HTTPS	HyperText Transfer Protocol Secure	This is a secure version of HTTP and uses the SSL/TLS protocol for encryption and authentication. The HTTPS protocol makes it more secure for website users to exchange confidential data such as financial data and information, and log-in credentials. HTTPS is becoming more common than HTTP as a protocol for transferring data and files over the internet as it offers more protection against threats and attacks.

▲ **Table 10.3** Common protocols and their purposes

Test yourself

- 1 What is an offline digital system?
- 2 What is white box penetration testing?
- 3 What is the purpose of a port scan?
- 4 Identify one action that a successful SQLI attack can carry out.
- 5 Which layer does the IPSec VPN operate at?

10.8 The interrelationship of components required for an effective computer security system

Security aims to protect digital systems, data and information. Part of this is to ensure that the digital systems, data and information are not compromised when/if a critical threat happens.

The CIA triad clarifies and defines the relationship between confidentiality, integrity and availability. Security must be used to maintain the CIA triad.

The CIA triad is covered in section 10.2, p. 239.

Identification, authentication, authorisation and accountability

The principles of identification, authentication, authorisation and auditing (IAAA) will also help increase security.

Every user needs:

- ▶ **identification** – this could be by use of usernames or biometrics
- ▶ **authentication** – additional information needs to be provided based on that provided at the identification stage. This could be a PIN, password/passphrase, or a token. The identification and authentication stages work together rather than separately
- ▶ **authorisation** – this is what the user is able to do. It links with setting and managing user privileges
- ▶ **auditing** – all actions carried out by authorised users will be recorded.

By using security, including the IAAA principles, the likelihood of a threat being successful is reduced because the identified vulnerabilities of the digital system, data, information and people will also be reduced.

Risk management

To identify any possible problems that may occur or be exploited, risk management processes should be completed on a regular basis. The risk management process should include:

- ▶ **Threats** – an identification of the possible threats that may occur. This should cover not only the digital systems but also people and the physical environment.
- ▶ **Vulnerabilities** – all vulnerabilities should be identified. These may have already been identified as a result of vulnerability testing.
- ▶ **Impact** – what is the impact of the threat/vulnerability? Is it negligible, moderate or serious? Depending on how high the impact level is will depend on the priority of taking remedial action.
- ▶ **Probability** – what is the probability of the threat happening or the vulnerability being exploited? The higher the probability is, the higher the remedial action priority.
- ▶ **Mitigation** – what action can be taken to reduce the threat level or close the vulnerability?

Threats are covered in section 10.3, p. 241.

Vulnerabilities are covered in section 10.4, p. 246.

Impacts are covered in section 10.5, p. 248.

Risk mitigation controls are covered in section 10.6, p. 249.

There is a strong relationship between all the different components, but by using security the chance of any of the components being compromised is reduced.

Project practice

An online games company provides games to its customers. Customers need to register their personal and payment details to buy and play the games.

Different options are available for the games. Some games are played online with the players' progress being stored on a dedicated games server. Other games are available to buy and download, meaning they can be played offline.

Some of the games are single player while others can be played by several players at once. If several players want to play the same game at once, each player must be a registered user.

Each customer has a username and password. The password is provided when registration is complete. The players can change their password to something more memorable. The username and password are stored on the games company's server.

The games company has been the victim of several data breaches and threats, including a DDoS attack, malware and malicious spam.

You have been asked to:

- ▶ Explain to the owner of the games company the importance of maintaining the CIA triad relating to customers' personal and payment details.
- ▶ Provide details about the threats that have happened and other potential threats to the games company.
- ▶ Explain how IDS and IPS can be used to increase security of the digital systems, data and information stored by the games company.
- ▶ Explain how firewalls and internet protocols can be used by the games company.
- ▶ Provide details of possible processes and procedures that could be implemented to mitigate against future attacks, and include recommendations.

Assessment practice

- 1 Explain why it is important to maintain the confidentiality of employees' salaries.
- 2 Discuss the importance of maintaining the CIA triad.
- 3 Explain the process of buffer overflow.
- 4 Identify and describe two different types of malicious spam.
- 5 Identify and describe two technical out-of-date vulnerabilities.
- 6 Define hashing and asymmetric encryption, explaining the difference between them.
- 7 Discuss how user access restrictions can be used to mitigate against threats and ensure security.
- 8 Compare the use of a password and a passphrase.
- 9 Explain the process of location-based multi-factor authentication.
- 10 Identify and describe one protocol that can be used in a VPN.

Core element 11: Testing



Testing is a check to establish whether the digital product meets the expected requirements and is defect free. Testing involves the execution of the digital components within the product using manual or automated tools. The purpose is to identify any errors, gaps or missing requirements when compared to the requested requirements.

Testing is very important, so that any issues can be found. Testing enables these issues to be identified early and resolved before the digital product is put into use. If tested correctly, it ensures the security, reliability and performance of the product. This will save time, be cost-effective and make the customers happy (customer satisfaction). Problems within a digital product can be expensive and even dangerous in some situations. At worst, they can cause human loss of life or injury, as well as monetary loss. A search of the internet will provide you with many examples of where products were insufficiently tested and caused serious problems.

Learning outcomes

In this core element you will learn about:

- 11.1** The purpose of testing digital components
- 11.2** The process of applying root cause analysis to problems

- 11.3** Testing methods and their application in the digital sector

11.1 The purpose of testing digital components

Purposes of testing

Functionality testing

This is used to confirm the functionality of digital components against the functional requirements (specification). The tests are used to verify each component by providing an input and comparing the output against the functional requirements. Functional testing is primarily **black box testing**. Functional testing checks the **user interface (UI)**, **application programming interfaces (APIs)**, database, security, client/server communication and so on. This form of testing can be carried out manually or by using automation.

Usability testing

This a method for confirming a digital component's functionality or digital components' readiness for release. It is performed by users who are part of the intended end users. Usability tests analyse the overall end user experience and consider how easy the product/system is for them to use so that they can complete sets of tasks that they would normally carry out.

Usability testing allows you to gather data that is required to identify any issues and improve the design.

Compatibility testing

This is a type of non-functional testing and user testing for software and/or hardware to confirm that the digital components can run on or alongside different hardware, operating systems, applications, network environments and even on mobile technology. There are different types of compatibility testing.

- ▶ **Networks** – used for analysing the performance of a system in a network using varying parameters such as bandwidth, operating speed and capacity.

Key terms

Black box testing: the testing of the software when the internal structure and design is not known to the tester.

User interface (UI): enables a person to control a software application or hardware device in a natural and intuitive way.

Application programming interface (API): software that enables two applications to talk to each other. Every time you use an app on your smartphone, for example Facebook or Twitter, you are using an API.

- ▶ **Devices** – used to check the compatibility of the digital component with different devices, for example printers, scanners, Bluetooth devices and so on.
- ▶ **Mobile** – used for checking the compatibility with mobile platforms such as iOS and Android.
- ▶ **Browser** – used in relation to software such as a website; to check that it is compatible with different web browsers such as Google, Firefox, and Edge.
- ▶ **Software versions** – used to confirm that the digital component will function with different types of software and operating systems. This includes previous versions of operating systems and other software, for example Windows 7 and Windows 10.
- ▶ **Hardware** – used to ensure that the digital component is compatible with different types of hardware and hardware configurations.

Compatibility testing includes forward and backward compatibility testing.

- ▶ **Forward compatibility testing** – used to confirm that the developed digital component is compatible with the latest hardware/software. However, you must remember that newer versions of hardware/software are always released and therefore you cannot confirm that the digital component will always remain compatible.
- ▶ **Backward compatibility testing** – used to confirm that the developed digital component will work with older versions of hardware/software. It is easier to predict the results as the changes from previous versions are known.

Consider an organisation that has customers and/or offices all over the world – the hardware/systems/devices can all be different. Tests must be carried out to ensure that any software/hardware can function as intended, regardless of where it is being used.

Accessibility testing

This form of testing is a subset of usability test and can include consideration for end users who have special accessibility needs, for example someone who has restricted sight or movement in the hands and/or arms. The intention of the testing is to ensure that the digital components pass both accessibility and usability standards.

Customer/client/end user satisfaction testing

This is usually referred to as user acceptance testing (UAT). This is the testing of the digital components to confirm whether the end user will have a positive experience (or not). The digital components are tested to ensure they meet the requirements of the customer/

client/end user. It also evaluates the compliance of the digital components with the requirements of the business and confirms that the required criteria for the end users have also been achieved.

Fault finding and debugging

Fault finding and debugging are important activities that are carried out during the development of software and maintenance. Fault finding is carried out to check if there are any errors and debugging is carried out to locate and fix these errors. The testing can be carried out manually or automated. There are different types of fault finding, for example unit, integration, system and stress testing. These are discussed in more detail later in this core element.

Impact assessment

This is a process used for considering the implications for businesses, the environment and people of the proposed implementation of digital components.

People will include end users and employees, as well as anyone else who could be affected. Impact assessment is carried out while there is still an opportunity to make changes to (or, if necessary, abandon) the proposals and implementation of any digital change.

Efficiency of individual components

Efficiency testing tests the performance of a component and the resources required in order to carry out its function. This is commonly used in software development. Efficiency testing will analyse what resources were required for the component to function effectively and how many were actually used. Testing efficiency takes into consideration people, tools, resources, processes and time in order to calculate the efficiency. The whole purpose of implementing any digital component is to support the completion of tasks with minimal effort. It is therefore important that the efficiency of any new digital component improves the completion of the tasks and does not hinder them.

Review accuracy of data

Data is one of the most valuable resources available to businesses regardless of the sector. Data is only useful if it is of a high quality. Bad data can lead businesses to make expensive mistakes. Some of the expense can be incurred due to the time employees must take correcting data errors that also cause mistakes with customers. In the manufacturing industry, incorrect data can result in the production of faulty products and in some cases can be dangerous to life. It is always important that any implementation of digital components does not have a negative impact on

the quality of any data. Therefore, rigorous testing must take place to ensure that any data and resulting calculations are accurate and of a high quality.

Ensuring desired outcomes

Any implementation of digital components must meet the needs of the business, stakeholders, customers and employees. It is of paramount importance to test digital components to ensure that they function as intended, efficiently and effectively. If products and/or services do not meet the expectations of the customers, clients and stakeholders, then a business can easily fail.



▲ Figure 11.1

Performance monitoring

Performance within today's digital environment is a necessity. Regardless of where data is stored, for example on premises, in data centres or in the cloud, the IT operations team must incorporate monitoring into service delivery. It acts as an early warning system that will alert the IT team when something has gone wrong (or is about to go wrong). This can include **downtime**, **outages**, application slowness and so on.

Digital components

Software

Software testing is important because we can all make mistakes. Some of these mistakes are unimportant, but some mistakes can be expensive or even dangerous.

Key terms

Downtime: a period when a system is not available. This may be an individual computer, a network, or servers.

Outages: loss of power to a computer system.

Here are some of the reasons why software testing is very important:

- ▶ To point out defects and errors that were made during the development phases of the software.
- ▶ To maintain customer satisfaction and for customers to have the belief that the business is reliable. If customers lose confidence in the business, they will go to a different business. Some issues can even lead to a financial penalty for the business.
- ▶ Quality control of a product – if the product being delivered to the customer is a quality product, then customer confidence and satisfaction are maintained.
- ▶ So that the facilities used to provide customers with products, services and applications are to a high standard with respect to accuracy, maintenance and reliability.
- ▶ To ensure the effective performance of products and applications.
- ▶ To ensure that the application will not result in failures. This can be very expensive in the future or in the latter stages of development. Effective testing ensures that bugs and issues are detected at an early stage during production. It also identifies any changes that may be required to the design at an early stage of the development life cycle.

Hardware

Hardware testing is important as it ensures that every component of a system is operating as it should and performing in accordance with the specified requirements. A well-designed, comprehensive and structured testing programme ensures that all aspects of the system are tested. This is especially important for key systems, for example systems for production lines and finance. The reasons for hardware testing are similar to those for software as stated above.

Data

This is covered in ‘Review accuracy of data’ earlier in this core element in section 11.1, p. 272.

Before performing any type of test, it is important to consider the data that is going to be used. What is used will depend on what is actually being tested. It is also not feasible to be able to use every possible piece of data and therefore testers must be able to select data from a limited range.

Test data can be:

- ▶ Valid – data that the program and/or system is likely to accept and process.

- ▶ Extreme – this is data that is from the extreme boundaries (highest and lowest potential data) from a range of data.
- ▶ Erroneous – this is data that should not be accepted and therefore cannot be processed.

Interfaces

Connections between different components is termed as the interface. Interface testing ensures that each component works with the other components and that there is no ‘gap’ in communication between them or miscommunication. The testing of the interface is a form of software testing that confirms the functionality of the software interface. Interface testing is an important aspect of software testing.

Test scripts

These are line-by-line descriptions that contain information about the transactions of the system. They should be carried out to validate the application or system being tested and be entered onto a test plan. A test script should list each step that should be taken and what the expected results are. The reasons for using test scripts are as follows:

- ▶ If it is prepared in advance, it helps to reduce the likelihood of errors during the testing process.
- ▶ It is the best approach to verify that nothing is missed and that the results are true as per the test plan.
- ▶ Testers can miss certain features if they are not aware of them or allowed to ‘do their own thing’ when looking at the product. It therefore focuses their attention on what tests are required.
- ▶ Testers may assume that a result is correct because there is no error message, when in fact the result could be incorrect. Therefore, the test script indicates the results they should be looking to achieve.
- ▶ It is useful when the user performance is important and specific.

ISO 29119 Part 1 defines a test script as ‘A test procedure specification for manual and automated testing’.

Test yourself

- 1 Explain the purpose of functionality testing.
- 2 Describe the term ‘interfaces’.
- 3 Discuss the importance of compatibility testing.
- 4 Identify two reasons for using test scripts.
- 5 Describe the term ‘impact assessment’.

11.2 The process of applying root cause analysis to problems

Obviously the purpose of RCA is to get to the ‘root’ of the problem, by asking questions such as:

- ▶ What is the problem?
- ▶ What has caused the problem?
- ▶ How can the problem be solved?

Once this is established, an assessment of the situation can take place and consideration be given to what lessons have been learnt and how similar problems can be mitigated in the future.

There is a clear process that should be followed when conducting an RCA to ensure that the analysis is efficient, effective and useful. While it is important to solve the problem, it is just as important to establish what is causing the problem and how this can be addressed. This is especially important when a business needs to continue to function. There is very little point in resolving a problem only for it to keep reoccurring and potentially disrupt operations.

Problem can be simple (one root cause) or it can be more complex (a number of root causes) and time must be given to establishing if all of the root causes associated with a problem have been identified. It is always important to focus on the problem itself with respect to how and why it happened as opposed to ‘who did what’.

Problem solving requires a careful and methodical approach. It is more effective to plan the approach to investigating the problem and follow a step-by-step process. This enables you to gather relevant and detailed evidence as to why and how the problem has occurred.

Documenting RCA is particularly important as there needs to be sufficient information to support the identification of any potential corrective actions that will be required. The implementation of corrective actions can also give an indication as to how future problems can reoccur. Decisions can be made as to whether there are adaptations or new processes, equipment, upgrades etc required as well as when they would be required to ensure that the problem does not arise in the future.

The ‘Five Whys’

This method for performing RCA is known as the Five Whys approach (sometimes written as 5 Whys or

5 Ys). This involves every answer to a ‘Why’ question being followed by a further and deeper ‘Why’ question. Eventually the root cause of the problem will be exposed. If there is more than one root cause, then the ‘Whys’ can look like a linked matrix. Consider this simple example:

Problem – I’ve got three points on my driving licence.

Why 1 – why have you got three points on your driving licence?

Response to Why 1 – because I was speeding.

Why 2 – why were you speeding?

Response to Why 2 – because I did not notice the speed restriction sign.

Why 3 – why didn’t you notice the speed restriction sign?

Response to Why 3 – because I was not looking at the road signs.

Why 4 – why weren’t you looking at the road signs?

Response to Why 4 – because I was not concentrating on the road signs.

Why 5 – why weren’t you concentrating on the road signs?

Response to Why 5 – because I was too busy talking to my friend on my mobile phone using hands free.

So, the root cause of the problem is that the driver was too busy talking to their friend on their mobile phone when driving, even though they were using hands free. This resulted in their lack of concentration on their driving, resulting in three penalty points on their licence.

The solution (and to prevent this from happening again) is not to use a mobile phone at all when driving, even if using hands free. The 5 Whys is just one method and others include Pareto, Fishbone etc.

When to use root cause analysis

RCA should take place when an issue occurs that results in outcomes that disadvantage an organisation and its stakeholders. Some criteria that can be used to determine if an RCA should be carried out are:

- ▶ failure of service delivery/functional operations
- ▶ loss of data
- ▶ the occurrence of an undefined process

- ▶ system downtime
- ▶ complaint or feedback from a stakeholder.

How to use the root cause analysis process

In order to carry out root cause analysis, there is a clear process that should be followed:

- ▶ It is important to identify what the problem is and the impact that it has on the stakeholders involved. How does it impact on the function of the business? If whilst investigating the problem, there is no immediate indication of an impact on the stakeholders, it is always important to consider if there is the potential for an impact to happen.
- ▶ What information is there available about specific issues/problems that have occurred? When did it happen, what activities/tasks were being carried out at the time, how did it happen? It is important to gather as much data and information as possible. This can include system logs, feedback from all relevant stakeholders internal and external to the organisation as well as identifying where the problem has occurred before. Basically anything that can help you investigate the problem.
- ▶ What would be the impact on an organisation and its stakeholders if the problem was not resolved at all, or if there was a delay in resolving the problem.
- ▶ Once you have gathered the information and data you need, you can then investigate the problem and identify what caused the problem to occur. Remember there can be more than one cause to a complex problem.
- ▶ Remember to use a method such as the 5 Whys approach i.e. you ask a 'why' question and for the answer, you ask further 'why' questions until the root cause of the problem is exposed.
- ▶ If there is more than one cause to the problem, then a systematic approach should be taken. Do not try and address all of the causes at the same time. Prepare a list of priorities with respect to the causes and slowly work your way through them. When prioritising the causes, consider the impact and resolutions that are required and always consider what effect this has on the functioning of the business. Some causes may be able to be addressed more quickly with very little, if any, downtime that will disrupt the running of the business. Others may take long and require e.g. a system to be taken down. Consider when it would be best to carry this out in order to minimise any disruption to the business processes. Safety can also play a big part

in this and therefore there may be occasions when systems have to be put on stop until the issue has been resolved.

- ▶ The main focus is to eliminate the problem and therefore suitable solutions have to be identified. The results of the investigation and the prioritisation of the tasks involved will assist in the identification of suitable solutions which can then be implemented. As previously stated, consideration has to be given to timescales such as when each solution can be implemented and who will implement the solution.
- ▶ As with all situations when there are changes made to any form of digital technology whether it is hardware or software related, there is always a requirement to monitor the process and make changes as and when required.
- ▶ The final step in the process is to establish how and when the system will be tested/monitored to ensure that it is performing as required.

Test yourself

- 1 Describe the core principles for RCA.
- 2 Identify the three goals of RCA.
- 3 Explain the Five Whys.
- 4 Identify two situations when RCA should be considered.
- 5 Discuss the steps that should be taken when carrying out RCA.

11.3 Testing methods and their application in the digital sector

Concept testing

Concept testing is used for:

- ▶ scoping and validating requirements
- ▶ informing decisions before committing time and resources to a project.

Market research is used to understand the strengths, weaknesses and areas of potential improvement for a particular concept. This could be any form of IT solution, for example development of software, network or digital system. Interested internal/external stakeholders are provided with the information relating to the basic concept. They then provide feedback which is then collated and analysed for consideration prior to the product being fully developed and/or released. Concept testing can cost time and money, but the

research can also save a lot of unnecessary costs in the long term.



▲ Figure 11.2

Usability/audience testing

Usability/audience testing involves:

- ▶ testing whether the functionality fulfils the desired outcome
- ▶ identifying usability problems
- ▶ determining user satisfaction with the product.

The aim of usability testing is to understand how end users interact with the digital product and whether it meets the end users' requirements. Data is gathered based on the results of the tests, so that usability issues can be identified and improvements made. There are two groups of people within a usability test and they are the end users and the observers. The ideal situation is that the two groups do not know each other. This way, the observers can gather data that is more objective.

A scenario is constructed for the end users to complete a set of tasks. These can be new tasks and/or old tasks that they already complete. End users are recruited to create a focus group that should be indicative of the target audience. The end users are then required to complete these tasks under controlled conditions.

The observers will then watch and/or measure the overall success of the end users completing the tasks. During this time, the observers will identify any usability issues. These issues will be recorded so that the product can be reviewed and any necessary changes can be made.

During usability/audience testing, it will also become apparent whether the end users have had a positive experience (or not). Therefore, it is also used to establish user satisfaction with the product.

Stress testing

Testing whether a system can function with expected demand by replicating real-world load

This is also sometimes referred to as load testing (but it is more than just load testing) and is a form of non-functional testing. It provides information on how the software/digital system conducts itself under specific loads/stresses and is also associated with performance testing.

Load testing

This is a type of performance test that is used to check how a system functions under a heavy volume of virtual users working simultaneously. Performance activities are carried out simultaneously over a period of time and the system is monitored to see how it copes with handling large volumes. Load testing is used when it is necessary to determine how many users the system can effectively handle at the same time.

Stress testing

This is also a type of performance test that is used to check the upper limits of the system. The system is therefore tested using extreme loads. These tests examine how the system will perform under intense loads as well as how it recovers when reverting to normal usage. Stress tests are also used to identify memory leaks, slowdowns, security issues and data corruption.

If a stress test includes a sudden high increase in the number of virtual users, it is called a spike test. A stress test that is carried out over a long period of time to check the system's sustainability with a slow increase in virtual users, is called a soak test.

Penetration testing

Penetration testing:

- ▶ is used to determine vulnerabilities in a controlled environment
- ▶ involves an authorised attack on a system.

Activity

Find and watch the video called 'What is penetration testing' at www.cisco.com.

What are the main points related to the importance of cyber security raised in the video?

Key terms

NCSC: the UK's National Cyber Security Centre.

Ethical hacking: an alternative term for penetration testing.

Penetration testing (also known as **ethical hacking**) can be carried out by white or grey hat hackers.

The **NCSC** defines penetration testing as:

'A method for gaining assurance in the security of an IT system by attempting to breach some or all of that system's security, using the same tools and techniques as an adversary might.'

There are many different types of penetration testing that can be carried out.

Network penetration testing

This can be carried out to look for internal and/or external openings to identify how the vulnerabilities could be exploited by internal and/or external attackers.

A network attack is the most common type of penetration test. Network attack tests may include intercepting network traffic, testing routers, stealing log-in details, exploiting network services, and discovering legacy devices and third-party appliances where updates have not been implemented.

Social engineering penetration testing

This can be carried out to look for human vulnerability. These tests try to convince employees to part with, for example, log-in details or sensitive data and information. This type of test evaluates the success or failure of the security policies, procedures and processes which have been implemented to protect against a social engineering attack. This type of test can uncover any weaknesses in employees' understanding of the security policies and procedures and may act as a catalyst for staff training.

Physical penetration testing

This attempts to test the physical security in place. This type of penetration testing aims to test access to rooms or buildings (in an attempt to steal and/or remove digital devices, hard drives or recycling containers) to assess the effectiveness of the current physical security measures. As with social engineering, this type of test can reveal weaknesses in employees' understanding of the security policies and procedures and may trigger staff training.

Research

Two other types of security testing that can be carried out are web application and wireless.

Research these types of testing and create an infographic detailing how and why these are carried out.

Black box testing

Black box testing involves:

- ▶ testing inputs and outputs against expected results
- ▶ measuring the functional requirements of a system.

The people carrying out the penetration tests are provided with no information except the name of the business or organisation. Black box testing is carried out from an external perspective with the aim of identifying ways that the digital systems could be accessed by attackers. The main disadvantage of using black box testing is that, because full and complete details have not been provided, vulnerabilities within the digital system may not be identified.

Black box testing is also used to test a system against external factors that are responsible for software failures. This form of black box testing concentrates on the input that is entered into the software and the output that is produced. It is based on the requirements for the system and checks the system to validate it against the predefined requirements.

The following parameters are checked when carrying out black box testing:

- ▶ the accuracy of the actions performed by the users
- ▶ how the system interacts with the inputs
- ▶ the response time of the system
- ▶ the use of data structures in the user interface
- ▶ any usability issues
- ▶ any performance issues
- ▶ a sudden application or system failure.

There are different types of black box testing and here are some examples:

- ▶ **Functional testing** – as previously stated in section 11.1, this is testing the functional requirements of the system.
- ▶ **Non-functional testing** – this is concerned with the non-functional requirements of the system and to determine how ready the system is according to the various criteria that are not covered by functional criteria.
- ▶ **Regression testing** – this is carried out after code fixes, upgrades and/or any other system

maintenance. This checks that any new changes have not had an impact on the system as a whole or any part of the system.

White box testing

This is when the people carrying out the penetration tests are provided with full and complete information about the digital system to be tested. White box testing aims to identify any existing vulnerabilities in the software and any incorrect configurations within the digital system.

The main purpose of white box testing is to test the workings of software as well as strengthening its security, usability and design. Also known as structural testing, the test selects the inputs to test and follows their path through the software until they

reach their expected outputs. White box testing is used in the unit, integration and systems phases of software testing. Although white box testing can find errors in various aspects of the software, it can miss problems in areas that are not tested by the tester.

Test yourself

- 1 Describe the difference between white box and black box testing.
- 2 Explain the purpose of stress testing.
- 3 How does usability/audience testing identify usability problems?
- 4 Describe network penetration testing.
- 5 Explain the difference between load and stress testing.

Project practice

You work in the IT department of a large organisation that sells insurance, for example property insurance, car insurance, travel insurance and so on. People can complete application forms online and obtain quotes. If they accept a quote, they can create a registered account and upload their details to pay for their insurance annually or monthly. The online area for each customer provides them with access to their insurance documents that they can download and print out.

Your company are having new software and hardware installed as well as a new network. The organisation has also had their website updated to make it 'more user friendly'.

Work in small groups and prepare a test strategy selecting appropriate tests from the ones that you have learned about in this core element. You must be able to justify your selection of tests

Assessment practice

- 1 What is the difference between backward and forward compatibility testing?
- 2 Identify and describe two types of black box testing.
- 3 Give another term for white box testing.
- 4 Ethical hacking is an alternative term for penetration testing. Is this true or false?
- 5 Discuss the process of applying root cause analysis.
- 6 Explain the role of debugging and fault finding in relation to the testing of digital components.
- 7 Describe the term 'impact assessment'.
- 8 Explain the importance of performance monitoring.
- 9 Describe the term 'efficiency tests'.
- 10 Explain the purposes of usability/audience testing.

Core element 12: Tools



In this core element you will learn about a range of digital tools that can make tasks easier to complete. Digital tools include programs, websites and online resources that can be used at home and at work. These can be used to:

- present information to others
- collaborate on projects and document creation
- organise and participate in meetings with other people

as well as providing the opportunity to interact with people in general.

Learning outcomes

In this core element you will learn about:

- 12.1** The application of digital tools and methods in a business context

- 12.2** The applications of collaborative communication tools and technologies in business

12.1 The application of digital tools and methods in a business context

Presentation tools

Presentation tools are software programs that utilise graphics, text, audio and video to accompany written or spoken presentations. They are used to aid communication with others and, if used well, help to aid the understanding of the information that has been written or spoken.

Slide/page presentation software

There is a variety of presentation software available that varies in the features and functions it provides. However, it must provide at least three essential features:

- ▶ a text editor with custom editing
- ▶ a method for inserting, editing and resizing graphics
- ▶ a method to organise and display the slideshow sequentially.

Some presentation software requires the program to be downloaded on the computer system before it can be used. Other programs can be used through a web browser, for example Prezi and Google Slides.

Presentation slides can be used for a variety of purposes and the next section looks at how they can be used within a business context.

Product demo

This is a demonstration of how a software application or a product works. It is used by people who are trying to promote their product/software to potential customers/clients. It is used to provide an overview of the product, how it works and its value. A product demo is important as it is an opportunity to get the prospective customer/client excited about the product. A presentation can include images and videos of the product working, as well as key points about the features and functions.

Sales meetings

These are meetings held internally in an organisation between members of the sales team. They are an opportunity for the sales team to discuss current sales, new products and other information which enables them to carry out their job roles effectively. Presentations can include images and videos of new

products that the sales team will be promoting, or graphs/charts about current sales figures.

Training

Presentations are a useful tool when delivering training to staff. The use of images and videos can reinforce what is being delivered. The purpose of training is to bring about change and in particular a change in behaviour. Just providing employees with an overload of information can demotivate them, but by using a variety of more engaging techniques within presentations, the training is more interesting, engaging and therefore motivates the employees to learn more effectively.

Promotion and marketing

Previously you read about the use of presentations for product demos. Promotion and marketing have many purposes that include the introduction of products and services, increasing a company's brand awareness, as well as driving sales. Presentations must be effective and include:

- ▶ attractive colour schemes
- ▶ relevance to the audience
- ▶ clear messages.

Good promotional and marketing techniques using presentations can mean the difference between getting the attention of your audience or losing your audience altogether. Promotion and marketing presentations are not just an advertisement for the marketing campaign for the product, but also include product packaging and service delivery.

The concept is the same regardless of whether the presentation is being used at an expo or other marketing events where there is the opportunity to attract customers.

Digital infographics

According to the Oxford English Dictionary, an infographic (sometimes referred to as an information graphic), is

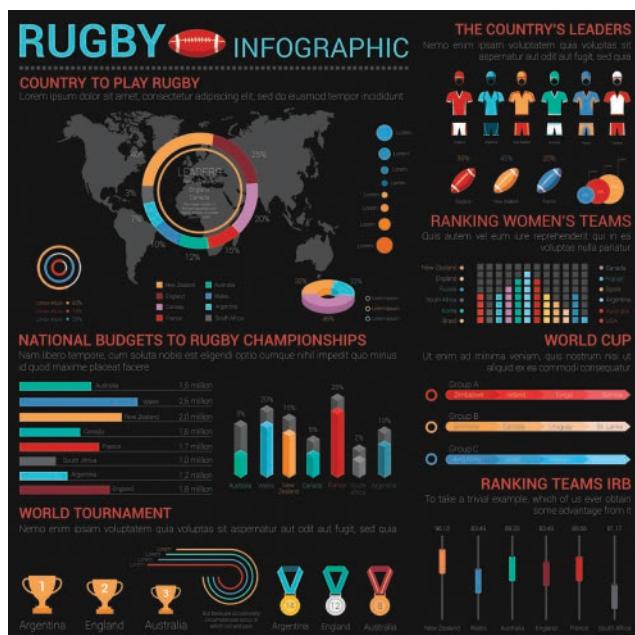
‘a visual representation of information or data’

But a digital infographic is more than that: it is a collection of images and charts with minimal text. It therefore provides an easy-to-understand overview of a subject.

Digital infographics are a valuable tool to provide visual communication, but it is important that any visual used within an infographic must help the reader to understand, as well as engage and excite them.

Posters

Do not confuse an infographic poster and an ordinary poster (sometimes referred to as an info poster). The difference between the two is based on the type of data. A poster is subjective and focuses on qualities and storytelling as opposed to quantifiable data. An infographic focuses on the quantifiable data and translates it into complex data visualisations. They therefore differ in design and purpose.



▲ Figure 12.1 An example of an infographic poster – the focus is on quantifiable data that has been presented in different ways

Research

Research different kinds of infographic posters and info posters. Consider how they are different and the information that they are being used to present. When looking at the different types of posters, ask yourselves these questions:

- ▶ Does the poster promote the story about the data? If so, this is an infographic poster.
- ▶ Does the poster promote a predetermined story/message where the data is only used as support? If so, this is an info poster.

Leaflets

This is a small sheet of printed paper that is used to present a short message clearly and concisely. Leaflets can be used by businesses to advertise their products and/or services. They are used for promoting things such as special offers, events and even the opening of a new store. They can be handed out to people face to face, for example in a shopping precinct or on the high street to people who are passing by, posted through the letterbox or stapled to a brochure or placed inside a newspaper or magazine.

Leaflets can be a cost-effective way for businesses to advertise their products and/or services and are quick to produce in-house. The most important thing about a leaflet is whether people will understand what it is saying by just giving it a quick glance.

Graphs

It is important to understand the difference between graphs and charts as the same terminology is often used to mean the same thing (and they are not). A chart presents information in the form of graphs, diagrams and/or tables. Graphs present the mathematical relationship between data sets. A graph is a type of chart – in fact all graphs are charts, but not all charts are graphs. The term chart includes a large number of methods for presenting information. Graphs are just one of these methods that presents data in a visual format.

Sales trends

Graphs are particularly useful for presenting information showing the trend of sales over a period of time. People can struggle with understanding and comparing sets of sales figures that have been presented in a written format. A graph enables the data to be presented as a visual image and is therefore more effective. Graphs are used by sales teams to present data and highlight the trends and patterns of the sales over time.

HOW TO WASH YOUR HAND



▲ Figure 12.2 An example of an info poster – here the focus is on 'telling a story' and it's not quantifiable

Market comparisons

Graphs are the ideal visualisation for presenting complex information. A graph can communicate the following types of information:

- ▶ **comparisons**
- ▶ **composition**
- ▶ **distribution**
- ▶ **relationship.**

Dashboards

Business dashboards are an information management tool. They are used to track **key performance indicators (KPIs)** and **metrics** and so on that are relevant to a business. Dashboards take their name from the car dashboard and provide a visualisation of complex data. This makes it easier for the user to establish current performance quickly.

Key terms

Comparisons: considering the positives and negatives, pros and cons, advantages and disadvantages of similar items.

Composition: the ‘makeup’ of something. In marketing terms it could be the composition of the customers: who they are and where they come from (the demographics). This helps with analysing the market a business is working in.

Distribution: in marketing terms, this is the spread of a product and/or service within the marketplace so that it has the potential for a large customer base. It involves looking at the locations where the product/service can be promoted to attract customers.

Relationship: in marketing terms, this refers to customer relationships. A graph can be used to establish the types of customers that buy certain products/services and how these products/services are purchased.

Key performance indicators (KPIs): used to monitor the critical areas of the business. A KPI is defined in the *Oxford English Dictionary* as

‘a quantifiable measure used to evaluate the success of an organisation, employee, etc. in meeting objectives for performance’.

Metrics: a quantifiable measure that is used to track and assess the status of a specific business process. Metrics are used to monitor all areas of a business.

Display/monitor key performance indicators

Sometimes referred to as a business dashboard, it provides a graphical representation of the KPIs,

metrics and measures that are used by an organisation to monitor and measure its performance against organisational objectives. This enables organisations to make business decisions based on data.

Management information

Management information dashboards are used to summarise complex data that is required to make strategic decisions within a business. It provides a clear indication of the organisation’s performance, identifies business opportunities and helps to inform the type of KPI management improvements that are required to generate more income and therefore more profit. Examples of management information systems include, inventory control, process control, HR, accounts and management reporting.

Business intelligence

These are information management and data visualisation solutions that are used to analyse current and historic data. They present easily understandable data analysis that will allow organisations to customise the information to be viewed as well as share the information with other people. The objective is to improve the strategic decisions of the organisation to help it gain a competitive edge.

Test yourself

- 1 Identify three essential features for presentation software.
- 2 Describe how presentations can be used in sales meetings.
- 3 Explain the difference between an infographic poster and an info poster.
- 4 Discuss how dashboards are used within a business context.
- 5 Explain the difference between charts and graphs.

Project management methodologies

A project management methodology is the guiding principles and processes used to manage a project effectively. The chosen methodology will define how the project team works and communicates. Therefore, the methodology that is selected will depend on the project team, the type of project and the **project scope**. Different project management methodologies have their advantages and disadvantages for different types of projects. Some are designed for speed while others are designed for more complex projects.

Key term

Project scope: a detailed outline of all aspects of a project. This will include the activities, resources, timelines and deliverables. It will also outline who the key stakeholders are, and the processes, assumptions and constraints to be taken into consideration.

Agile

Agile project management uses an iterative approach to delivering a project throughout its entire project life cycle. This means that it is a very adaptable methodology to use. Agile has several frameworks that can be used and the one selected will depend on:

- ▶ the size of the organisation
- ▶ the structure of the team
- ▶ resource availability
- ▶ stakeholder requirements.

Each framework has its own strengths/weaknesses and advantages/disadvantages. The framework that works for one team may not be the best framework for another team.

Frameworks

Scrum

This is used in the development of software that is based on iterative and incremental processes. Scrum is a fast, flexible, adaptable and effective framework. It is designed to deliver value to the stakeholders throughout the development of the project. Scrum works in a transparent environment which means that the needs of the stakeholders are satisfied through open and continuous communication, as well as collective responsibility and progress. The development begins with a general idea of what the deliverables are and a list of characteristics that are placed in order of priority that meets the requirements of the stakeholders/clients.

Scrum is carried out in blocks that are short and periodic known as sprints. Each sprint usually lasts from two to four weeks. At the end of each sprint there is an opportunity for feedback and reflection. Each sprint provides a complete deliverable that is a variation of the final deliverable that will be presented to the stakeholders/clients.

The starting point is a list of requirements (objectives) that formulates the project plan. The stakeholders/clients prioritise the requirements based on cost and value. This is how the various iterations and deliverables are determined.

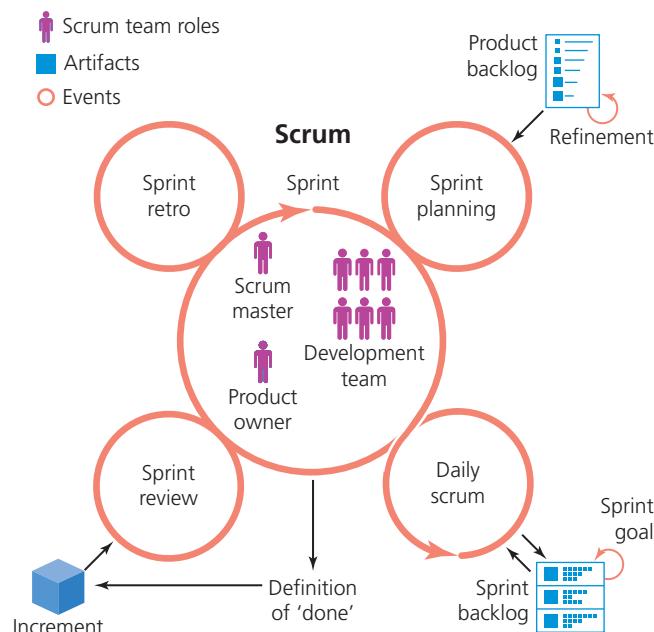
It is an easy methodology to implement and is popular because it can get results fast. Although Scrum is used primarily in software development, it is also being implemented by sales and marketing teams.

Scrum roles

The product owner – responsible for defining the work that needs to be carried out and prioritising the flow of the work. They need to know what the project deliverables are and why these are important. They act as an expert guide for the team as they work on the project. Unlike similar roles in other project management contexts, the product owner remains actively involved by reviewing and re-prioritising work based on changes and feedback. They are also responsible for communicating any changes of priorities and explaining their impacts to the project team.

The scrum master – they are classed as the protector of the team. This means that they ensure that all team members can focus on the project, and they work they are required to do without any distractions. The scrum master is the expert in relation to how scrum works and its application. They ensure that the product owner and the project development team remain within the scrum framework.

The development team – a typical scrum team consists of between five and nine people based on the requirements of the project and their individual expertise. The team will act collectively to establish how to achieve their goals based on the priorities set by the product owner. As a team they are guided



▲ Figure 12.3 The Scrum process

by the scrum process and monitored by the scrum master. Because of the level of autonomy given to the development team, it helps to create a good working relationship between them and therefore creates a positive working environment.

Sprint planning – this starts off the sprint and is used to define what can be delivered during the sprint and how it will be achieved. The product owner will describe the objective of the sprint and what backlog items will help to achieve the goal.

Daily scrum – this is a short 15-minute meeting for the development team. It is held at the same time and place every working day of the sprint. If the product owner or scrum master is involved with items in the sprint backlog, they will also participate in the daily scrum.

Sprint review – this is one of the most important meetings within Scrum. The team meet to review the completed work and determine what changes if any are required.

Sprint retro – this is a meeting that is held at the end of a sprint and is used to discuss what went well in the previous sprint cycle and what improvements can be made to the next sprint cycle.

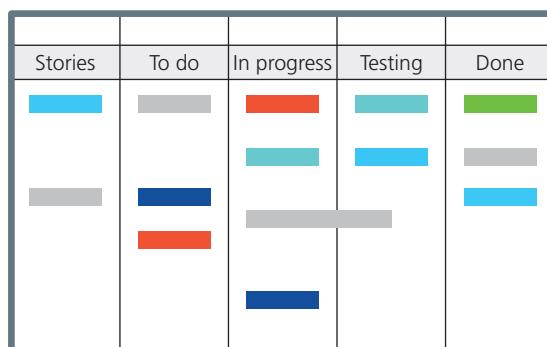
Product backlog – these are items that can be completed by the Scrum team within one sprint cycle and agreed as ready for selection during a sprint planning meeting.

Sprint backlog – is a document containing the breakdown of the deliverables to be completed during the sprint. It outlines what is required to be completed (and why) as well as how the tasks will be completed. It helps to track progress and estimate the workload of future sprints.

Kanban

The Kanban process is based on extracting work from a backlog and only completing it when it is required. This is known as the 'Just-in-Time' approach. This particular framework uses something known as the 'Kanban Board' and this is the centre of the entire process. A simple Kanban Board can consist of three columns headed 'To do', 'In progress' and 'Completed' tasks. Other columns can be added to include other steps in the workflow, for example design, development and testing. Team members move cards representing a single task or work unit into the columns depending

on what stage it is at. For example, if a task is selected from the 'To do' column, then once the work has commenced, it is moved to the 'In progress' column and so on. This provides a visual status of individual tasks. Kanban Boards can be physical boards or a digital board where team members in different locations are able to collaborate, track and manage progress in real time.



▲ Figure 12.4 A Kanban Board

Lean

Lean was originally initiated in the manufacturing industry, in particular with the Toyota car manufacturer in the 1950s. It is now part of the agile framework and is also applied in software development. The purpose of lean project management is to maximise the value while minimising the waste.

In the manufacturing process, Lean identifies three types of **waste** (commonly referred to as the 3Ms) as follows:

- ▶ Muda – activities that consume resources but do not provide an added value
- ▶ Muri – the overuse of equipment and employees
- ▶ Mura – operational irregularities that decrease productivity and efficiency.

Key term

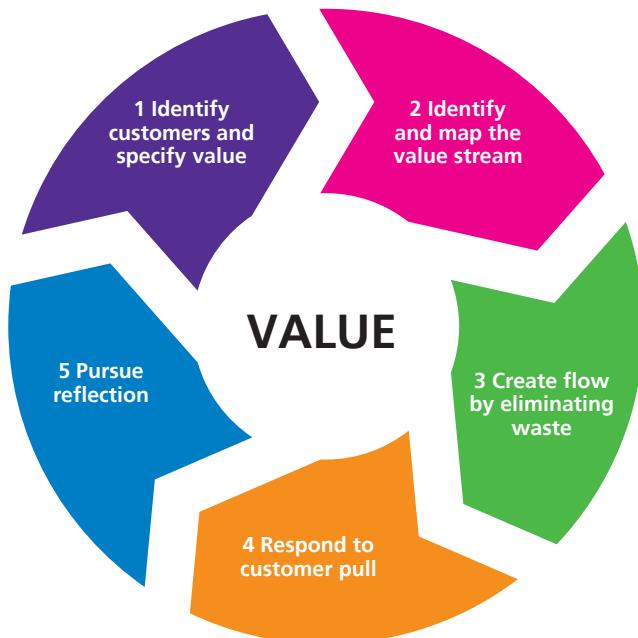
Waste: any activity that consumes resources of all types but brings no value to the end user/customer.

The purpose of lean project management is to reduce the 3Ms within the project process. Lean project management can:

- ▶ lower inventory and storage costs
- ▶ reduce overall costs
- ▶ reduce lead in times
- ▶ provide better quality
- ▶ improve efficiency and productivity
- ▶ enhance customer satisfaction.

Lean development principles can be applied to any digital environment and the practice is based on the following five principles:

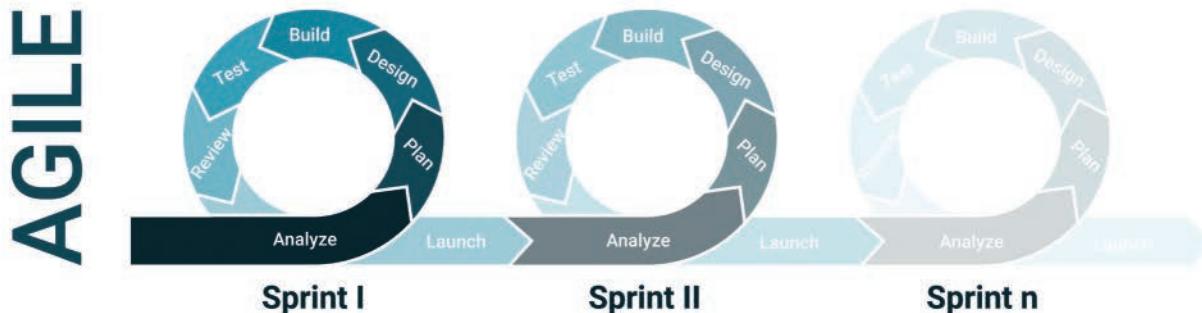
- ▶ identify customers and specify value (deliver what your customer needs as opposed to what they asked for)
- ▶ identify and map the value stream (clarifies the overall processes to identify flaws and/or unnecessary steps and eliminates them)
- ▶ create flow by eliminating waste (create a continuous flow of work processes by eliminating any unnecessary activities from the process)
- ▶ respond to customer pull (no item of work is commenced until there is a demand for it)
- ▶ pursue perfection (continuous review and monitoring of the processes and workflow to ensure that there is continuous improvement).



▲ Figure 12.5 Five principles of the Lean framework

Sprints

The term 'sprint' is used specifically in the Scrum method. As previously stated, Scrum is regular and repeatable work cycles. These cycles are known as



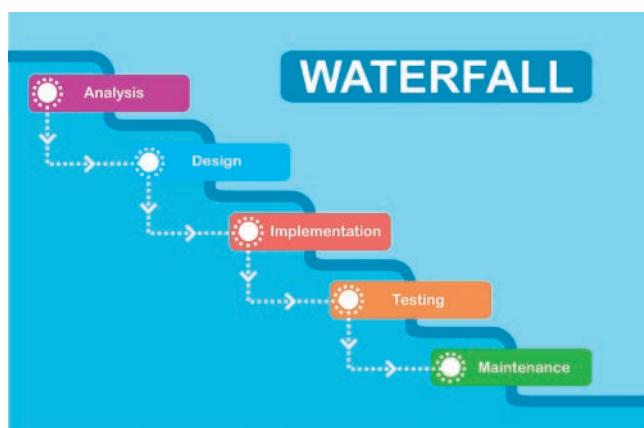
▲ Figure 12.6 The sprint framework cycle

sprints and have a limited time. Sprints are used to develop a deliverable (product) increment. Each sprint block builds on the previous sprint block. In many cases the previous developments are replaced or discarded altogether. The process is as follows:

- ▶ Each sprint begins with a sprint planning meeting where the sprint is planned in detail. The requirements are discussed from the product backlog (a prioritised list of work activities). The identified requirements are selected and decisions made on how these requirements will be met.
- ▶ The most important activity during the sprint is called the daily scrum. This daily scrum meeting is short (around 15 minutes) and is always held at the same location. This is to determine the working progress of the team.
- ▶ A sprint review takes place when the sprint is finished and the incremented product is presented to the product owner and any other interested stakeholders. A check is made that all of the sprint backlog requirements have been met, and those that have not been met will be put back into the product backlog.
- ▶ A sprint retrospective meeting is also held by the scrum team in private at the end of each sprint. This is to allow the team to reflect on what went well, what did not go so well and how things can be improved.
- ▶ Once the sprint review and sprint retrospective meetings have been held, the next sprint starts, and the process is repeated.

Waterfall

This is one of the oldest project management methodologies. This means that the first phase must be completed before moving on to the next phase. It is a very rigid structured approach for project management and there are therefore risks associated with it. It is suitable for small and simple projects or projects with fixed requirements. But it is not suitable for large, complex projects which have dynamic (constantly changing requirements, activities and/or progress) project needs.

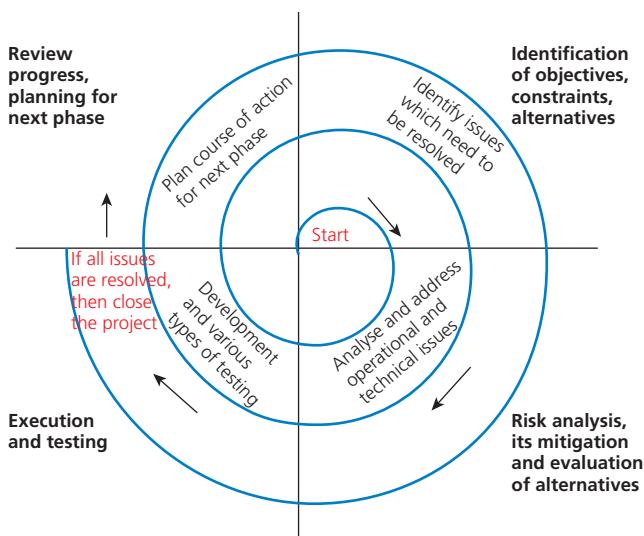


▲ Figure 12.7 Waterfall project management methodology

Spiral

The spiral methodology has an emphasis on risk analysis. There are four phases to the spiral model as follows:

- ▶ **Planning** – the requirements for the project are gathered during this stage. This can include the business requirements specification (BRS) and the system requirements specification (SRS).
- ▶ **Risk analysis** – during this phase, risks are identified and alternative solutions considered. A prototype is usually created at the end of this phase and any risks identified are addressed with alternative solutions considered and implemented.
- ▶ **Development** – the product is developed and tested during this phase.
- ▶ **Evaluation** – the customer evaluates the project at its current stage and format before the project continues to the next spiral.



▲ Figure 12.8 Spiral methodology

A software development project will repeatedly work through these phases in iterations (called spirals). The baseline spiral starts with the planning phase where the requirements are established, and risks assessed. Each of the spirals builds on the baseline spiral.

Advantages

- ▶ It is appropriate for large and critical projects.
- ▶ High-risk analysis takes place, therefore there is greater risk avoidance.
- ▶ There is robust approval and documentation control.
- ▶ Further functionality can be added at a later stage.
- ▶ For software development, the software is produced earlier.

Disadvantages

- ▶ The risk analysis requires a lot of expertise.
- ▶ The success of the project is dependent on the risk analysis phase.
- ▶ It can be a costly method to use.
- ▶ It is not suitable for small projects.

Rapid application development

This is an agile project management strategy which is very popular in software development. It has the benefit of providing a fast project turnaround time. The faster turnaround time is because the rapid application development (RAD) methodology minimises the planning staging and concentrates on the prototype development stage. This allows project managers and stakeholders to measure progress and communicate in real time on issues that arise or changes that need to be made. The result is greater efficiency, faster development and effective communication. There are four main phases as outlined below.

Planning

This is like a project scoping meeting but not so large. It is, however, still critical for the overall success of the project. The clients (software users), developers and other team members discuss the expectations and goals for the project as well as any possible problems and how they could be addressed. This stage therefore involves:

- ▶ analysing the current problem (which may require a degree of research)
- ▶ defining the project requirements
- ▶ finalising the project requirements with the approval of every stakeholder.

Everyone involved in the project must have the opportunity to evaluate the expectations and goals for the project and make their views known. It is important that each key stakeholder, developer and team member approve the project, the requirements, the goals and the expectations to avoid any miscommunication and changes that could prove costly further on into the project life cycle.

Design

This is the stage where the development begins through a series of prototype iterations. The clients work with the developers to ensure their needs are being met throughout the design process. The gathering of feedback on working models means that they can be adjusted and improved. RAD emphasises the use of software and user feedback over strict planning and requirements recording. This enables a developer and client to work together and use their experience to make sure that they have all aspects of the development covered. Users will test each prototype at each iteration to ensure that it is meeting expectations. Any 'bugs' in the software are resolved during the iterative process. This process enables the developer to make adjustments to the prototype until a satisfactory design is achieved.

Rapid construction

This is where the prototype that has been agreed is converted into a working model. The majority of issues and changes have been carried out during the iterative design phase. Therefore, developers can construct the final working model more quickly. This phase consists of a number of steps as follows:

- ▶ preparation for rapid construction
- ▶ program and application development
- ▶ coding
- ▶ unit, integration and system testing.

The software development team work together to ensure that everything is working as intended and that the end product (deliverable), meets the clients' objectives and expectations. This is an important phase because the clients continue to provide input throughout the process. They can suggest changes, alterations or new ideas that can solve any problems that may arise.

Cutover

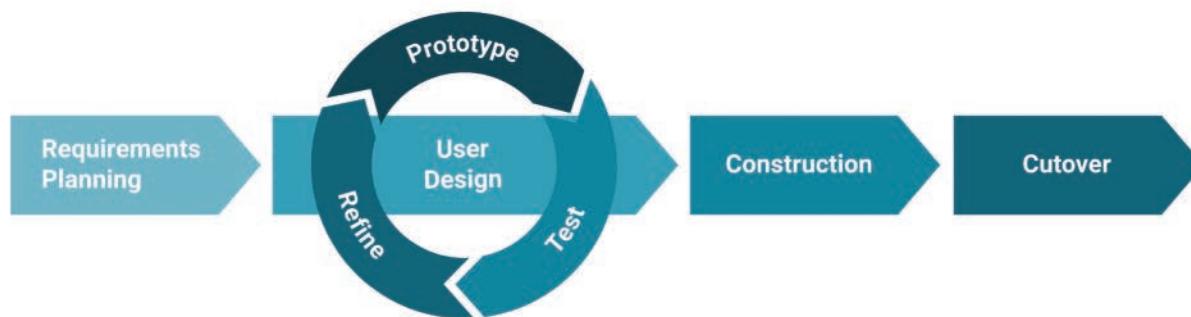
This is the implementation phase where the finished product (deliverable) is launched. This can include data conversion, testing and changeover to the new system, as well as training for the end users. Final changes are made while the software is monitored and issues arise.

Advantages

- ▶ The project can be broken down into small tasks that are easy to manage.
- ▶ Because the project is task-orientated, the project team's efficiency can be optimised by assigning tasks according to team members' expertise.
- ▶ Clients receive their working product (deliverable) in a short timeframe.
- ▶ The efficiency of the design and build process is improved by continuous communication and feedback between all interested parties.

Test yourself

- 1 Compare the agile frameworks, Scrum, Kanban, Lean and Sprints.
- 2 The Waterfall methodology is suitable for large and complex projects. True or false?
- 3 What framework has columns representing 'To do', 'In progress' and 'Completed' as a minimum?
- 4 Explain the spiral methodology.
- 5 Discuss the stages of the RAD methodology.



Rapid Application Development (RAD)

▲ Figure 12.9 Rapid application design (RAD) methodology

Project management tools and their applications

Gantt charts

In order for a project to be completed successfully, a large number of activities must be controlled to ensure that they are carried out on schedule. If a deadline/milestone is missed for the completion of a task, then the task becomes out of sequence. This can have an impact on the rest of the project. The delivery of the final product (deliverable) could be delayed, and this may increase the overall cost of the project. A Gantt chart is useful for seeing quickly everything that must be completed, as well as when it must be completed by. Gantt charts provide all this information visually. All the tasks associated with the project are outlined and in order of sequence against a timescale.

There are three main relationships between the sequential tasks in a Gantt chart. These are:

- ▶ **Finish to start (FS)** – FS tasks cannot start before a previous related task is finished. They can, however, start later.
- ▶ **Start to start (SS)** – SS tasks cannot start until the previous task has been started. They can, however, start later.

- ▶ **Finish to finish (FF)** – FF tasks cannot end before the previous task ends. They can, however, end later.

There is also **Start to finish (SF)** but this is rarely used.

Flowcharts

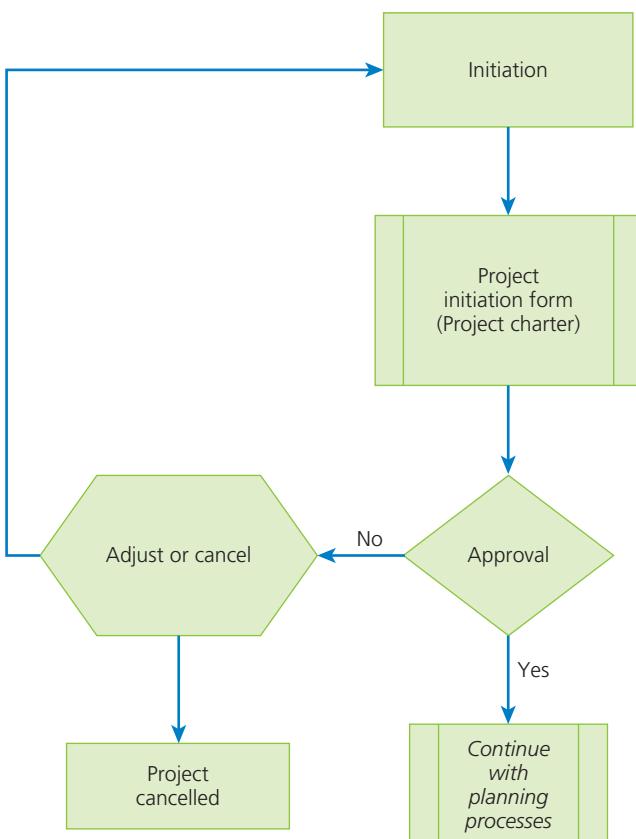
A flowchart is a specific kind of visual display that is made up of geometric shapes that are connected by lines and arrows. They represent processes, workflows, systems or computer algorithms. The visualisation of a step-by-step process and so on helps the reader to better understand what must happen and the sequence. The benefits of using flowcharts include:

- ▶ **visual clarification** – a single document can be used to show complex processes and sequences
- ▶ **simplified communication** – it is a useful way to communicate and document how a process works
- ▶ **efficient co-ordination of events** – it shows the sequence of events and this helps to prevent taking unnecessary steps that waste time and resources
- ▶ **effective analysis** – because a flowchart shows the step-by-step sequence of a process and the action required, it can highlight the less obvious flaws that can arise.

PROJECT TIMELINE INFOGRAPHIC TEMPLATE



▲ Figure 12.10 Image of a Gantt chart



▲ Figure 12.11 Flowchart for the initiation phase of the project life cycle

Stakeholder power–interest matrix

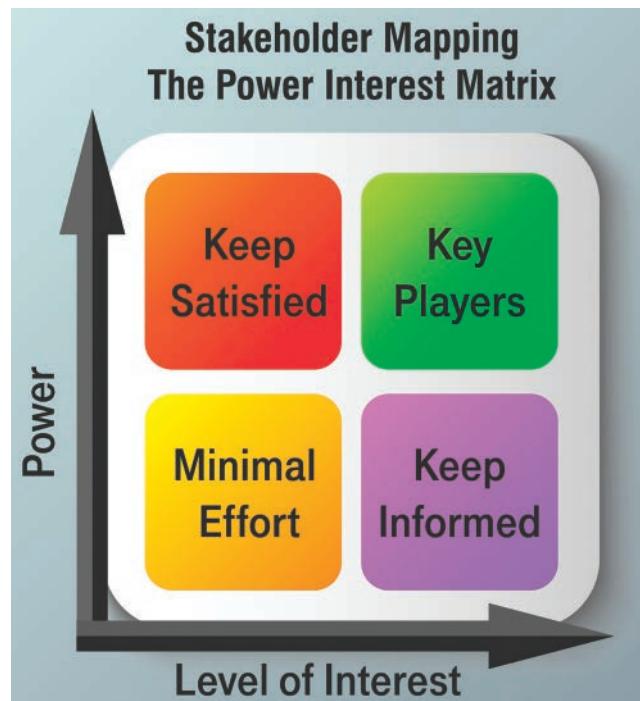
This is used to analyse a project stakeholder's power and interest in a project. This helps to determine the actions that are required to ensure their goals are aligned with the project. There are two variables that can have an impact on a project and these are power and interest.

- ▶ **Power** – this is the ability of the stakeholder to stop or change the project.
- ▶ **Interest** – this is the size of the overlap between a stakeholder's goals and the project's goals.

These two variables are plotted onto a graph with the *x* axis for the interest and the *y* axis for the power. The simple graph in Figure 12.12 provides a very good analysis of the stakeholder's interaction with the project.

- ▶ Stakeholders with high power and high interest are key stakeholders. They are heavily invested in the project and must be actively managed.
- ▶ Stakeholders with high power and a low interest must be kept 'satisfied'. They can cause problems over minor issues.

- ▶ Stakeholders with low power and a high interest must be kept informed and can cause problems if they do not get what they want.
- ▶ Stakeholders with low power and low interest must be monitored carefully but with minimal effort. It is important to note if they become more powerful, as they can have a future impact on the project.



▲ Figure 12.12 Stakeholder power–interest matrix

Budget sheets

A project without a budget is like a computer without any power. A budget is essential to start a project and get the wheels in motion. Creating a project budget is an essential part of any project.

A project budget is a combination of the costs of all activities, tasks and milestones that the project must fulfil. It is the total amount of money required to complete the project and it should be approved by all stakeholders.

The project budget is created during the initiation phase of a project that is continually monitored until the project is complete. There are at least three reasons why a project budget is so important:

- 1 It is an important mechanism to secure project funding. A project budget will inform the stakeholders of the amount of finance that is required to complete the project and when this finance is required.

- 2 A project budget plan is a tool used to control the cost of the project. It enables the project manager to measure the actual cost of the project against the approved budget. It provides an overview of what money has been spent and how much of the budget remains. The project budget plan will indicate how the project is progressing and if any changes to the original plan are required.
- 3 Project budgets can have a direct effect on an organisation's financial viability. When the feasibility of a project is calculated and the resource constraints are considered, a project budget will improve the overall success of the project.

Planning the costs of projects is an essential activity when developing a project budget. It is important to create a list of items that are relevant to the project and the costs that need to be considered. Table 12.1 includes some of the more common project cost categories that should be considered.

Project category	Example
Travel	Travelling as part of the project
Human resources	Salary for members of the project team
Materials	Can include software, hardware and any other materials required for the project
Research	Research costs as part of project delivery
Professional services	Legal advice, consultants, market research companies, etc.
Capital expenditure	Equipment/technical upgrades as part of the project
Training	Can be staff training or for members of the project team and includes workshops, conferences, external training expertise
Contingency reserves	Provides flexibility and reduces potential risk of budget overruns; usually about 5 to 10% of the overall budget

▲ **Table 12.1** Common project cost categories to be considered

Evaluation tools

Tools fall into two categories:

- **quantitative** – tools used to measure how many, how much, how big and so on.
- **qualitative** – tools used to measure things like awareness, attitude, appreciation characteristics and qualities.

Marketing analytics tools

These are tools that collect and measure marketing data that is used to improve performance. It could be to improve the performance of a website, an app or a social media page.

Search analytics

This is the use of data to research particular customer interactions. It is used by website owners to review their performance on search engines and improve their presence. Search analytics includes things such as volume trends and analysis, reverse searching (this is entering websites and looking at their keywords), keyword monitoring, search results, website comparisons, advertisement spending and so on.

Social media analytics

This is the reviewing of data in relation to social media conversations – what the conversations mean and how they can be used. Social media analytics also includes the tracking of conversations and measuring campaigns. This enables businesses to look at how their social media activities have influenced their business results. Businesses use the data from social media analytical tools to help them make changes to their operations and direct their business decisions and strategy.

Social media analytics is not just about counting the number of likes and shares, replies, comments and link clicks. These are important, but it is also important to understand why certain social media pages get a lot of engagement from the audience, what people post on social media, the products that have a lot of images on social media pages and why this may be. Businesses can establish how customers react to their business, their products and their services. This then allows them to create marketing messages, and address any product issues and/or customer concerns.

Financial analytical tools

These are used to evaluate and interpret an organisation's financial status, and are an efficient way to ensure the organisation receives a good level of profit for the investments it makes. These tools can help to evaluate the market and ensure wise investments that can return maximum profit levels. Financial analytical tools can also be used to extract and analyse internal and external information relating to the business. These tools can be used to support a SWOT analysis. SWOT means:

- | | |
|------------------|---------------------|
| ► S – strengths | ► O – opportunities |
| ► W – weaknesses | ► T – threats. |

The economic conditions of the current state of the market are analysed by the managers within a business, using SWOT analysis. The information for the SWOT analysis is provided by various financial analytical tools.

Reporting tools

There are several types of reporting tools, for example dashboard software, data visualisation software, scorecard tools and of course report writers.

- ▶ Dashboard software was discussed previously and basically enables an organisation to produce critical reports that are important to the successful functioning of the business.
- ▶ Visualisation software converts data into a visual representation that is easier for readers to understand.
- ▶ Scorecarding relates to performance data and therefore identifies the high achievers.
- ▶ Report writers are software that enable a person to create various styles of reports in real time for businesses that have constantly changing needs.

Data mining

Data mining is a process used to analyse big sets of scattered data, to make sense of it and convert it to useful information. It does this by looking for anomalies, patterns or correlations in order to produce informative models that can predict results.

Data mining techniques include:

- ▶ Tracking patterns – recognising patterns in the data set,
- ▶ Classification – categorising the attributes of the data, allowing you to draw conclusions from the results. Categorising risk factors in to low, medium and high and being able to determine the order of priority to mitigate against the risks.
- ▶ Association – looking for the correlation between one set of attributes and another set of attributes e.g. people who bought a specific product also bought another product at the same time eg on Amazon you will see the ‘people also bought’ information.
- ▶ Anomaly/outlier detection – if there is a sudden unusual spike in the data set, it would need to be investigated to establish the reason.
- ▶ Clustering – this is similar to classification but is where sets of data are grouped based on their similarities. E.g. grouping the demographics of customers with respect to age and location.
- ▶ Prediction – modelling the data can help an organisation identify historical trends which can help to make accurate future predictions.

See Core element 3 for more on data warehouses, data cleaning and data lakes.

Test yourself

- 1 Identify the three main relationships in a Gantt chart.
- 2 Explain why budget sheets are important in project management.
- 3 Describe the term ‘data mining’.
- 4 Explain how financial analytic tools are used.
- 5 Describe how flowcharts are used in project management.

12.2 The application of collaborative communication tools and technologies in business

Communication tools and technologies

Intranet

These are private, secured networks. They are used to share information within an organisation. Intranets are used to communicate, collaborate and share documents between people within the organisation. They are useful because they enable the staff to work together regardless of their geographical location. An intranet is used to centralise information and therefore maximises productivity. Organisations use intranets to:

- ▶ improve internal communication between employees, and share organisational updates, policies and notices
- ▶ make repetitive tasks easier to complete
- ▶ improve and enhance employee engagement through minimising and centralising information that would otherwise be unavailable
- ▶ provide employees with a platform that enables them to share information
- ▶ centralise all information in one place.

There are more and more organisations becoming decentralised, with staff working in many locations. Therefore, intranets have become more and more important.

Shared workspaces

These are workstations that are accessed by remote employees, freelancers, consultants and anyone else who does not have an office space. Flexible working

and alternative working arrangements have become more and more popular. There has been an increase in the use of shared workspaces. Sometimes these workspaces are referred to as co-working spaces or virtual workspaces and can take many forms in many different environments. Some are digital spaces, while others are real spaces in buildings. Some examples of shared workspaces are explored here.

Online shared workspaces:

- ▶ **Virtual and collaborative** – these are environments that virtual workers use to communicate in real time. These can include virtual meetings, whiteboards, videos and so on.
- ▶ **Virtual and shared** – this is a simulated environment where colleagues can share information. The environment may be interactive, but it is not used in a collective manner. Instead, it is shared and used as individuals. An example is the sharing of documents on Google Drive.

On-premises shared workspaces:

- ▶ **Physical and collaborative** – these are shared workspaces/co-working spaces that are created in an office, allowing employees to work more closely together. New businesses just starting up will have shared office space as opposed to the initial costs for their own premises.
- ▶ **Physical and shared** – this involves spaces that are shared and used by multiple people but on an individual basis. This is sometimes referred to as 'hot desking'. The room may be used by several different people at different times for different reasons.

Shared documents

Document sharing is literally what it says – to share one or more documents with other people. It allows two or more people to use the internet or a piece of software to access a document at the same time. These documents can exist on a computer and be shared via a network. They can be accessed by someone in the same office or building or even in another town, city, or country. Documents can also be shared on a local network in an office, or over the internet and even in the cloud.

As you can see, there are different ways that documents can be shared – between two computers or between a computer and a server. A document that is shared between a computer and a server is uploaded to the storage area on the server. This enables it to be shared with others who have the relevant permissions to access it. People can, if they want, download the document from the server to their own computer.

Discussion threads

Discussion threads are sometimes referred to as topic threads or threaded discussions. Discussion threads refers to two things that are related. First, they are the grouping together of all comments or discussions about one topic. These are usually handled by software or a moderator. Secondly, a discussion thread can be in relation to a topic which is being discussed by a group of people. The thread is a single topic and all comments relating to that topic are listed with it.

There are several ways a single discussion thread can be grouped. Moderated sites that have posts in the same thread may not show up straight away until the moderator checks the post and approves the comment. Also, most recent posts will display first and the comments are grouped in reverse order.

Discussion threads can provide people with an option to reply to a single post in the discussion. This may be listed below the original post. Businesses will use discussion threads to interact with their customers or even for employees to collaborate and share thoughts and ideas.

Online shared storage

This is the storing of electronic data with a third-party service provider that is accessed via the internet. It is sometimes referred to as 'hosted storage', 'internet storage' or 'cloud storage'. There are numerous service providers offering online data storage. Some will only store particular types of data, for example photographs, music or data backups. Others will allow the storing of any type of file/data. These service providers will usually offer a small amount of storage for free, with a fee for additional storage capacity. The fee is usually paid on a monthly or annual basis.

One of the biggest benefits of online storage is that the data can be accessed from any location in the world on any number of devices that have internet access. It simplifies the transference of data among devices and means that files can be shared between different users. This is particularly useful for businesses. Online data storage is also an advantage when it comes to backing up data and disaster recovery situations. This is because the data is stored off-site and online. In natural disasters such as fire, flooding, earthquakes and so on on-site backups could well be damaged (and in many cases would most certainly be damaged). Online backups via data storage will not be affected unless, of course, there is natural disaster that is widespread across the country/world.

Many people do have concerns about the security of online data storage and some service providers have

experienced significant **outages** (although this only happens occasionally). Therefore, this also leads to concerns about the reliability of online storage. Most online storage facilities provide enhanced security measures and automated backup capabilities to ensure that the data is never lost. Online data storage is easier for sharing and transferring data.

Key term

Outage: the temporary suspension/stopping of an operation which can be due to power failures and/or system failures.

Mark-up

There are several meanings of the term 'mark-up' but they basically refer to the same thing – they are comments and tracked changes within a document/file. This is so that the changes made can be tracked when modified by several people.

Track changes

This is used to keep track of what has been added and/or deleted from a document. Document additions are usually displayed in colour and underlined. Deletions are also displayed in colour with a strikethrough. They are particularly useful when several people are collaborating on a document. It enables each team member to see what changes have been made to the original document.

Comments

These are like sticky notes that are placed in a document. They are useful when several people are working on a document. It is easier to ask a question or leave a comment for other members of the team to see rather than inserting those comments and/or questions into the flow of the document. There are usually options to be able to reply to the comments and have a discussion around them.

Video conferencing

This is a method of visual communication. It facilitates face-to-face, live communication without the need for people to travel to the same location. Think of an organisation with offices around the world which needs to hold a meeting with its managers. There is no need for people to start flying to one location – they can still have their meeting but by video conferencing instead. However, the organisation must remember the difference in time zones between countries and how

good the internet access is in different countries. Many businesses also conduct meetings with their customers who are in different countries using video conferencing facilities. As with everything, there are the advantages and disadvantages.

Features of video conferencing can include:

- ▶ **Chat software** – this is a useful feature if there are issues with bandwidths which can hinder the video and/or audio calls. People can use the 'chat box' to communicate that is also a secure environment. The additional bonus is that the chat logs can be saved.
- ▶ **Application sharing** – this allows multiple participants to interact by viewing documents, diagrams etc even without the specific software that create the file on their computer. It supports collaborative working in the same way that face-to-face communication does.
- ▶ **File transfer** – this allows any participant within the conference to send files to another conference participants or multiple participants.
- ▶ **Electronic whiteboards** – this enables participants to draw or type on the board and/or upload images, diagrams and/or documents. A participant can also highlight specific areas of an image or diagram or sections within a document.

There are a lot of video conferencing tools available, and many have additional features that can benefit different organisations. Examples of video conferencing software includes Skype; Microsoft Teams, Cisco Webex and Zoom.

Advantages

- ▶ **Cuts costs** – reduces travel and accommodation costs incurred by companies. Businesses can interact with employees and clients and share screens, files, documents, audio and video.
- ▶ **Improved productivity** – employees can discuss problems and seek advice from a person without delay and therefore work is not held up waiting for someone to 'come and see you'. It prevents the communication gap and therefore reduces the potential for any issues and delays in the work.
- ▶ **Fewer time barriers** – although people in different countries may be in different time zones, there are also time barriers that are reduced due to video conferencing. This is because there is no delay in waiting for people to travel from location to location. This therefore provides a more continuous workflow.
- ▶ **Reduced effect on environment** – fewer car/train/plane journeys are made.

Disadvantages

- ▶ **Technical issues** – there could be a malfunction with the hardware or software that could reduce or hinder the functionality of video conferencing, or even stop it working altogether. Skilled technicians are usually required to address any problems and this can delay the work and add a maintenance charge to the organisation's budget.

- ▶ **Financial strain** – installing a video conferencing system can be expensive and place a financial burden on some smaller organisations. The technology is not always cheap and requires regular maintenance.

Project practice

You work for a software development company and you have been asked to present information to interested stakeholders to promote the company as a developer of apps for mobile technology. The stakeholders are interested in the following information about your company, as well as the types of products you create:

- ▶ What project management methodology will your company use and why?
- ▶ What project management tools will you be using and how will you share them with the stakeholders?
- ▶ How will you have regular meetings with the stakeholders to keep them up to date when they are from different countries?
- ▶ What evaluation tools will be used to see how successfully the apps are performing against

the selected success criteria, and how will the information be presented?

The stakeholders live in different countries.

Prepare a report for your manager detailing the following:

- ▶ What information are you going to provide to the stakeholders in answer to their questions above?
- ▶ How are you going to present this information to the stakeholders as they will need something to take away and read?
- ▶ How are you going to have this initial meeting with the stakeholders and what will you need to consider?

Assessment practice

- 1 Explain the purpose of a product demo.
- 2 Describe how graphs can be used to present market trends.
- 3 Describe the Kanban project management methodology.
- 4 Explain the purpose of project management methodologies.
- 5 Discuss the advantages and disadvantages of video conferencing.
- 6 Explain the purpose of balance sheets in project management.
- 7 Describe the term 'online storage'.
- 8 Describe the term 'Sprints'.
- 9 Explain how discussion threads could be used in a business environment.
- 10 Discuss shared workspaces and how they can be used in a business environment.

Core skills

During your study for the T level qualification you will need to demonstrate a range of core skills. Some of these core skills will be demonstrated through your Employer Set Project (ESP).

The core skills you will need to demonstrate will depend on the route you are taking. The routes are:

- ▶ Digital Business Services (DBS)
- ▶ Digital Support Services (DSS)

It does not matter which pathway you are following in the Digital Support Services route as the core

skills are the same for the Digital Support and the Digital Infrastructure & Network Cabling routes.

Each core skill will have links to the route core underpinning knowledge.

Demonstration of each core skill will also provide evidence for the General Competencies in English, Maths and Digital. These general competencies are the same for the DBS and DSS routes and are shown in the following table.

General English		General Maths		General Digital	
GEC1	Convey technical information to different audiences	GMC1	Measuring with precision	GDC1	Use digital technology and media effectively
GEC2	Present information and ideas	GMC2	Estimating, calculating and error spotting	GDC2	Design, create and edit documents and digital media
GEC3	Create texts for different purposes and audiences	GMC3	Working with proportion	GDC3	Communicate and collaborate
GEC4	Summarise information/ideas	GMC4	Using rules and formulae	GDC4	Process and analyse numerical data
GEC5	Synthesise information	GMC5	Processing data	GDC5	Be safe and responsible online
GEC6	Take part in/lead discussions	GMC6	Understanding data and risk	GDC6	Controlling digital functions
		GMC7	Interpreting and representing with mathematical diagrams		
		GMC8	Communicating using mathematics		
		GMC9	Costing a project		
		GMC10	Optimising work processes		

Digital Business Services

There are six core skills for the DBS route. These are:

- CS1** Working with stakeholders to clarify and consider options to meet requirements
- CS2** Research and investigate relevant sources and data to meet requirements
- CS3** Apply a valid approach to solving data problems, identifying and resolving issues while recording progress and solutions to meet requirements
- CS4** Ensure that actions identify and mitigate risk to security
- CS5** Communicate information clearly to technical and non-technical stakeholders
- CS6** Reflect and evaluate their own performance and understand the need for continuous learning and development

CS1 Working with stakeholders to clarify and consider options to meet requirements

This core skill links to the knowledge in five of the route core elements. These areas are:

- 1** Business context
- 2** Culture
- 8** Legislation
- 9** Planning
- 12** Tools

Part of any job role in the digital industry is to work with internal and/or external stakeholders. In working with these stakeholders you may be asked to consider their requirements and present options, one of which can be selected. Part of the option selection process will be to elicit specific requirements. This is to ensure that the options you present will fully and completely meet the requirements.

As part of this process, data will need to be collected, entered, processed and analysed in line with the relevant standards, guidelines and legislation. As options are formulated it is important that any discussions are fully and correctly documented to form an audit trail. The option process will also include discussions with stakeholders. How these discussions are carried out will depend on the type of stakeholders the discussions are being held with. This may take the form of an informal or a formal discussion and, during this discussion, the type of language and technical terms will need to be considered.

It is likely that following the option formulation process, and following discussions, one of these options will be selected. To ensure that the option is the correct one and meets the specified needs, an informed decision needs to be made. An informed decision can only be made when all the data and information have been presented. The data and information could include budget and timescales, risks and the cultural impact of the option.

When you are completing the ESP it is likely that specified requirements will be presented, data will need to be collected in the form of research and any communication required will be defined as formal or informal.

The demonstration of this core skill will also provide evidence for general competencies in English, Maths and Digital. These are shown in the following table.

General English	General Maths	General Digital
GEC1	GMC2	GDC1
GEC2	GMC5	GDC3
GEC3	GMC10	GDC5
GEC6		

CS2 Research and investigate relevant sources and data to meet requirements

This core skill links to the knowledge in four of the route core elements. These areas are:

- 3** Data
- 7** Learning
- 8** Legislation
- 11** Testing

When carrying out most tasks in the digital industry, data will need to be gathered to provide data and information to be able to consider options and to substantiate any final decisions.

The starting point will be the specified requirements which will be provided by stakeholders or management. Research will have to be carried out to provide the data and information needed. It is important that the sources of the data and information are valid and reliable and show limited, if any, bias. When selecting sources to gather the data and information required, it is very important that the relevant standards, guidelines and legislation are fully and completely complied with.

When sources have been identified and selected, the required data and information need to be gathered. Searches will have to be carried out to identify the data and information that will meet the specified requirements. It is important that the search criteria used provide relevant data and information. If the search criteria are incorrect or not complete then the data and information located will be irrelevant for the purpose or incomplete. Incorrect and irrelevant data is not useful and could lead to incorrect decisions being made.

The data and information located will need to be validated and verified to ensure that any conclusions are correct and not misleading. As with many other tasks in the digital industry, it is important that any discussions are fully and correctly documented to form an audit trail.

In your ESP you will need to carry out a research task. Information will be provided about the research you need to carry out. It is also possible that you will be provided with data sets which you will need to interrogate, using search criteria, to elicit valid, reliable and unbiased data and information to meet specified requirement(s).

The demonstration of this core skill will also provide evidence for general competencies in English, Maths and Digital. These are shown in the following table.

General English	General Maths	General Digital
GEC5	GMC5 GMC10	GDC1 GDC2 GDC4 GDC5

CS3 Apply a valid approach to solving data problems, identifying and resolving issues while recording progress and solutions to meet requirements

This core skill links to the knowledge in seven of the route core elements. These areas are:

- 1 Business context
- 3 Data
- 4 Digital analysis
- 5 Digital environments
- 7 Learning

9 Planning

11 Testing

Most problems are not one big problem but can be broken down into component parts. The first task when faced with a problem is to identify the scope: this means finding out what the exact problem is. It is very easy to assume the scope of the problem, but this can cause issues when trying to solve the problem.

By defining the scope of the problem it is then possible to break this down into component parts. By identifying the component parts of the problem it will be possible to prioritise each component. This allows each component part to be analysed and a potential solution or fix to be found.

By identifying and prioritising problems, a plan can be formed and implemented which will then allow the already potential solutions to be implemented and tested. As with many other tasks, all components, priorities, possible and actual solutions, and the testing that has taken place, must be fully and completely documented to provide an audit trail. This can then be reused if the same problem occurs at a later date. Again, it is very important that the relevant standards, guidelines and legislation are fully and completely complied with.

In your ESP you should identify the problem or issue from the provided information and find a solution. By breaking down the problem you will be able to provide a solution that solves the problem, has an audit trail and can be communicated to stakeholders.

The demonstration of this core skill will also provide evidence for general competencies in English, Maths and Digital. These are shown in the following table.

General English	General Maths	General Digital
GEC1	GMC5	GDC1
GEC3	GMC10	GDC4

CS4 Ensure that actions identify and mitigate risk to security

This core skill links to the knowledge in four of the route core elements. These areas are:

- 1 Business context
- 8 Legislation
- 9 Planning
- 10 Security

Every digital system, including solutions to a problem or issue, can have security risks. These risks can have a huge impact on any digital system and the data and information stored on it. Any action taken, and activity carried out, relating to a digital system should minimise the security risks.

Potential risks should be identified before they begin to cause problems to the digital system, the data and information and the users. The risks can be classified as threats or vulnerabilities. Each of these can have an impact, but the impact may vary. When assessing threats and vulnerabilities the probability, as well as the impact, needs to be considered.

It is very important that all proposed actions are considered for risks including threats and vulnerabilities. Each risk should be assessed for the probability of it occurring and the impact this would have. If the probability of the risk occurring is high, then an alternative proposed action with a lower level of risk may need to be found.

If the probability is low, and the impact is minimal, then risk mitigation controls should be defined. Every risk needs to be mitigated against; this will further lower the probability and impact.

As with many other tasks, all actions, the identified risks and mitigation controls should be fully and completely documented to provide an audit trail. Again, it is very important that the relevant standards, guidelines and legislation are fully and completely complied with.

In your ESP it is likely that you will be required to justify to a specified audience the actions and decisions you have taken. You may need to assess the risks, including the probability and impact, and propose mitigation controls that can be used. It will be very important that you are able to justify, using probability and impact, the decisions you have made. You may also be required to provide details of the risk mitigation controls you have selected.

The demonstration of this core skill will also provide evidence for general competencies in English, Maths and Digital. These are shown in the following table.

General English	General Maths	General Digital
GEC3	GMC6	GDC1
GEC4	GMC10	GDC4
GEC5		GDC5

CS5 Communicate information clearly to technical and non-technical stakeholders

This core skill links to the knowledge in five of the route core elements. These areas are:

- 1 Business context
- 3 Data
- 6 Diversity and inclusion
- 9 Planning
- 12 Tools

When working with stakeholders, information will have to be provided. The stakeholders will have a range of digital knowledge, and understanding of technical terms, including abbreviations. Those working in the digital industry, as with most industries, will use a lot of abbreviations when they are talking to each other. This is acceptable as it can be assumed that the abbreviations are understood.

However, some stakeholders may have a limited level of digital knowledge and understanding of technical terms. When communicating information, the digital knowledge and understanding of technical terms will need to be considered carefully. It is important that when asked to communicate information, the requirements in terms of terminology, level of digital knowledge and whether the information is to be communicated formally or informally should be ascertained. If these requirements are not ascertained, then it is possible that the stakeholders will not understand the information which could lead to incorrect decisions being made.

The scope of how the information is to be communicated is also very important. This should, in addition to the requirements, be ascertained before any creation of the presentation of the information is started. It may be that regular communication is needed with specified methods of communication presentation being defined. A requirement relating to the content of the communication may also be provided. For example, a formal meeting may be required with a presentation, with an accompanying digital communication. It is also important that where any communication is to take place is determined, for example face to face or online, as this can also affect the communication method and contents. If the project is multi-faceted, then a formal project plan with budgetary costings may be required on a regular basis

so that the stakeholders can make informed decisions to keep the project on time and on budget.

It is important that during, and after, each time information is communicated a detailed record is kept of, for example, any comments, action points and timescales as these will need to be revisited to form an audit trail for future reference. Again, it is very important that the relevant standards, guidelines and legislation are fully and completely complied with.

In your ESP it is likely that you will be required to communicate the data and information you have been working on. The stakeholders may be identified and whether the information is to be presented formally or informally and in which format, for example an email, a report or digital slides. When you are creating the communication method you must keep referring back to the specified requirements.

The demonstration of this core skill will also provide evidence for general competencies in English, Maths and Digital. These are shown in the following table.

General English	General Maths	General Digital
GEC1	GMC10	GDC1
GEC2		GDC2
GEC3		GDC3
GEC4		GDC4
GEC6		GDC5

CS6 Reflect and evaluate your own performance and understand the need for continuous learning and development

This core skill links to the knowledge in three of the route core elements. These areas are:

- 2** Culture
- 7** Learning
- 12** Tools

After each task or project is completed, there are always things that:

- went well.
- could have been done in a different way
- or didn't go to plan.

Time should be taken for reflection and evaluation. There are some formal reflective techniques that can be used to complete this process. They are included

in section 7.3, p.177 (Types of reflection and creativity techniques and how they influence practice within the digital sector).

How often a reflective evaluation takes place will depend on the task or project. If tasks are small and similar in context, then a reflective evaluation could be carried out after a number of these tasks has been completed. What is important is that the purpose of the evaluation is determined and data and information gathered during the tasks are considered.

The reflective evaluation will need to consider your own performance and the processes that were carried out. Each process carried out during the completion of a task or project should have had expected outcomes defined. During the reflective evaluation, the expected and actual outcomes should be considered. If the actual outcomes were different from the expected outcomes, then the reflective evaluation should consider the reasons for this. It may also be appropriate to consider the tools and techniques used and how these had an impact on the actual outcomes.

The reflective evaluation will need to come to a conclusion. The conclusion should draw together everything that has been considered, including how well the tasks or project met the specified requirements. Details about what has been learned and what needs to be learned could also be considered. This conclusion will help to identify areas where learning needs to be completed and how this learning will increase knowledge and technical skills.

In your ESP it is likely that one of the tasks, probably the final one, will be a reflective evaluation. You should use one of the reflective techniques to carry out the evaluation and cover all the items provided in the ESP brief. While it is difficult to be critical of yourself, this is necessary if lessons are to be learned, which will inform future learning and development.

The demonstration of this core skill will also provide evidence for general competencies in English, Maths and Digital. These are shown in the following table.

General English	General Maths	General Digital
GEC3	GMC10	GDC4
GEC4		

Digital Support Services

There are four core skills for the DSS route. These are:

- CS1** Communicate information clearly to technical and non-technical stakeholders
- CS2** Working with stakeholders to clarify and consider options to meet requirements
- CS3** Apply a logical approach to solving problems, identifying and resolving faults, while recording progress and solutions to meet requirements
- CS4** Ensure activity avoids risks to security

CS1 Communicate information clearly to technical and non-technical stakeholders

This core skill links to the knowledge in five of the route core elements. These areas are:

- 1** Business context
- 3** Data
- 6** Diversity and inclusion
- 9** Planning
- 12** Tools

The core skill also links to two of the pathway core elements:

- 1** Careers within the digital support services sector
- 2** Communication in digital support services

When working with stakeholders, information will have to be provided. The stakeholders will have a range of digital knowledge, and understanding of technical terms, including abbreviations. Those working in the digital industry, as with most industries, will use a lot of abbreviations when they are talking to each other. This is acceptable as it can be assumed that the abbreviations are understood.

However, some stakeholders may have a limited level of digital knowledge and understanding of technical terms. When communicating information, the digital knowledge and understanding of technical terms will need to be considered carefully. It is important that when asked to communicate information, the requirements in terms of terminology, level of digital knowledge and whether the information is to be communicated formally or informally should be ascertained. If these requirements are not ascertained, then it is possible that the stakeholders will not understand the information which could lead to incorrect decisions being made.

The scope of how the information is to be communicated is also very important. This should, in addition to the requirements, be ascertained before any creation of the

presentation of the information is started. It may be that regular communication is needed with specified methods of communication presentation being defined. A requirement relating to the content of the communication may also be provided. For example, a formal meeting may be required with a presentation, with an accompanying digital communication. It is also important that where any communication is to take place is determined, for example face to face or online, as this can also affect the communication method and contents. If the project is multi-faceted, then a formal project plan with budgetary costings may be required on a regular basis so that the stakeholders can make informed decisions to keep the project on time and on budget.

It is important that during, and after, each time information is communicated, a detailed record is kept of, for example, any comments, action points and timescales as these will need to be revisited to form an audit trail for future reference. Again, it is very important that the relevant standards, guidelines and legislation are fully and completely complied with.

In your ESP it is likely that you will be required to communicate the data and information you have been working on. The stakeholders may be identified and whether the information is to be presented formally or informally and in which format, for example an email, report or digital slides. When you are creating the communication method you must keep referring back to the specified requirements.

The demonstration of this core skill will also provide evidence for general competencies in English, Maths and Digital. These are shown in the following table.

General English	General Maths	General Digital
GEC1	GMC10	GDC1
GEC2		GDC2
GEC3		GDC3
GEC4		GDC4
GEC6		GDC5

CS2 Working with stakeholders to clarify and consider options to meet requirements

This core skill links to the knowledge in five of the route core elements. These areas are:

- 1** Business context
- 2** Culture
- 3** Data

9 Planning

12 Tools

The core skill also links to one of the pathway core elements:

2 Communication in digital support services

Part of any job role in the digital industry is to work with internal and/or external stakeholders. In working with these stakeholders you may be asked to consider their requirements and present options, one of which can be selected. Part of the option selection process will be to elicit specific requirements. This is to ensure that the options you present will fully and completely meet the requirements.

As part of this process data will need to be collected, entered, processed and analysed in line with the relevant standards, guidelines and legislation. As options are formulated, it is important that any discussions are fully and correctly documented to form an audit trail. The option process will also include discussions with stakeholders. How these discussions are carried out will depend on the type of stakeholders the discussions are being held with. This may take the form of an informal or a formal discussion and, during this discussion, the type of language and technical terms will need to be considered. It is likely that following the option formulation process, and following discussions, one of these options will be selected. To ensure that the option is the correct one and meets the specified needs, an informed decision needs to be made. An informed decision can only be made when all the data and information have been presented. The data and information could include budget and timescales, risks and the cultural impact of the option.

When you are completing the ESP it is likely that specified requirements will be presented, data will need to be collected in the form of research and any communication required will be defined as formal or informal.

The demonstration of this core skill will also provide evidence for general competencies in English, Maths and Digital. These are shown in the following table.

General English	General Maths	General Digital
GEC1	GMC2	GDC1
GEC2	GMC5	GDC3
GEC3	GMC10	GDC5
GEC6		

CS3 Apply a logical approach to solving problems, identifying and resolving faults, while recording progress and solutions to meet requirements

This core skill links to the knowledge in seven of the route core elements. These areas are:

1 Business context

3 Data

4 Digital analysis

5 Digital environments

7 Learning

9 Planning

11 Testing

The core skill also links to one of the pathway core elements:

3 Fault analysis and problem resolution

Most problems are not one big problem but can be broken down into component parts. The first task when faced with a problem is to identify the scope: this means finding out what the exact problem is. It is very easy to assume the scope of the problem, but this can cause issues when trying to solve the problem. By defining the scope of the problem it is then possible to break this down into component parts. By identifying the component parts of the problem, it will be possible to prioritise each component, in a logical order. This allows each component part to be analysed and a potential solution or fix to be found.

By identifying and prioritising problems, a logical plan can be formed and implemented which will then allow the already potential solutions to be implemented and tested. As with many other tasks, all components, priorities, possible and actual solutions, and the testing that has taken place, must be fully and completely documented to provide an audit trail. This can then be reused if the same problem occurs at a later date. Again, it is very important that the relevant standards, guidelines and legislation are fully and completely complied with.

In your ESP you should identify the problem or issue from the provided information and use a logical approach to find a solution. By logically breaking down the problem you will be able to provide a solution that solves the problem, has an audit trail and can be communicated to stakeholders.

The demonstration of this core skill will also provide evidence for general competencies in English, Maths and Digital. These are shown in the following table.

General English	General Maths	General Digital
GEC1	GMC5	GDC1
GEC3	GMC10	GDC4

CS4 Ensure activity avoids risks to security

This core skill links to the knowledge in four of the route core elements. These areas are:

- 1 Business context
- 8 Legislation
- 9 Planning
- 10 Security

The core skill also links to one of the pathway core elements:

- 3 Fault analysis and problem resolution

Every digital system, including solutions to a problem or issue, can have security risks. These risks can have a huge impact on any digital system and the data and information stored on it. Any action taken and activity carried out relating to a digital system should minimise the security risks.

Potential risks should be identified before they begin to cause problems to the digital system, the data and information and the users. The risks can be classified as threats or vulnerabilities. Each of these can have an impact, but the impact may vary. When assessing threats and vulnerabilities the probability, as well as the impact, needs to be considered.

It is very important that all proposed actions are considered for risks including threats and

vulnerabilities. Each risk should be assessed for the probability of it occurring and the impact this would have. If the probability of the risk occurring is high, then an alternative proposed action with a lower level of risk may need to be found.

If the probability is low, and the impact is minimal, then risk mitigation controls should be defined. Every risk needs to be mitigated against; this will further lower the probability and impact.

As with many other tasks, all actions, the identified risks and mitigation controls should be fully and completely documented to provide an audit trail.

Again, it is very important that the relevant standards, guidelines and legislation are fully and completely complied with.

In your ESP it is likely that you will be required to justify to a specified audience the actions and decisions you have taken. You may need to assess the risks, including the probability and impact, and propose mitigation controls that can be used. It will be very important that you are able to justify, using probability and impact, the decisions you have made. You may also be required to provide details of the risk mitigation controls you have selected.

The demonstration of this core skill will also provide evidence for general competencies in English, Maths and Digital. These are shown in the following table.

General English	General Maths	General Digital
GEC3	GMC4	GDC1
GEC4	GMC6	GDC4 GDC5

ASSESSMENT

Types of assessment

This qualification is assessed in several ways.

► Core Component:

- two written examinations
- employer-set project (ESP)

About the Core Component assessment

As shown above, there are three assessments for the core components of the NCFE T level Technical Qualification in:

- Digital Business Services (DBS)
► Digital Support Services (DSS).

There are two traditional exams (Papers A and B) and an externally set core project (ESP). Each of the three components will contribute a different percentage weighting towards your final core component grade.

Component	Percentage (%) weighting	
	DBS	DSS
Paper A	35	34
Paper B	35	41
ESP	30	25

Exams

Digital Business Services

Each of the two exam papers covers different core elements.

	Paper A	Paper B
Section A	Context (R1) Culture (R2)	Testing (R11) Tools (R12)
Section B	Digital environments (R5) Diversity and inclusion (R6)	Legislation (R8) Security (R10)
Section C	Learning (R7) Planning (R9)	Data (R3) Digital analysis (R4)

Each exam lasts for 2 hours and is worth 100 marks, plus 6 marks for quality of written communication (QWC). This equals 106 marks in total. You will be

► Occupational Specialist Component:

- synoptic assessment

told on the front of the question paper which questions have the QWC marks allocated to them.

This may sound like a long time, but time goes very quickly when you are doing an exam.

Digital Support Services

Each of the two exam papers covers different core elements.

	Paper A	Paper B
Section A	Context (R1) Culture (R2)	Careers within the digital support services sector (P1) Communication in digital support services (P2) Fault analysis and problem resolution (P3)
Section B	Digital environments (R5) Diversity and inclusion (R6)	Testing (R11) Tools (R12)
Section C	Learning (R7) Planning (R9)	Legislation (R8) Security (R10)
Section D		Data (R3) Digital analysis (R4)

Paper A lasts for 2 hours and is worth 100 marks, plus 6 marks for quality of written communication (QWC). This equals 106 marks in total. You will be told on the front of the question paper which questions have the QWC marks allocated to them.

Paper B lasts for 2 hours 30 minutes and is worth 125 marks, plus 6 marks for quality of written communication. This equals 131 marks in total. You will be told on the front of the question paper which questions have the QWC marks allocated to them.

This may sound like a long time, but time goes very quickly when you are doing an exam.

Exam command words

All exam questions use a command or keyword, such as 'identify' or 'describe'. You must recognise these because the words determine what you are required to do to be awarded the allocated marks. The allocated marks are shown in [] usually at the end of the question.

These words determine what is required so if you understand their demands, it will help you to formulate your answer.

The main command/keywords are detailed below.

State, give, identify

You should answer these questions with a single word or phrase. These questions are low demand and are usually worth 1 mark per answer required. For example:

Identify **two** different types of testing. (2)

Some of these types of questions will need a specific number of answers. In the example question, you will see that the two is in bold. This means you need to provide two answers. There may be numbers 1 and 2 on the answer lines to help you structure your answer.

Describe

This is moving to a higher level of demand. These answers are usually allocated 2 marks, but sometimes more. If a context is given in the question, you need to provide an answer that matches this context.

Identify and describe

Identify and justify

Identify and explain

These questions are asking you to do two steps in your answer. The first step is to identify, and the second step is to describe, justify or explain what you have just identified.

Justification means giving reasons for your identification.

You need to provide a correct identification before you can be considered for the marks allocated for the rest of the question. For example:

Identify **one** layer in the TCP/IP model
explaining its function. (4)

In the example question, the number **one** is in bold. This means you have to identify one TCP/IP layer. If this answer is correct, then your answer explaining the function of this layer can be considered for marks. In this example question, the explanation would be worth 3 marks.

Explain

This is moving to a higher level of difficulty than a describe question. These questions can be allocated 2 or 3 marks, but sometimes more. If a context is given in the question, you need to provide an answer that matches this context. For example:

Explain **one** benefit and **one** drawback of connecting devices to form a network. (6)

This question requires an answer that focuses on a benefit and a drawback of connecting devices to form a network. There are 6 marks available for this whole question. Therefore, it is logical to assume that 3 marks are available for the benefit and 3 marks for the drawback. You may find the words 'benefit' and 'drawback' on the answer lines. As with numbers, this will help you to structure your answer.

Compare

For this command/keyword you will need to write about the two different alternatives provided in the question.

The most common mistake on 'Compare' questions is to write about one of the alternatives in one paragraph and the second alternative in a different paragraph. To be considered for the marks available it must be clear that you have made comparisons. Use words such as: 'however', 'and', 'but'.

Discuss/evaluate/analyse

These command/keywords require a structured extended answer. They can be allocated 6 to 12 marks. Depending on the question, you may need to consider different viewpoints and ideas, as well as strengths and weaknesses or benefits and drawbacks.

The question may ask that two different aspects are specifically included in the answer; to maximise the marks for this it is important that you include both aspects.

An analysis requires an answer that breaks down an idea, usually provided in the question, into component parts. Each component part will need to be considered before a conclusion is reached.

These types of questions will be marked using a Levels of Response mark scheme. This means you will get marks for the depth of your answer and the application of the knowledge and understanding to the context of the question.

Examples

In some questions you may be asked to provide an example in your answer. In this case there is a high probability that the example will have a mark(s) allocated to it. It is important that any example you provide in your answer must be appropriate to the context of the question.

If the question context was that of security of a college and an example was required, an example relating to health would not be appropriate and you would not gain the allocated mark(s) for the example.

There are **other types of questions** that may be included in either of the exam papers. Some of these types are outlined below.

Tables

You may be asked to complete a table in either of the exams. It is important that you answer in the appropriate area of the table. Examiners will only award marks if the answer is in the correct place. Each correct answer in a ‘complete the table’ question is generally worth 1 mark.

Diagrams

You may be asked to draw a diagram, for example a flowchart, in the exams. It is probably best to stop and think before you start to draw the diagram. It is also important to draw the diagram asked for in the question. If you make a mistake, then either cross it out neatly or start a new diagram on the additional pages or extra paper available.

Exam hints and tips

- ▶ Always read the instructions carefully, that is what is the command/keyword asking for, for example identify, select, state, describe, explain, discuss, analyse, evaluate, justify and so on.
- ▶ Concentrate on one question at a time and ask yourself the following:

- Do I understand what the question is about?
 - How many marks is the question worth? You should try to work to one minute per mark.
 - How many parts are there to the question?
 - Can I provide a well-constructed answer?
 - How am I going to answer the question?
 - Do I need to include examples?
 - Do I need to relate my answer to a particular context?
 - Do I need to use technical terminology?
- It is important that the person marking your paper can not only read your handwriting but can also understand what it is you are trying to tell them. If they cannot read it or understand it, they cannot award you marks.
- If you make a mistake, cross it out neatly and then start again. There may be extra pages at the back of the exam paper, or you can ask for extra paper. If you use the extra pages or paper, then you must make it clear where your answer can be found.
- When you have finished answering the questions, and if you have time, go back over your answers. Read carefully what you have written and ask yourself:
- Have I answered the question?
 - Have I answered all parts of the question?
 - Have I met the demands of the command/ keyword, for example have I explained?
 - Have I used the correct technical terminology?

Core component project (ESP)

The core component project is externally set and focuses on creating a solution for a business. This project is referred to as an Employer-set Project – ESP. Which ESP you will complete will depend on your route and specialism.

Each ESP will provide a context, with each task having a brief. You may be provided with data files which can be used during the completion of the assessed tasks. For example, you may be provided with an email template, specification documents or relevant data set(s).

Digital Business Services (Data Technician) ESP tasks

The ESP for the Data Technician route includes a familiarisation task and five assessed tasks.

There are five assessed tasks which will need to be completed, as shown in the table below.

Task number	Focus	Number of allocated hours	Marks allocated
1	Planning a project	3	18
2(a)	Characteristics of data	2	12
2(b)	Data	4	20
3	Presentation of data	4	22
4	Reflective evaluation	2	8

Each task will have a brief. You will be told if you are able to access any web pages during the controlled hours allocated for any of the tasks. You will be able to use offline versions of any software to produce your evidence.

Each task brief will include a section relating to the outcomes needed for submission. These are the outcomes that are needed so that your evidence can be assessed. You will be told which file format to use when saving your evidence. You will also be told the filename convention which must be used when you save your evidence to your assessment evidence folder.

It is vitally important that you follow these instructions and do not deviate from them at all. If you fail to follow the instructions on the submission of your evidence, your evidence may not be marked.

Pre-release task

The pre-release task will be issued a maximum of three weeks before you start work on the assessed tasks. The aim of the pre-release task is to enable you to complete research relating to the industry sector the business is included in. You will be given a task brief which provides details about the business and the business sector. The brief will also provide details about different areas that should be considered during your research.

There is no time limit for completing this task, but it needs to be submitted to your tutor one week before you start Task 1.

This pre-release task will enable you to become familiar with the ways that digital tools and technologies are used in the industry sector.

You will need to carry out research during the time allocated for completion of this pre-release task. You will be able to access the internet and make notes about the results of your research.

When carrying out the research, it is important that you do not get distracted and just focus on the business sector that the ESP is applicable to. One strategy you could use to focus your research is to read the brief and then plan what needs to be covered in your research.

The brief will provide an overview of the business and the digital system that will be the focus of the assessed tasks. It is probable that the aims and requirements of the digital system will also be provided in the brief. There may also be some suggested considerations provided in the brief.

The aims, requirements and suggested considerations should be the starting point for you planning your research.

You are not required to submit for assessment any of your findings from your research, but you do need to submit the results to your tutor. These are some guidelines that need to be complied with:

- ▶ The results of your research should be a maximum of four A4 pages, excluding references.
- ▶ The research should be in word-processed format using Arial font, size 12pt, in black, and within standard border sizes.
- ▶ The references should clearly show the sources, including quotes, that have been used to support your ideas and opinions.
- ▶ The results of your research should be saved in a PDF format and a declaration of authenticity will need to be signed to confirm the results of your research are your own work.

Task 1 Planning a project

Task 1 focuses on planning the project. You will be given a task brief which will provide information to help you complete this task and the outcomes that are required. You will be provided with further information that will help you to create the required planning outcomes. It is very important that you read all parts of the task before you start to plan. When planning, it is important that you consider all relevant information. You may be provided with files to help you create and present your outcomes.

You will be able to use the research you carried out in response to the pre-release task. You will be able to access the internet while carrying out Task 1. The websites you are able to access are only those which will help to produce the required output for this task. A copy of your internet history will be included in the evidence for this task.

There are 18 marks available for this task, 2 of which are allocated for your English skills.

You may need to draw on the knowledge you developed while studying areas R9 Planning and R12 Tools, and the knowledge, skills and understanding of the core content of your specialist pathway.

There will be two main requirements for the planning including:

- ▶ using a project management tool, for example a flowchart
- ▶ a rationale which explains the judgements you made, the potential risks and issues, justifications for the decision you made with examples linked to the scenario.

There are 3 hours allocated for the completion of Task 1. So, a good starting point to ensure you do not run out of time could be to allocate 1.5 hours to each requirement. Each requirement of Task 1 has different marks allocated. The marks allocated to each requirement for Task 1 are shown in this table.

Requirements	Marks allocated
Project planning	8
Rationale	8
English skills	2

It is probable that the project management tool to be produced will be given in the brief. These tools may include:

- ▶ budget sheets
- ▶ critical path analysis (CPA)
- ▶ flowchart
- ▶ Gantt chart
- ▶ programme evaluation review technique (PERT)
- ▶ stakeholder power–interest matrix.

When you are using a project management tool you will need to break down the specified requirements given in the context. You should consider all details given and ensure that the output is clear, complete and specific to the given context. It may be that to make the output appropriate for the specified audience, colour, a key and a clear-to-read font should be considered and used where appropriate.

When creating the output, it is important that the rules for creating the project management tool are followed correctly and fully.

Rationale

When you are selecting any options, you will need to be able to justify your choice as this justification will

form part of the final part of this task – the rationale. The form the rationale should take will be specified in the task. For example, the rationale may take the form of a document or an email.

The rationale will explain the planning decisions you took, including justifications. When developing your rationale for the decisions you made during the planning you need to consider:

- ▶ the order of tasks/project considerations
- ▶ any project dependencies that need to be considered
- ▶ the potential risks and issues that may arise as a result of your decisions.

There are 2 marks allocated for your English skills. To maximise your English marks you should consider:

- ▶ the consistent and accurate construction of complex sentences
- ▶ correct spelling, grammar and punctuation.

Task 2(a) Characteristics of data

Task 2(a) focuses on characteristics of data and how it can be used in business. As with Task 1 you will be given a task brief which contains the task's requirements and the required outcomes. It is, again, very important that you read all parts of the task. This is to help you understand what is required from you and how to present your outcomes.

You will be able to use the research you carried out in response to the pre-release task. You will not be able to access the internet while carrying out this part of Task 2.

You may need to draw on the knowledge you developed while studying area R3 Data, and the knowledge, skills and understanding of the core content of your specialist pathway.

There will be one main requirement for this part of Task 2:

- ▶ the characteristics and application of data you would need given the requirements in the brief.

There are 2 hours and 12 marks allocated for this part of Task 2.

You will need to produce an output which includes:

- ▶ the fundamental characteristics of data including examples relevant to the context
- ▶ how the data can be used, including examples that are relevant to the context
- ▶ how the data meets the needs of the context
- ▶ a justification of why the decisions you have made meet the specified needs of the context.

The characteristics of data you may be asked to consider include:

- ▶ type
- ▶ sources (internal or external)
- ▶ storage (on premises or cloud).

What is important is that you select the relevant characteristic(s) of data that meet the requirements of the brief. You should also be able to justify how the data can be used and applied.

While completing this part of Task 2, it is important that you keep referring to the brief. By doing this you can check that you are meeting the defined requirements which will help when you are completing your justification.

Task 2(b) Data

Task 2(b) focuses on characteristics of data and how it can be used in business. As with previous tasks you will be given a task brief which contains the task's requirements and the required outcomes. It is, again, very important that you read all parts of the task brief. This is to help you understand what is required from you and how to present your outcomes.

This task will be completed on a date set by NCFE. You will be able to use the research you carried out in response to the pre-release task. You will be able to access the internet while carrying out this part of Task 2. The websites you are able to access are only those which will help to produce the required output for this task. As with Task 1, a copy of your internet history will be included in the evidence for this task.

You may need to draw on the knowledge you developed while studying area R3 Data, and the knowledge, skills and understanding of the core content of your specialist pathway.

It is likely that you will be provided with data sets which can be used to complete this task.

There will be three main requirements for this task:

- ▶ cleansing provided data and producing a data model
- ▶ processing, and outputting, provided data sets to create a new data set to meet the needs of the business, including variables/queries/formats
- ▶ defining the technical actions taken during the processing and analysis of the data including the selection of data types, to meet the defined requirements of the context.

There are 4 hours allocated for the completion of Task 2(b). So, a good starting point to ensure you do not

run out of time could be to allocate 1 hour 15 minutes to each requirement. This will provide 15 minutes 'wiggle room'. There are 20 marks available for this task. Each requirement of Task 2(b) has different marks allocated. The marks allocated to each requirement for this part of Task 2 are shown in this table.

Requirements	Marks allocated
Cleansing and data model	6
Creation of a new data set	6
Rationale	8

The initial data set to be cleansed will contain errors. It is important that you look for any errors which are present in the data set. These errors could include data type or format errors. The data modelling tool you may be asked to create includes:

- ▶ entity relationship diagram (ERD)
- ▶ data flow diagram (DFD).

As in previous tasks, when the output required is a diagram, it is important that the rules for creating the data modelling tool are followed correctly and fully. For example, if an ERD is required then the diagram should include:

- ▶ primary key(s)
- ▶ foreign key(s)
- ▶ cardinality
- ▶ attributes.

When combining and analysing the data sets it is important to review the specified requirements. It is probable that you will need to combine data sets that have been sourced internally and externally. You may need to select different parts of the data sets to enable you to output data and information which are relevant.

You may also need to use statistical methods to, for example, identify trends and patterns and correlate the data. The data should be outputted in a format that meets the specified needs and the target audience.

The rationale you produce will need to be specific and targeted at the end user as defined in the brief. You will need to demonstrate, when creating your rationale, your understanding, and the appropriateness, of the analysis and processing of the data sets and how this informed your output format. You will also need to consider why you selected the data included in the output to form the new data set.

Each part of your rationale will need to consider the specified requirements of the brief and how the output is relevant to each requirement.

Task 3 Presentation of data

Task 3 focuses on communicating a message to a specified target audience. As with previous tasks you will be given a task brief which contains the task's requirements and the required outcomes. It is, again, very important that you read all parts of the task. This is to help you understand what is required from you and how to present your outcomes.

You will be able to use the research you carried out in response to the pre-release task. You will be able to access the internet while carrying out this task. The websites you are able to access are only those which will help to produce the required output for this task. As with Tasks 1 and 2(b), a copy of your internet history will be included in the evidence for this task.

You may need to draw on the knowledge you developed while studying area R3 Data, and the knowledge, skills and understanding of the core content of your specialist pathway.

It is likely that you will be provided with the data sets which you created in Task 2 and these can be used to complete this task.

There will be one requirement for this task:

- ▶ to produce a specified digital communication to provide information about your data analysis to a specified target audience.

There are 4 hours allocated for the completion of Task 3. There are 22 marks available for this task which includes 2 marks for your English and 4 marks for demonstrating digital skills. The marks allocated to each part of Task 3 are shown in this table.

Requirements	Marks allocated
Presentation of data	16
English skills	2
Digital skills	4

Your digital communication should be written in a way that is appropriate for the specified audience. This may be a technical or non-technical audience. The language and technical terms you use should be appropriate to the audience. The language and technical terms should also be in context for the message of your digital communication. Any examples used should also be in context.

The construction of the communication should also be appropriate for the specified message. It may be that a

range of components can be used. This could include, for example:

- ▶ data tables
- ▶ graphs and charts
- ▶ images and graphics
- ▶ infographics
- ▶ maps
- ▶ text.

It is probable that the content of the digital communication could include:

- ▶ how data analytics can be used, including advantages and disadvantages with relevant examples
- ▶ the impacts on external and internal stakeholders, including key factors that could influence decisions
- ▶ how your solution meets the needs of the context, including consideration of potential risks, mitigations and implications.

It is important that any digital communication meets the standards required. For example, if digital slides are produced then these should:

- ▶ use a template to ensure the layout is consistent including background, headers and footers, colours and text font
- ▶ make appropriate use of transitions
- ▶ have an appropriate amount of text on each slide – there should not be too much
- ▶ have a consistent level of readability.

There are 2 marks allocated for your English skills. To maximise your English marks you should consider:

- ▶ the consistent and accurate construction of complex sentences
- ▶ correct spelling, grammar and punctuation.

There are 4 marks allocated for your digital skills. To achieve these marks you need to demonstrate that you can use the technical features of the application. To maximise your digital skills marks you should consider:

- ▶ inputting the data in a relevant and appropriate way
- ▶ labelling features, for example graphs, to support communication
- ▶ ensuring that the design features used, for example colour, font size and so on, increase accessibility
- ▶ using appropriate file types for any components.

Task 4 Reflective evaluation

Task 4 focuses on a reflective evaluation. As with previous tasks you will be given a task brief which

contains the task's requirements and the required outcomes. It is, again, very important that you read all parts of the task. This is to help you understand what is required from you and how to present your outcomes.

You will be provided with the evidence you created for previous tasks. This means that you can refer to this and use examples from your evidence in your reflective evaluation.

It is likely that you will be provided with a template which can be used to complete this task.

You may need to draw on the knowledge you developed while studying area R7 Learning.

The areas that need to be included in your reflective evaluation may be provided to you in the brief. It is also probable that the target audience who will read your evaluation will also be provided.

There will be one requirement for this task:

- ▶ a reflective evaluation.

There are 2 hours and 8 marks allocated for this task.

The reflective evaluation should be written in a way that is appropriate for the specified audience. This may be a technical or a non-technical audience. The language and technical terms you use should be appropriate to the audience. The language, technical terms and examples should also be in the context of the brief and the evidence you have produced.

You will need to select a reflective technique to use when you are creating your evaluation. The techniques you could select include:

- ▶ Kolb's experiential learning cycle
- ▶ Gibbs' reflective cycle
- ▶ Boud, Keogh and Walker's model.

Your reflective evaluation should consider:

- ▶ your understanding of the specified requirements
- ▶ the actions you carried out and the tools and techniques you used to achieve the aims, requirements and outcomes
- ▶ how well your proposed solution has met the needs of the brief
- ▶ your performance, including what you have achieved and what you found difficult including the need for further learning continuous professional development (CPD).

Digital Support Services (Digital Support) Assessed tasks

There are four assessed tasks which will need to be completed. These are shown in the table below.

Task number	Focus	Number of allocated hours	Marks allocated
1	Troubleshooting and test plan	2 hours 30 minutes	22
2	Interview and communication	2 hours 10 minutes	12
3	Project proposal	4 hours	24
4	Post-project review	3 hours 30 minutes	12

In addition to the marks shown in the table, marks will be available for the demonstration of Maths and English skills. These, and the tasks that the marks are attributed to, are shown in the table below.

Skill	Task(s)	Marks available
Maths	3	2
English	2, 3 and 4	4

Each task will have a brief. You will be told if you are able to access any web pages during the controlled hours allocated for any of the tasks. You will be able to use offline versions of any software to produce your evidence.

Each task brief will include a section relating to the outcomes needed for submission. These are the outcomes that are needed so that your evidence can be assessed. You will be told which file format to use when saving your evidence, and the filename convention which you must use when you save your evidence to your assessment evidence folder.

It is vitally important that you follow these instructions and do not deviate from them at all. If you fail to follow the instructions on the submission of your evidence, your evidence may not be marked.

Task 1 Troubleshooting and testing

Task 1 focuses on troubleshooting a fault based on a specified set of problems and issues and designing a test plan. You will be given a task brief which will provide information to help you complete this task and the outcomes that are required. You will be provided with further information that will help you to diagnose the fault. It is very important that you read all parts of the task before you start to troubleshoot the fault. When planning your troubleshooting, it is important that you consider all relevant information. You may be provided

with files to help you create and present your outcomes. This task will be completed on a date set by NCFE.

You will be able to access the internet while carrying out Task 1. The websites you are able to access are only those which will help to produce the required output for this task. A copy of your internet history will be included in the evidence for this task.

You may need to draw on the knowledge you developed while studying area R11 Testing, and the knowledge, skills and understanding of the core content of your specialist pathway.

There will be two requirements for this task:

- ▶ a troubleshooting document in response to a specified fault
- ▶ a test plan document.

There are 2 hours 30 minutes allocated for the completion of Task 1. So, a good starting point to ensure you do not run out of time could be to allocate 1 hour 15 minutes to each requirement. Each requirement of Task 1 has different marks allocated. The marks allocated to each requirement for Task 1 are shown in this table.

Requirements	Marks allocated
Troubleshooting document	6
Test plan	16

You will need to diagnose the fault and record your steps to rectify (troubleshoot) the specified fault. It is important that you consider which troubleshooting framework and tools you will use during the troubleshooting process. It is also important that all technical aspects are included with the correct use and application of technical language. The troubleshooting document could include:

- ▶ user details
- ▶ test dates
- ▶ computer specification and software
- ▶ proposed tests
- ▶ expected outcomes of tests
- ▶ record of diagnosis.

The test plan you create must be full and complete. The audience for the test plan will be provided to you in the brief. The test plan should be logical in structure and order of tests. The test plan could include:

- ▶ administrative details including dates, name of tester
- ▶ test date
- ▶ hardware and software specifications
- ▶ actual and relevant tests to be carried out in a logical order including, where relevant, diagrams/images

- ▶ full and complete details of expected outcomes
- ▶ remedial action required.

Task 2 Interview and communication of information

Task 2 focuses on an interview to elicit information and the communication of the results of your interview to a specified audience.

You will be given a task brief which will provide information to help you complete this task and the outcomes that are required. You will be provided with further information that will help you to plan your questions for the interview.

You will be able to access the internet while carrying out this task. The websites you are able to access are only those which will help to produce the required output for this task. A copy of your internet history will be included in the evidence for this task.

You may need to draw on the knowledge you developed while studying area R11 Testing, and the knowledge, skills and understanding of the core content of your specialist pathway.

There will be two requirements for this task:

- ▶ an interview to elicit information
- ▶ communication of your findings to a specified audience.

Each requirement of Task 2 has different marks allocated. The marks allocated to each requirement for Task 2 are shown in this table.

Requirements	Marks allocated
Interview	6
Communications	6

There are 2 hours 10 minutes allocated for the completion of this task. You will be allocated an interview time. The interview will take 10 minutes. The hour before your interview time is for you to investigate the issues and problems and formulate your questions. The questions must be based on the information provided in the brief. It may be that you are able to consider the root cause analysis (RCA) process when you are constructing your questions and the order you will ask them in. An audio recording of your interview will form part of your evidence for this task.

After your interview, you will be allocated 1 hour to produce the communication(s) as detailed in the brief. It is likely that you will be provided with a template to create your communication(s).

When you are compiling your interview questions, you will need to consider specific requirements that are directly linked to the brief context. The questions should follow a logical order and be relevant. The language you use in your questions should be appropriate to the person you are interviewing. Details about this person may be provided in the brief. You should aim to elicit all the information from the interview to help you create the communication(s) as required by the brief.

When you are conducting your interview, you may need to consider:

- ▶ active listening
- ▶ use of different types of questions, for example open and closed
- ▶ use of clear and concise language including any technical terminology.

The communication(s) should be targeted at the audience defined in the brief. This means that the language used, including technical terms and style (formal/informal) should be appropriate to the technical knowledge of the audience. The communication(s) should be relevant to the context of the brief and demonstrate problem solving and analytical thinking across all the issues and solutions you elicited during your interview.

Task 3 Project proposal

Task 3 focuses on a project proposal to meet a specific need.

You will be given a task brief which will provide information to help you complete this task and the outcomes that are required. You will be provided with further information that will help you to create your project proposal.

You will be able to access the internet while carrying out this task. The websites you are able to access are only those which will help to produce the required output for this task. A copy of your internet history will be included in the evidence for this task.

You may need to draw on the knowledge you developed while studying areas R5 Digital environments and R10 Security.

There is one requirement for this task:

- ▶ a project proposal.

There are 4 hours allocated for the completion of this task. This task will be completed on a date set by NCFE. You may be provided with files to help you create and present your outcomes.

You will need to consider the information provided in the brief and any further files provided when creating your project proposal. When creating your project proposal, you should consider:

- ▶ the current specified issues
- ▶ how these issues can be solved and the impact this will have on the context
- ▶ any hardware, software and cloud services that may be required to implement your proposal, including justifications for your decisions
- ▶ the costs of implementing your proposed solution (fixed and ongoing)
- ▶ how your solution can be implemented
- ▶ any potential cyber security issues and how these can be mitigated against.

There are 2 marks allocated for your Maths skills. To maximise your maths marks you should consider:

- ▶ the accuracy of any calculations
- ▶ the correct use of units, for example currency, number of items.

Task 4 Testing methods and project review

Task 4 focuses on creating a testing method to measure the effectiveness of your solution, and a project summary.

You will be given a task brief which will provide information to help you complete this task and the outcomes that are required. You will be provided with further information that will help you to complete this task, for example the audience, for example technical or non-technical.

You will be able to access the internet while carrying out this task. The websites you are able to access are only those which will help to produce the required output for this task. A copy of your internet history will be included in the evidence for this task.

You may need to draw on the knowledge you developed while studying areas R7 Learning and R11 Testing.

There will be two requirements for this task:

- ▶ a testing method
- ▶ a project summary for a specified audience.

Each requirement of Task 4 has different marks allocated. The marks allocated to each requirement for Task 4 are shown in this table.

Requirements	Marks allocated
Testing method	6
Project summary	6

There are 3 hours 30 minutes allocated for the completion of Task 4. So, a good starting point to ensure you do not run out of time could be to allocate 1 hour 30 minutes to each requirement which will allow 30 minutes of ‘wriggle room’.

You will have covered a range of testing methods in your course. These include:

- ▶ concept testing
- ▶ usability/audience testing
- ▶ stress testing
- ▶ penetration testing
- ▶ black box and white box testing.

When you are creating your testing method you must consider:

- ▶ the audience
- ▶ the purpose of the testing method, for example the effectiveness of the solution
- ▶ where relevant, the different types of questions that can be used
- ▶ the rules related to the testing method.

It is important that you create a testing method that elicits as much useful information about the system and that all information is relevant to the context. The areas that you need to cover in your testing method may be provided as part of the requirements in the brief.

The second part of this task is a project summary. The audience for this summary will be provided to you in the brief. The summary is just that. The summary should include:

- ▶ a brief overview of the key issues
- ▶ the proposed solution
- ▶ identified security issues
- ▶ how you mitigated against possible issues identified
- ▶ an evaluation of your own performance using a reflective model.

You will need to select a reflective technique to use when you are creating the evaluation of your own performance. The techniques you could select include:

- ▶ Kolb’s experiential learning cycle
- ▶ Gibbs’ reflective cycle
- ▶ Boud, Keogh and Walker’s model.

As this task is part of the assessment for your English skills, you should ensure that your spelling, punctuation and grammar are correct and that any technical terms are used correctly. You should also make sure that the format of the evidence you produce is professional and targeted at the target audience.

Digital Support Services (Digital Infrastructure & Network Cabling) Assessed tasks

There are four assessed tasks which will need to be completed. These are shown in the table below.

Task number	Focus	Number of allocated hours	Marks allocated
1	A tested solution to a fault	2 hours 30 minutes	22
2	Interview and communication	2 hours 10 minutes	12
3	Project proposal	4 hours	22
4	Post-project review	3 hours 30 minutes	12

In addition to the marks shown in the table, marks will be available for the demonstration of Maths and English skills. These, and the tasks that the marks are attributed to, are shown in the table below.

Skill	Task(s)	Marks available
Maths	3	2
English	2, 3 and 4	4

Each task will have a brief. You will be told if you are able to access any web pages during the controlled hours allocated for any of the tasks. You will be able to use offline versions of any software to produce your evidence.

Each task brief will include a section relating to the outcomes needed for submission. These are the outcomes that are needed so that your evidence can be assessed. You will be told which file format to use when saving your evidence, and the filename convention which you must use when you save your evidence to your assessment evidence folder.

It is vitally important that you follow these instructions and do not deviate from them at all. If you fail to follow the instructions on the submission of your evidence, your evidence may not be marked.

Task 1 Fault finding and testing

Task 1 focuses on finding a fault based on a specified set of problems and issues, and designing a test plan. You will be given a task brief which will provide information to help you complete this task and the outcomes that are required. You will be provided with further information that will help you to diagnose the fault. It is very important that you read all parts of the task brief before you start to troubleshoot the fault.

When planning your troubleshooting, it is important that you consider all relevant information. You may be provided with files to help you create and present your outcomes. This task will be completed on a date set by NCFE.

You will be able to access the internet while carrying out Task 1. The websites you are able to access are only those which will help to produce the required output for this task. A copy of your internet history will be included in the evidence for this task.

You may need to draw on the knowledge you developed while studying area R11 Testing, and the knowledge, skills and understanding of the core content of your specialist pathway.

There will be two requirements for this task:

- ▶ a configuration document in response to a specified fault
- ▶ a test plan document.

There are 2 hours 30 minutes allocated for the completion of Task 1. So, a good starting point to ensure you do not run out of time could be to allocate 1 hour 15 minutes to each requirement. Each requirement of Task 1 has different marks allocated. The marks allocated to each requirement for Task 1 are shown in this table.

Requirements	Marks allocated
Configuration document	6
Test plan	16

You will be provided with control documents that will help you to diagnose the fault, and a document to record your steps to rectify (troubleshoot) the specified fault. It is important that you consider which troubleshooting framework and tools you will use during the fault finding process. It is also important that all technical aspects are included with the correct use and application of technical language.

The test plan you create must be full and complete. The audience for the test plan will be provided to you in the brief. The test plan should be logical in structure and order of tests. The test plan could include:

- ▶ administrative details including dates, name of tester
- ▶ test date
- ▶ hardware and software specifications
- ▶ actual and relevant tests to be carried out in a logical order
- ▶ full and complete details of expected outcomes
- ▶ remedial action required.

Task 2 Interview and communication of information

Task 2 focuses on an interview to elicit information and the communication of the results of your interview to a specified audience.

You will be given a task brief which will provide information to help you complete this task and the outcomes that are required. You will be provided with further information that will help you to plan your questions for the interview.

You will be able to access the internet while carrying out this task. The websites you are able to access are only those which will help to produce the required output for this task. A copy of your internet history will be included in the evidence for this task.

You may need to draw on the knowledge you developed while studying area R11 Testing, and the knowledge, skills and understanding of the core content of your specialist pathway:

- ▶ Pathway Core element 1: Careers within the digital support services sector
- ▶ Pathway Core element 3: Fault analysis and problem resolution

There will be two requirements for this task:

- ▶ an interview to elicit information
- ▶ communication of your findings to a specified audience.

Each requirement of Task 2 has different marks allocated. The marks allocated to each requirement for Task 2 are shown in this table.

Requirements	Marks allocated
Interview	6
Communications	6

There are 2 hours 10 minutes allocated for the completion of this task. You will be allocated an interview time. The interview will take 10 minutes. The hour before your interview time is for you to investigate the issues and problems and formulate your questions. The questions must be based on the information provided in the brief. An audio recording of your interview will form part of your evidence for this task.

After your interview, you will be allocated 1 hour to produce the communication(s) as detailed in the brief. It is likely that you will be provided with a template to create your communication(s).

When you are compiling your interview questions, you will need to consider specific requirements that

are directly linked to the brief context. The questions should follow a logical order and be relevant. The language you use in your questions should be appropriate to the person you are interviewing. Details about this person may be provided in the brief. You should aim to elicit all the information from the interview to help you create the communication(s) as required by the brief.

When you are conducting your interview, you may need to consider:

- ▶ active listening
- ▶ use of different types of questions, for example open and closed
- ▶ use of clear and concise language including any technical terminology.

The communication(s) should be targeted at the audience defined in the brief. This means that the language used, including technical terms, and style (formal/informal) should be appropriate to the technical knowledge of the audience. The communication(s) should be relevant to the context of the brief and demonstrate problem solving and analytical thinking across all the issues and solutions you elicited during your interview.

Task 3 Project proposal

Task 3 focuses on a project proposal to meet a specific need.

You will be given a task brief which will provide information to help you complete this task and the outcomes that are required. You will be provided with further information that will help you to create your project proposal.

You will be able to access the internet while carrying out this task. The websites you are able to access are only those which will help to produce the required output for this task. A copy of your internet history will be included in the evidence for this task.

You may need to draw on the knowledge you developed while studying areas R5 Digital Environments and R10 Security.

There is one requirement for this task:

- ▶ a project proposal.

There are 4 hours allocated for the completion of this task. This task will be completed on a date set by NCFE. You may be provided with files to help you create and present your outcomes.

You will need to consider the information provided in the brief and any further files provided when creating

your project proposal. When creating your project proposal, you should consider:

- ▶ the current specified issues
- ▶ how these issues can be solved and the impact this will have on the context
- ▶ any hardware, software and cloud services that may be required to implement your proposal including costs (fixed and ongoing)
- ▶ a network diagram showing your proposed solution
- ▶ any network and cyber security issues and how these can be mitigated against.

There are 2 marks allocated for your Maths skills. To maximise your maths marks you should consider:

- ▶ the accuracy of any calculations
- ▶ the correct use of units, for example currency, number of items.

Task 4 Testing methods and project review

Task 4 focuses on creating a testing method to measure the effectiveness of your solution, and a project summary.

You will be given a task brief which will provide information to help you complete this task and the outcomes that are required. You will be provided with further information that will help you to complete this task, for example the audience, for example technical or non-technical.

You will be able to access the internet while carrying out this task. The websites you are able to access are only those which will help to produce the required output for this task. A copy of your internet history will be included in the evidence for this task.

You may need to draw on the knowledge you developed while studying areas R7 Learning and R11 Testing.

There will be two requirements for this task:

- ▶ a testing method
- ▶ a project summary for a specified audience.

Each requirement of Task 4 has different marks allocated. The marks allocated to each requirement for Task 4 are shown in this table.

Requirements	Marks allocated
Testing method	6
Project summary	6

There are 3 hours 30 minutes allocated for the completion of Task 4. So, a good starting point to ensure you do not run out of time could be to allocate 1 hour 30 minutes to each requirement which will allow 30 minutes of ‘wriggle room’.

You will have covered a range of testing methods in your study. These include:

- ▶ concept testing
- ▶ usability/audience testing
- ▶ stress testing
- ▶ penetration testing
- ▶ black box and white box testing.

When you are creating your testing method you must consider:

- ▶ the audience
- ▶ the purpose of the testing method, for example the effectiveness of the solution
- ▶ the rules related to the testing method.

It is important that you create a testing method that elicits as much useful information about the system and that all information is relevant to the context. The areas that you need to cover in your testing method may be provided as part of the requirements in the brief.

The second part of this task is a project summary. The audience for this summary will be provided to you in the brief. The summary is just that. The summary should include:

- ▶ a brief overview of the key issues
- ▶ the proposed solution
- ▶ identified security issues

- ▶ how you mitigated against possible issues identified
- ▶ an evaluation of your own performance using a reflective model.

You will need to select a reflective technique to use when you are creating the evaluation of your own performance. The techniques you could select include:

- ▶ Kolb's experiential learning cycle
- ▶ Gibbs' reflective cycle
- ▶ Boud, Keogh and Walker's model

As this task is part of the assessment for your English skills, you should ensure that your spelling, punctuation and grammar are correct and that any technical terms are used correctly. You should also make sure that the format of the evidence you produce is professional and targeted at the target audience.

A last note

Examiners who will mark your exam papers, and moderators who will assess the evidence you provide for your ESP, are essentially nice people who would like to give you marks. But they cannot read your mind. So, it is really important that you make sure that everything you write, in your exam and the ESP, is clear and unambiguous.

Good luck with your exams and the ESP.

Glossary

Access rights Control over what a user has access to in a digital system, for example folders, files and data/information.

Accounts payable Money that is paid out by the organisation.

Accounts receivable Money that is coming into the organisation.

Active matrix A Liquid Crystal Display screen technology that controls each pixel using capacitors. This enables the pixels to change colour and brightness more rapidly.

Active sensors Sensors requiring an external signal or a power signal.

Analogue sensors Produce a continuous output signal relating to the quantity being measured.

API A software interface that provides a service to other software. It is a connection between digital devices or between software.

Application programming interface (API) Software that enables two applications to talk to each other. Every time you use an app on your smartphone, for example Facebook or Twitter, you are using an API.

Application Specific Integrated Circuit (ASIC) A microchip designed for a specific application such as a handheld digital device or as a transmission protocol.

Autonomous system (AS) A large network or group of networks that have a unified routing policy. Every computer or device that connects to the internet is connected to an AS. This is because the internet is a network of networks.

Bias A tendency, inclination or prejudice toward or against something or someone.

Big data Very large data sets that can be analysed to produce information such as trends and patterns. Big data cannot be analysed using traditional data analysis tools.

Bilateral Trade agreements made between countries in order to promote trade and commerce. Trade barriers such as tariffs, import quotas and export restrictions are removed. This is to encourage trade and investment between the countries. While bilateral agreements can expand the available market for businesses within a country, they can also result in the closure of smaller businesses who cannot compete with much larger multinational businesses.

Black box testing The testing of the software when the internal structure and design is not known to the tester.

Bots Used by businesses online to provide answers to customers'/service-users' questions, as well as product information and suggestions for products they can buy or articles that they can read.

Bot Short for robot, this is an autonomous program that is on a network or the internet that has the ability to interact with systems or users.

Bottleneck When congestion occurs within a production system, for example a computer network or an assembly line in a factory. It occurs when the workloads arrive at such a speed that the production process has difficulty in processing them quickly enough.

Brand A type of product manufactured by a particular company under a particular name.

Brand differentiation This is what sets your brand apart from the competition. Why should customers look at your brand before others? (Think of Richard Branson and Virgin, or Jeff Bezos and Amazon.) That is brand differentiation.

Brand values These are at the centre of any brand and are incorporated into the look of the brand, the marketing content and language used, and the relationships that are built with customers through good customer service. Brand values are the beliefs that the company or individual holds as essential to delivering the products or services they provide.

Buffer Contains data stored in random access memory for a short amount of time before it is used.

Business model innovation Improving advantage and value creation by making simultaneous and mutually supportive changes to the business's value proposition to external stakeholders and its operating model.

CAA Civil Aviation Authority.

CAD Computer Aided Design.

Capital gains/losses The profits or losses from selling an asset, financial investments, real estate and so on.

Carbon footprint The amount of carbon released into the atmosphere from the activities of individuals, organisations and communities.

Cathode Ray Tube (CRT) A vacuum tube containing an electron gun at one end and a fluorescent screen at the other end.

Cloud instance A virtual server instance from a public or private cloud network. A single hardware is implemented into software and runs on the top of multiple computers. It is very dynamic and enables users to not worry about how many servers can fit onto a single hardware application causing performance issues, for example system performance degenerating at particularly busy times.

Cloud services A wide range of services delivered on demand to businesses and individuals over the internet. They are designed to provide easy and affordable access to applications and resources such as file storage, without the need for internal infrastructure or hardware.

Code of conduct A document which defines rules, values, ethical principles and vision.

Comparisons Considering the positives and negatives, pros and cons, advantages and disadvantages of similar items.

Competition law The purpose of this law is to promote healthy competition. It makes it illegal for anticompetitive agreements to be in place between two or more organisations, for example to share markets and fix prices. It also makes it illegal for businesses to abuse their dominant market position.

Composition The ‘makeup’ of something. In marketing terms it could be the composition of the customers: who they are where they come from (the demographics). This helps with analysing the market a business is working in.

Confidentiality, integrity and availability (CIA) Also known as the CIA triad.

Consumer confidence How confident consumers are in the state of the economy and their own personal financial situation.

Correlation The mutual relationship or connection where one thing affects or depends on another thing, for example the effect is dependent on the cause.

CRM Customer relationship management.

Customer touchpoints Any point of contact between a business and a customer, for example through email, call centres, websites, social media, advertisements, third-party review sites and so on.

Cyber security The practice of defending computers, servers, mobile devices, electronic systems, networks and data from malicious attacks.

Dashboard A digital interface that is used to obtain, combine and analyse data across a business. It provides

an in-depth analysis of the business as well as providing a real-time indication of the function of the different departments within the business. This can include productivity, trends and activities as well as the key performance indicators.

Data analytics The science of analysing raw information to answer specific business questions.

Data at rest Data stored on a digital device or storage medium.

Data cleaning The process of going through data looking for errors and correcting them or excluding data where errors have been located.

Data encryption software Software that is used to encrypt a file or data.

Data in transit Data being sent to one or more authorised users.

Data Over Cable Service Interface Specification (DOCSIS)

A globally recognised telecommunications standard. It supports high-bandwidth data transfer via existing coaxial cable systems that were originally used for the transmission of cable television programme signals.

Data packets Small units of data which are sent and received when accessing the internet or any other type of network.

Data redundancy This is a condition that is created within data storage technology where the same piece of data is held in two separate places. Whenever data is repeated it is data redundancy. Although it can occur by accident, it can also be done deliberately for the backing up and recovery of data.

Data silo A group of raw data accessible by one department but not available to the other departments within the organisation.

Data sprawl The vast amounts and variety of data produced by organisations on a daily basis.

Data subject The person the data is about.

Data transfer protocol (DTP) The technique used to store consecutive segments of data (e.g. a file) on different physical storage devices.

Data virtualisation Connects all types of data sources regardless of the file types and location. The data is then combined, and users can access the combined data through reports, mobile apps, websites, dashboards and portals.

DBMS Database management system.

Decomposition Breaking a complex problem into smaller sub-problems.

Deep learning An artificial intelligence function that works like the human brain. It is used to process data, detect objects, make decisions, and for speech recognition and language translation. It is able to learn without human supervision.

Demographics The characteristics of people, for example age, ethnicity and gender.

Developmental Concerned with the development of someone, something or even both.

Digital sensors Work with discrete digital data. The digital data is used for conversion and transmission.

Distributed control system (DCS) This is a system of sensors, controllers and other associated computers and technologies that are distributed across an industrial plant, for example an oil refinery. Each of the elements of a DCS serves a unique purpose. This includes data acquisition, process control, data storage and graphical displays. A DCS communicates with a centralised computer system through the industrial plant's local area network and makes automated decisions based on real-time production trends.

Distribution In marketing terms, this is the spread of a product and/or service within the marketplace so that it has the potential for a large customer base. It involves looking at the locations where the product/service can be promoted to attract customers.

Diversity The range of political beliefs, race, culture, sexual orientation, religion, class and/or gender identity differences.

Dividend payments Money paid regularly by a company to the shareholders. These are paid out from the profits of the company.

Dividend policy Contains the structure of the payouts made to shareholders based on how many shares a shareholder has and the profits made by the business.

Domain name The name of the website, for example google.com.

Downtime A period when a system is unavailable, offline or not operational. This may be an individual computer, a network, or servers.

DPP Director of Public Prosecutions.

DSE Display screen equipment.

Eavesdropping Also referred to as sniffing or snooping. Eavesdropping is when someone takes advantage of an unsafe or unsecure network in order to steal information transmitted through digital devices.

Economic recession A decline in economic activity that spreads across the entire economy and lasts more than

a few months. It can be related to income, employment, industrial production and retail sales.

Economic shifts This is a change in the structure of an economic system resulting in changes to societies, cultures and everyday life both on a national and a global level.

Elastic computing solutions Provision of variable service levels based on the changing needs of the business.

Electromagnetic interference (EMI) This is the disruption of electronic operations and electronic devices from electronic emissions. EMI travels in waves and can cause devices to malfunction (which can result in dangerous outcomes).

Embargo A government order restricting business with a specific country or the exchange of specific goods. An embargo is usually implemented as a result of political or economical issues between different countries. Embargos imposed on a country can have a serious impact on their economy.

Encapsulation Information is taken from a higher level and a header is added to it, treating the higher layer information as data. The Internet Protocol packet is then encapsulated into a layer 2 Ethernet frame. The frame is then converted into bits at layer 1 and sent across the local network.

Encryption code/key A set of characters, a phrase or numbers that are used when encrypting or decrypting data or a file.

Ethernet This is a form of communication protocol that connects computers within a network.

Ethernet adapter Also referred to as a Network Interface Card (NIC), it plugs into a slot on the motherboard. It enables the computer to access the network. Many NICs are now built into the chipsets on the motherboards of PCs and laptops as opposed to being a physical card.

Ethical hacking An alternative term for penetration testing.

Ethics Rules, actions and behaviours defining permissible actions/behaviours to address moral obligations.

External bus Sometimes referred to as the expansion bus. This is a connection between a computer and external devices.

External stakeholders Groups outside an organisation, for example shareholders.

Facial recognition software Software that can identify or confirm someone's identity using their face in a photo, video or in real time.

Field Programmable Gate Array (FPGA) An integrated circuit consisting of internal hardware blocks. The

hardware blocks have user-programmable interconnects to enable customisation of operations for a specific application.

Firmware A small piece of software that makes hardware work as intended. Firmware consists of programs that are used to make devices work. Without firmware, many electronic devices would not work at all.

Firmware Code, added at the time of manufacturing, written to a hardware device's non-volatile memory. It is the software that allows the hardware to run.

Foreign key These are used to link tables together. A foreign key is a field in one table that is linked to a primary key in a different table.

Frequency distribution An overview of all distinct values within a variable and the number of times they occur.

Green energy A type of energy that is generated using natural resources such as sunlight, wind or water. Green energy does not harm the environment by releasing greenhouse gases into the atmosphere.

Green IT This is related to the practice of environmentally sustainable computing. The aim is to minimise the negative impact of IT operations on the environment by improving the design, manufacture, operation and disposal of computers and computer-related products in a more environmentally friendly way.

Haptics Using technology to stimulate the senses of touch and motion to reproduce the sensations that would be felt by someone interacting directly with the physical object.

Hash A number generated from a string of text.

Human machine interface (HMI) A user interface that connects a person to a machine, system or device.

Hyperlink Can be displayed as an icon, a graphic or text, and links to another file or object. The World Wide Web is comprised of trillions of hyperlinks that link pages and files to one another. A hyperlink is usually displayed in blue and is usually underlined.

Hypervisor Software that creates and runs virtual machines, separating a system's operating system and resources from the hardware to allocate to the virtual machines.

ICMP Internet Control Message Protocol.

ICO Information Commissioner's Office.

Inbound traffic Comes from outside the network through the firewall into the network.

Industrial control systems (ICS) An important aspect of the operation technology sector. These are systems that are used to monitor and control industry processes, for example oil refinery cracking towers or power

consumption on electricity grids. They are extremely critical for all industry processes.

Inflation The increase in the cost of commonly used goods and services, for example food, clothing, transportation and housing. The higher the costs, the less purchasing power (money available to spend) people and businesses have.

Integrated Development Environment (IDE) A software application providing a range of functions and facilities for software development. It usually includes a source code editor, automated build tools and a debugger.

Intellectual property (IP) Creative work which can be treated as an asset or physical property. IP covers four main areas – copyright, trade marks, design rights and patents.

Intelligent software agents Autonomous programs that can be aware of and interpret data that is sensed from the environment, reflect on events in the environment and take appropriate actions to achieve identified goals without permanent input from a user.

Internal rate of return (IRR) This is the annual growth rate of an investment a business is expected to generate. In the case of a project, it is the annual increase in profits/benefits on completion of the project.

Internal stakeholders Groups within an organisation, for example owners and employees.

International Book Standard Number (ISBN) A number that uniquely identifies a book. It usually has ten digits with an 11th digit being a check digit.

Internet Protocol (IP) The string of numbers an internet service provider assigns a device, for example 192.168.1.38.

IT services The services provided by a team of IT support specialists.

Iteration Repeating steps, or instructions, over and over again until a condition is met.

ITIL Information Technology Infrastructure Library.

JSON JavaScript Object Notation.

Kernel A computer program that is the core of an operating system. An operating system has control over the computer system and therefore the kernel also has control over all aspects of the system. It is the most important component of an operating system. When a computer system starts up, the kernel is the first program to be loaded after the bootloader. This is because the kernel has to control the rest of the start-up process for the operating system. The kernel remains in memory until the operating system is shut down. It is responsible for low-level tasks such as memory and disk management.

and task management and device management. It is an interface between the user and the hardware components of the computer system.

Key performance indicator (KPI) A quantifiable measure used to evaluate the success of an organisation in meeting predefined performance objectives.

Key performance indicators (KPIs) Used to monitor the critical areas of the business. A KPI is defined in the *Oxford English Dictionary* as 'a quantifiable measure used to evaluate the success of an organisation, employee and so on in meeting objectives for performance'.

Last mile connectivity This refers to the final stage of the telecommunications network, delivery to the end user.

Latency The delay between the instruction for transfer and the start of the transfer.

Machine learning (ML) The process of getting computers to learn, think and act like humans. As with humans, computers that are implemented for machine learning will improve their learning over time due to the constant feeding of data and information from real-world situations.

Machine-to-machine (M2M) Any technology that enables networked devices to exchange information and perform actions without the manual assistance of humans. It supports the communication between systems enabling them to make autonomous decisions.

Media Access Control (MAC) This is a code in the device's Network Interface Card, identifying the physical device.

Metrics A set of numbers that gives information about a particular process or activity.

Metrics A quantifiable measure that is used to track and assess the status of a specific business process. Metrics are used to monitor all areas of a business.

Middleware Software which is 'in the middle' of the operating system and the applications working on it. It allows communication and data management for distributed applications by operating as a hidden translation. It is used to link two separate applications together.

MOOCs Massive Open Online Courses.

Morals The principles of what people believe is right or wrong.

NCSC The UK's National Cyber Security Centre.

Net present value (NPV) This is used to calculate the total value at the current time of the expected income generated.

Node Any physical device within a network that is able to send, receive and/or forward information. A computer is a node if connected to a network.

Non-governmental organisation (NGO) A non-profit organisation that is independent of government, for example an organisation which aims to address a social or political issue.

Non-linear thinking The ability to make connections and draw conclusions from unrelated concepts or ideas.

Non-root bridge Often referred to as a remote or repeater bridge. It establishes a connection to the root bridge or another repeater bridge to connect the wired local area network (LAN) to part of the bridged LAN.

Ofcom The regulator for communications services.

Operational intelligence Data analysis that enables decisions and actions to be made in business operations, based on real-time data as it is generated and collected. The data analysis process is automated and the results are integrated into operational systems for immediate use by the managerial staff and other relevant employees.

Opt-in When a person has to take a specific positive step, for example ticking a box, sending an email or clicking a button or icon, to say they consent to receiving marketing.

Opt-out When a person must take a positive step to refuse or unsubscribe from marketing.

Outage The temporary suspension/stopping of an operation which can be due to power failures and/or system failures.

Outbound traffic Comes from inside the network through the firewall out of the network.

Overheads Ongoing expenses that businesses are required to pay that are not related to the production of goods and/or services.

Packets A small segment of a larger message. Any data sent over computer networks is divided into packets. They are combined back into the larger message by the computer/device that receives them.

Pain points Issues that occur which people will work around. In some instances, they are not even aware they are happening.

Passive matrix A Liquid Crystal Display screen technology that uses a grid of vertical and horizontal wires to display an image on the screen. Each pixel is controlled by an intersection of two wires in the grid. When the electrical charge is altered at a given intersection, the colour and brightness of the corresponding pixel can be changed. Passive matrix is relatively simple and inexpensive to produce, but the disadvantage is that the charge of two wires (vertical and

horizontal) must be changed in order to change just one pixel. The response time is therefore slow. Fast movement may appear blurry or faded.

Passive sensors Do not require external power signals and directly generate an output response.

Patch Software code that can be downloaded and installed, after the software program is originally installed, to correct an issue with that program.

Permissions A list of attributes that determine what a user can do with files and folders, for example read, write, edit or delete.

Personal data Any information relating to an identified or identifiable living individual.

Point-to-multiple networks This is where a single data link is shared by more than two devices.

Point-to-point networks Sometimes referred to as P2P, this is a data link providing a path from one fixed point to another. This streamlines communication links between points.

Primary key A field in a table that allows each record to be uniquely identified. For example, every person 16 years or older in the UK has a National Insurance number. This uniquely identifies a person.

Programmable logic controllers (PLC) Industrial computer control systems that constantly monitor the state of input devices and make decisions that are based upon a custom program to control these devices. They have the ability to replicate and change operations or processes while simultaneously collecting and communicating important information.

Project scope A detailed outline of all aspects of a project. This will include the activities, resources, timelines and deliverables. It will also outline who the key stakeholders are, and the processes, assumptions and constraints to be taken into consideration.

Proportionate When it is appropriate, and no more than necessary, related to the problem concerned.

Public sector The sector that provides a range of governmental services, including infrastructure, public transport, state education, healthcare, police, fire and military services.

Qualitative data Data that is non-numerical.

Quantitative data Data that is numerical.

Quotas Imposed by the government to restrict the number/monetary value of goods that can be imported and/or exported during a particular period of time. The

purpose of quotas is to reduce imports so that there is an increase in domestic production, therefore restricting competition from other countries. Sometimes governments impose quotas when there are concerns about the quality and/or safety of products from another country.

Radio frequency identification (RFID) Tiny chips that contain information which is transmitted when near a receiver.

Radio frequency interference (RFI) This is unwanted signals in the radio frequency spectrum used by Wi-Fi networks (most commonly 2.4 GHz and 5 GHz). Some other electronic devices use the same radio waves as Wi-Fi networks. This causes the prevention of the transmission of data and can create delays and performance degradation.

Relational database A database that has relationships between the tables to reduce data duplication.

Relationship In marketing terms, this refers to customer relationships. A graph can be used to establish the types of customers that buy certain products/services and how these products/services are purchased.

Relative significance Having meaning only in relation to something else.

Return on investment (ROI) A measure used to evaluate how well an investment has performed. It is expressed as a percentage that is calculated by dividing the potential income from the benefits by the cost of the project.

RFC Request for Comments.

Risk In the context of business, risk refers to factors that could lead to the failure of the business or a drop in its profits.

Root bridge A bridge that is located at the starting point of a wireless infrastructure topology. It is usually connected to the main wired backbone local area network.

Sanctions Political trade restrictions that are implemented against specific countries, with the intention of maintaining or restoring international peace and security.

Scalability The ability of a digital system to respond to variable amounts of load (users, requests, connections, etc.) while maintaining good performance in a cost-efficient way.

Search engine This is software that is accessed via the internet which searches a database of information according to the query that has been input by the user. The search engine will provide a list of results that best match what the user is trying to find based on the search criteria that was entered. There are many different search engines available, for example Google, Yahoo, Bing and Ask.

Secure Sockets Layer (SSL) Standard technology used to keep an internet connection secure. Data that is transmitted between the user and the website (or between two systems) is encrypted and therefore impossible to read; this prevents unauthorised people from reading sensitive and personal information.

Segregation/segmentation Dividing a computer network into smaller parts.

Selection A decision or question.

Semantics The process followed when executing a program in a specific language.

Sequence The specific order in which instructions are performed in an algorithm.

Service management The activities involved in the design, creation, delivery, support and management of IT services.

Shadow data Data that is automatically generated and recorded as we use the internet.

Social engineering The art of manipulating people so that confidential information can be found out.

Socioeconomic status This is the social standing or class of an individual or groups of individuals. It can be classified based on a combination of factors such as education, income and occupation.

Software as a service (SaaS) A cloud-based service where software is accessed via a browser as opposed to being downloaded onto a network or PC.

Stakeholders Any individual, group or organisation that is impacted by the operations of an organisation. These can include customers, suppliers, employees, communities, government and even the ecosystem.

Stakeholders Anyone with an interest in a business or organisation. Stakeholders can be individuals, groups or other organisations, or businesses that are affected by the organisation's activity.

Subsidies Given to businesses in order to support an industry, where it is struggling against international competition or where the international businesses have lowered their prices so that the local businesses cannot make a profit without the subsidy.

Supervisory control and data acquisition system (SCADA) System software and hardware that enables industrial organisations to control industrial processes locally or at remote locations. It facilitates the monitoring, gathering and processing of real-time data and directly interacts with devices, for example sensors, valves, motors and pumps, through the use of human-machine interface software. It also records the events that occur in a log file.

Syntax The structure or format of data.

Tariffs Taxes that are charged on the import of goods from other countries. Thus the price of imported goods is increased to try and persuade consumers to buy products made in their own country.

Thin Film Transistor (TFT) Used in high quality, flat display Liquid Crystal Displays. There is a transistor for each pixel on the screen allowing the electrical current that illuminates the display to turn on and off at a faster rate. This makes the display brighter and motion smoother.

Trace table A tool used to test or dry run algorithms to make sure no logical errors occur while calculations are being processed. Each column represents a variable and the rows represent the numerical input and the output of the variable.

Trade mark A word, name, symbol, design, or a combination of them, used in commerce to identify and distinguish the goods of one manufacturer and/or seller from those of another manufacturer/seller. It also indicates the source of the products.

Transaction When something is added to a blockchain. Also known as an entry.

Transformational Producing a change or improvement in a situation.

Transitional The transition (movement) from one position, stage, state or concept to another.

Transport Security Layer (TSL) An updated and more secure version of Secure Sockets Layer.

Uniform Resource Identifier (URI) This is also called the internet address, web address or Uniform Resource Locator (URL) (which is a form of URI). These terms are standardised naming conventions used to address documents accessible over the internet and intranet. An example of a URL is <https://www.ncfe.org.uk>, the URL for the NCCE website.

Unique identifier A series of letters and numbers that are unique to one person.

User interface (UI) Enables a person to control a software application or hardware device in a natural and intuitive way.

Validation Checks that the data being entered into a digital system is sensible and reasonable. Checks the data against pre-set rules.

Value There are two forms of value in the business model. The value proposition made by the business of the value to the external stakeholders for accepting the digital transformation, and the business values shared with the

internal stakeholders and the benefits that the digital transformation will have for the business and for them as individuals.

Variable A value that will change usually as a result of an input or of a calculation being carried out.

Verification A check to see whether the data being entered into a digital system is identical to the source document or initial data entry.

Virtual assistants Bots that perform various tasks that include understanding the users' questions, providing relevant information and creating product descriptions. These are available 24/7 for the customers/service-users and improve their overall customer experience.

Virtualisation Using their own physical hardware, a company can create and use virtual resources such as servers, devices, or computing resources. The results are:

reduction in costs of hardware, associated infrastructure and maintenance; reduction in operating costs; reduction in downtime due to security or other risks; and improved reliability as different host machines share the load.

Warrant A document issued by a legal or government official that authorises the police or other authority to make an arrest, search premises or carry out some other action relating to the administration of justice.

Webmarking An internet link to a web page listing patent(s) which cover the product instead of marking the product itself with the actual patent number.

Work In the context of research and knowledge sources 'the work' can be an information source, for example an academic paper, textbook or electronic information source.

Index

3D printing 175–6
 5G 176–7
 abstraction 102–3, 106–7, 109–10
 access 47, 65–6, 96–8, 148, 154, 196–9,
 239
 to capital 231
 codes 239, 248, 254
 controls 56, 96–7, 248, 253–8
 to people 231
 rights 255
 accessibility 14, 49, 198–9, 271
 accountability 34
 accounts payable/receivable 16
 addiction 69, 71–2
 Adobe 196
 advertising, targeted 13, 52, 95
 adware 243
 aggregation 140
 agile methodology 283, 286
 aims 217–19
 air gaps/gapping 260, 264
 alarm systems 256
 algorithms 101–2, 107–10
 analysis 88, 92–5, 100–11, 127–8, 227,
 229, 232–3, 290–1, 298, 302
 analytics 13–14, 23, 95, 290–1
 animation 90
 anti-malware 126, 249–50
 anti-spyware 126
 anti-virus software 126, 249–50
 application layers 133, 135, 137
 application programming interface
 (API) 96–7, 184, 271
 application software 126
 Application Specific Integrated Circuit
 (ASIC) 114–15
 artificial intelligence (AI) 12–14, 39,
 171–3
 assessment 304–17
 assumptions, reasonable/documentated
 221
 audiences 11, 53, 186
 audits 34, 44, 229
 augmented reality (AR) 89, 173–4
 authentication 247
 author expertise 185
 authorisation 247
 automation 14–17, 27, 62–3, 249–50
 autonomous system (AS) 132
 backups 32–3, 148–9, 258–9

barriers 175, 256, 293
 baseline reports 223
 behaviour 21–2, 37, 64
 best practice 26–7, 155
 bias 154, 161, 185–6
 bilateral trade 6
 biometrics 257
 bit size 114
 Black, Asian and Minority Ethnic
 (BAME) 160–1
 black box testing 266, 271, 277
 block storage 80
 blockchain 174–5
 board of directors 3
 bots/botnets 13–14, 62, 241
 bottlenecks 14
 bottom-up approaches 103
 brands 11–12, 12, 17–18, 18, 25, 51, 54,
 151
 breaks, taking 190
 bridges 123
 briefs 307–16
 British Airways 196
 British Computer Society (BCS) 211–12
 British Standards Institution (BSI) 210
 budgets 43, 49, 220–1, 289–90
 buffer overflow 244
 bugs 247
 business cases 217–18
 business context 1–58, 297–9, 301–3
 business environment 5–11
 business growth 12, 35–6, 61
 business insight 20
 business intelligence 20, 282
 business loss 54
 business models 20, 27
 business rates 7
 business to business (B2B) 5
 business to customer (B2C) 5
 business to many 5
 cables 121–2, 209–10
 cache 114
 capital 4, 231
 carbon footprint 9–10, 40–1
 central processing unit (CPU) 113–15,
 117
 centralisation 42
 change 23–6
 factors driving 35–43
 management 22–35, 43, 44–5
 monitoring 44, 46, 293
 resistance to 30–1, 53, 65
 responding to 42–6
 change advisory boards (CABs) 28, 29
 change requests 28–9
 charities 2, 198
 Chartered Institute of Information
 Security (CIISec) 211–12
 chassis 113
 check digits 85
 citations 186–7
 Civil Aviation Authority (CAA) 177
 civil liberty 206–7
 clients 4, 217, 238, 271–2
 see also customers; end users; users
 clock speed 113–14
 closed-circuit television (CCTV) 256
 cloud computing 19–20, 26, 33, 79–80,
 87, 116, 144–6, 149, 292
 codes of conduct 55–7, 158–9, 211–12
 comments 293
 communication 21, 65–6, 150, 299–301,
 312–13, 315–16
 and best practice 26
 and change 43–4, 45
 channels 12, 14
 and decomposition 104–5
 face-to-face 60, 64
 formal/informal 92
 interception of 192
 and pain points 49
 and project planning 222, 224
 regarding dependencies 224
 regulation 192–3
 remote 38, 66
 synchronous/asynchronous 66
 tools for 291–4
 comparison-making 282
 compatibility 247, 271
 competition 12–13, 25
 competitive advantage 25
 competitors 4, 41–2, 76
 composition 282
 computational thinking 102–8
 Computer Aided Design (CAD) 175
 Computer Misuse Act (CMA) 1990
 194–6, 240
 computer vision syndrome (CVS) 70
 computers, quantum 168–9
 computing systems 113–18, 139–44

concept testing 275–6
confidentiality 55, 237–41
confidentiality, integrity and availability (CIA) triad 239–40, 258
configuration management 32
connectivity 154–5
consent 203–4
consumer protection 9, 197
consumer trends 37
context 186
contingency planning 227
continuous learning and development 258, 300
contracts 238
Controlling the Assault of Non-Solicited Pornography and Marketing Act 2003 – USA 205
copying 200
Copyright, Designs and Patents Act (CD&PA) 1988 199–200, 206–7
core component project (ESP) 296–304, 306–17
cores 114
cost-benefit analysis 221
cost-efficacy 62, 142–3, 146
costings 219
costs 16–17, 149, 175, 230, 293
Creative Commons 200
creativity technique 181–2
criminal law 206–7
criminals, disguised 245
crises 25
critical path analysis 232–3
cross party focus/agendas 7
cross site scripting (XSS) 242
cryptography, quantum 170
culture 8, 48, 59–72, 297, 300–1
customer bases 21
customer confidence 151
customer experience 13–15, 46, 50–1
customer profiles 48–9, 95
customer relationships management (CRM) 97
customer retention rate (CRR) 13
customer satisfaction testing 271–2
customer touchpoints 11
customers 4, 21–2, 46–52, 75, 95, 238
cyber attacks 25–6, 52, 151, 194–6, 205, 208, 241–4
cyber bullying 67–9
cyber hygiene 248
cyber security 239
dashboards 17, 90, 94, 282, 291
data 56, 73–99, 237, 297–9, 301–2, 308–10
access 96–8

accuracy reviews 272
analysis 88, 92–5, 127–8
applications 80–1, 92–6
big data 23, 76
characteristics 74–84, 308–9
collection 127–8
contiguous 138
corruption 25–6
entry 84–6, 87
error checks 85–6
formats 87–8
and the Internet of Things 127–9, 171
loss 264
maintenance 86–7
manipulation 127–8
personal 202–3, 238
presentation 89–90, 92, 310
privacy issues 63, 86
processing 81
qualitative/quantitative 92
redundancy 88, 117
regulations 194, 197–8, 202–6
research and investigation 297–8
risk mitigation 249–62
shadow 65
sources 74–7
storage 77–81, 83, 87, 151, 168, 174
testing 272, 273
transfer 151
trends/patterns 93, 94
types 74, 84–5
virtualisation 50, 140
visualisation 90–1, 92
data analytics 13, 14, 23, 95
data at rest 252, 253
data breaches 50, 52–3, 196, 198, 211, 213, 240–1, 245–6, 255
data cleaning 75
data dictionaries 82–3
data flow diagrams (DFDs) 83–4
data hygiene 248
data lakes 76
data link layers 134, 136
data mining 93, 291
data modelling 81–4
Data Over Cable Service Interface Specification (DOCSIS) 121
data packets 133–9, 141, 250
Data Protection Act (DPA) 2018 194, 197–8, 202–4, 206, 240, 248
data repositories 75
data as a service (DaaS) 79, 144–5
data silos 79
data sprawl 79
data subjects 203
data tables 90–1

data in transit 252, 253
data warehouses 75–6
database management system (DBMS) 83, 97
database as a service (DBaaS) 80
databases 77, 80, 259, relational 77, 88
deadlines 219
debt 37
debugging 272
decision making 23, 34, 95
decomposition 102–5, 107
decomposition diagrams 109
deep learning 12, 171–2
dehumanisation 62
deliverables 221, 223, 228, 230
demography 38, 155, 161–4
denial-of-service 241
departments 3
dependencies, identification 224
design thinking 181–2
developer kits 184
device hardening 147–8
Digital Business Services (DBS) 296–300, 304, 306–11
digital divide 66
Digital Economy Act (DEA) 2017 155, 196–8, 206
digital ecosystems 26
digital environments 112–52, 298, 302
digital footprints 63
digital identities 22, 65
digital manufacturing 20
digital slides 89
Digital Subscriber Line (DSL) 122
Digital Support Services (DSS) 296, 301–5, 311–17
digital system administrators 87
digital system performance 94
digital waste (e-waste) 10, 41
digitalisation 11–22
Director of Public Prosecutions (DPP) 194
directory-based structure 88
disaster recovery 33, 143, 150
discrimination 156–8
discussion threads 292
display screen equipment 71, 117–18, 190–1
dispute resolution 206
distributed control system (DCS) 128
distribution 282
diversity and inclusion 48, 153–65, 299, 301
dividends 3, 4
DNA data storage 168

- documentation 34–5
 documents 14–15, 292
 domain names 12
 downsizing 36
 downtime 27, 53, 151, 272
 drones 177
 e-learning 183–4
 eavesdropping 120
 eBay 196
 economic factors 7, 9, 37, 38, 231
 edge computing 127
 education 38, 143–4
 efficiency 14, 39, 146–7, 272
 elastic computing solutions 19–20, 145
 electromagnetic interference (EMI) 113
 Electronic Communications Privacy Act (ECPA) 1986 – USA 205
 Electronic Industries Alliance/ Telecommunications Industry Association (EIA/TIA) 209–10
 email accounts 239
 embargoes 6
 emerging technology 9, 39, 168–87
 employees 3, 15
 access controls 253–4
 access to 223, 229, 231
 and change 30–1, 44
 data 74
 and diversity and inclusion 159–60
 and health and safety 189–91
 monitoring 61, 63–4, 93–4
 and project planning 219
 retention 163
 rights 3
 salaries/perks 237
 training 258
 turnover 150
 as vulnerability 245, 248
 Employer Set Project (ESP) 296–304, 306–17
 employers 189–91
 emulation 140
 encapsulation 121
 encryption 246, 252–3, 266
 End of Life (EOL) 147, 247
 end users 3, 47–52, 54, 271–2
 enforcement 204
 engagement 47
 Enigma 105
 entity relationship diagrams (ERDs) 77, 82–3, 88
 environment 9–10, 40–1, 231, 293
 Equality Act 2010 156–9, 164
 Equality and Human Rights Commission (EHRC) 158–9
 equipment 220
 equity 37
 estimates 219, 220
 Ethernet 121–2, 141, 210–11
 ethical issues 51, 55–6, 60–7
 European Convention on Human Rights (ECHR) 201–2, 205
 European Union (EU) 40
 evaluation 290–1, 300, 310–11
 Everything as a Service 145
 evidence 186–7
 exams 304–6
 extended reality (XR) 89, 173–4
 external bus 114, 115
 extinction 25
 eye strain 70, 191
 facial recognition software 105
 facilities 219–20
 fall-open electronic locks 247
 fans 117
 fault finding 272, 314–15
 feedback 28, 81
 fibre optics 122
 Field Programmable Gate Array (FPGA) 114, 115
 files 77–9, 87–8, 126
 finance 15–17, 20–1, 29, 37, 47, 50, 74, 87, 147, 240, 294
 financial analytics 290–1
 financial contingency planning 220–1
 financial loss 25, 52, 264
 fines 54
 firewalls 126, 249–51, 262
 firmware 141, 246–7
 fiscal policy 15–16
 ‘Five Whys’ approach 274
 fixes 27–8
 flash drives 116
 flowcharts 109–10, 288–9
 forecasting 95, 220
 foreign keys 83
 foreign trade 6
 Freedom of Information Act 2000 193–4
 functionality 50, 271, 277
 funding/revenue streams 5, 37
 gambling 69, 71–2
 gaming 69
 Gantt charts 288
 Garbage In, Garbage Out (GIGO) 86
 General Data Protection Regulation (GDPR) 202–6
 government 5–6, 16, 36, 56, 76, 162–4, 197
 graphical user interface (GUI) 90
 graphics processing unit (GPU) 116
 graphs/charts 90, 94, 281–2, 288
 green energy 10, 40–1
 Green IT 142
 greenhouse gases 9–10, 40
 hacking 56–7, 192–6, 241–2
 ethical 265, 276–7
 haptics 173
 harassment 157
 hard drives 78, 116
 hardware 44, 48, 120–4, 150, 250–1
 out-of-date 147, 246–7, 259
 and project planning 220
 testing 271, 273
 hashing 253
 hazards 62
 health and safety 9, 62, 71, 189–92, 231
 Health and Safety at Work Act 1974 189
 Health and Safety (Display Screen Equipment) Regulation 1992 190–2
 heat maps 91
 honeypots 260–1
 hops 138
 human error 51, 245
 human machine interface (HMI) 128
 human resources 237
 human rights 201–2, 205
 Human Rights Act (HRA) 1998 201–2
 hyperlinks 127
 HyperText Transfer Protocol (HTTP) 130, 132
 HyperText Transfer Protocol Secure (HTTPS) 131, 267
 hypervisors 139, 142
 hypotheses 181
 identification, authentication, authorisation and auditing (IAAA) 268
 impact analysis 31–2, 272
 inbound traffic 262
 inclusivity 48–9, 153–65, 299, 301
 income 8, 38
 industrial contexts 128–9
 industrial control system (ICS) 128
 industry standards 55, 207–11
 inflation 6, 37
 infographics 91, 280–1
 information 191
 access 66, 239
 commercially sensitive 237–9
 communication 299–301, 315–16
 confidential 237–41
 management information 282
 research and investigation 297–8
 risk mitigation 249–62

- storage 168
up-to-date 34
- Information Commissioner's Office (ICO) 193, 240
- information systems 80–1
- infrastructure 16, 31, 197
- Infrastructure as a Service (IaaS) 144–5
- innovation 20, 25, 27, 39, 159, 168–87
- inputs 80, 84–5, 101, 107, 117
- Institute of Analysis and Programmers (IAP) 211–12
- Institute of Electrical and Electronics Engineers (IEEE) 210–11
- Integrated Development Environment (IDE) 184
- intellectual property (IP) 197, 200, 238
- Intellectual Property Act (IPA) 238
- intelligent software agents 62
- interfaces 273
- internal rate of return (IRR) 221
- International Book Standard Number (ISBN) 85
- International Organization for Standardization (ISO) 204, 207–8, 210
- internet 169–70, 205
- Internet Control Message Protocol (ICMP) 264
- Internet Engineering Task Force (IETF) 204, 208–9
- internet layer 138
- Internet Message Access Protocol (IMAP) 131
- Internet Protocol (IP) 120, 130–4, 137–9, 261
- internet security assurance 262–7
- Internet of Things (IoT) 127–30, 170–1
- interviews 312–13, 315–16
- intranet 291
- intrusion detection system (IDS) 251–2, 264
- intrusion prevention system (IPS) 251–2
- Investigatory Powers Act (IPA) 2016 192–3
- investment 4, 23, 63
- isolation 140
- issues management 225–7
- iteration 101, 108
- JavaScript Object Notation (JSON) 96
- job losses 54, 57, 62, 175
- 'Just-in-Time' approach 284
- Kanban 284
- kernels 124
- key loggers 243
- key performance indicators (KPIs) 17, 95, 282
- keyboards 118
- Kitemark logo 210
- knowledge 31, 49, 155, 182–7, 257
- large or medium enterprises 2
- last mile connectivity 119
- latency 176
- leadership role 219
- leaflets 281
- Lean 284–5
- learning 166–87, 297–8, 300, 302
- legal factors 9, 40, 53–4, 240
- legislation 9, 39, 188–215, 297, 298, 303
- and codes of conduct 55, 207
 - criminal law 206–7
 - and hacking 57
 - inclusion and diversity 156–9
 - industry standards 207–11
 - international requirements 204–6
 - keeping up to date with 25, 213–14
 - and payment methods 39
 - UK requirements 189–204
- licences 54, 200
- lighting 10, 40, 129–30, 190–2, 256
- Linux 124–6
- load testing 276
- local area network (LAN) 119, 211
- location 66, 258
- logical link control (LLC) 134
- machine learning 62, 128, 171–2
- machine-to-machine (M2M) 128
- mail protocols 131
- mainboards/motherboards 113
- malware (malicious software) 242–3, 249–51, 264
- managed execution 140
- Management of Health and Safety at Work Regulations 1999 190
- management information 282
- Manual Handling Operations Regulations 1992 189
- maps 91, 106
- 'mark-up' 293
- market comparisons 282
- market research 11, 21, 51, 275
- market trends 8, 37–8
- marketing 11–14, 74, 95, 203–4, 280, 290
- markets 42
- Massive Open Online Course (MOOC) 183
- Media Access Control (MAC) 120, 134
- media exposure, positive 51
- medical information 237
- mental health 68–9
- meta critic 52
- metrics 94, 282
- metropolitan area network (MAN) 119
- middleware 124, 125
- milestones 223, 228
- mixed reality (MR) 89, 173–4
- mobile technology 61–2, 271
- models 106
- modularisation approach 103–4
- mouse 118
- multi-factor authentication 239, 256–8
- multi-platform multimodal formats 47
- 'must have, should have, could have'
- (MoSCoW) 234
- National Cyber Security Centre (NCSC) 249, 265, 277
- national insurance 6
- natural disasters 246, 292
- net present value (NPV) 221
- network attached storage (NAS) 78–9
- network function virtualisation 140–1
- Network Interface Card (NIC) 121
- network interface device (NID) 121
- network interface layer 138
- network layers 133–4, 135
- network monitoring 264
- network operating system (NOS) 126
- network penetration testing 265, 277
- network protocols 130
- network segregation (segmentation) 263
- network utilisation 128
- networking reference models 132–9
- networks 64, 119–20, 264, 271
- nodes 132
- non-compliance 53, 213–14
- non-governmental organisations (NGOs) 2, 198
- non-linear thinking 172
- not fit for purpose 53–4
- not for profit 2
- object storage 79–80
- objectives 30, 36, 217–19
- occupation 8–9, 38
- Ofcom 196–7
- offline networks 264
- online sales (e-commerce) 12–13, 39
- Open Shortest Path First (OSPF) 132
- open standards 22
- Open Systems Interconnection (OSI) 132–7, 139
- operating procedures 149, 149–50
- operating systems 124–6, 140–2
- operational integrity, digital 22–8

operational intelligence 23
 operational management 95
 operations 14–17, 26–8, 42
 opportunities 147
 opt-in/opt-out 204
 optical drive 113
 order 206
 organisations 2, 9, 22–8, 49–50, 56,
 92–6, 150–1, 163–4, 172–3, 219,
 248–9
 outages 272, 293
 outbound traffic 262
 outcomes 218, 230, 272
 outputs 61, 81, 101, 107, 117
 outsourcing 4, 144
 owners 3
 packet switching 138–9
 packets 133–9, 141, 250
 pain points 49–50
 pandemics 41
 passwords 239, 242, 247, 254–5
 patches 249–50, 259
 patents 197, 199–200
 pattern recognition 102, 105–6
 payloads 139
 Payment Card Industry Security
 Standards Council (PCI SSC) 211
 payment methods 39
 peers 184
 penetration testing *see* hacking, ethical
 performance 93–4, 272, 276, 300
 peripheral component interconnect
 (PCI) 121
 peripherals 117–18
 perks 237
 permissions (privileges) 255
 personal area network (PAN) 119
 personal/professional development
 166–87
 personalisation 13, 22
 pharming 244
 phishing 244
 phone numbers 239
 physical layers 134, 136
 pilots 27
 ping tests 264
 planning 216–35, 286–7, 297–9, 301–3,
 307–8
 platform interoperability 22
 Platform as a Service (PaaS) 144–5
 point-to-multiple networks 119
 point-to-point networks 119
 policies 42, 49, 55, 150, 253–8
 political factors 6–7, 36
 pornography 205
 port scanning 266

portability 140, 145
 portable storage devices 78
 Post Office Protocol (POP) 131
 post-project reviews 45
 posters 281
 posture 70, 71
 predictive analysis 95
 premises 219
 presentation 280–2, 310
 presentation layers 133, 135
 primary keys 83
 printing, 3D 175–6
 prioritisation 43, 219, 223–4, 226, 234
 privacy issues 52–3, 63, 86, 205
 private sector 2
 probability and impact matrix 226
 problem solving 100–11, 274–5, 298,
 302–3
 procedures 55, 150, 253–8
 processes 20, 26–8, 31, 42, 83, 102–8,
 170–1, 262–6, 274–5
 processor types 115
 product demos 280
 product development 51
 product diversification 24–5
 product range 21
 product use analysis 51
 productivity 61–2, 126, 293
 products 41–2, 159–61
 professional bodies 167, 184
 professional networks 184
 professional practice 55, 56
 profiles 151
 profit margins 238
 programmable logic controller (PLC)
 128
 programme evaluation review
 technique (PERT) 232
 project communication plans 222
 project health reports 223
 project life cycle 221–4
 project management 219, 282–90, 308
 project planning 216–35
 project proposals 313, 316
 project reviews 313–14, 316–17
 project scope 217–18, 231–2, 282–3
 promotion 11–12, 280
 property, protection 206
 proportionate 202
 prosecution 57
 protection software 126
 protocols 130–9, 262, 267
 prototypes 181
 pseudocodes 109
 psychological impacts 67–9
 public sector 2, 198–9

Public Sector Bodies (Websites
 and Mobile Applications) (No.2)
 Accessibility Regulations 2018 158,
 198–9
 quality 44, 62, 228–9, 272
 quantum 168–70
 quotas 6
 radio frequency identification (RFID)
 254
 radio frequency interference (RFI) 113
 random access memory (RAM) 114–16
 ransomware 243
 rapid application development (RAD)
 286–7
 rationales 308
 reach 61
 Read Only Memory (ROM) 116
 recession 37
 recruitment, inclusive 160
 reduce, reuse, recycle 10, 41
 redundancy 147
 redundant array of independent disks
 cards (RAIDs) 117
 reflection 177–80, 300, 310–11
 regression testing 277–8
 relationship 282
 remote access Trojan (RAT) 243
 remote working 15, 38–9, 60–1, 64
 removable media 264–5
 repetitive strain injury (RSI) 70, 71
 reporting schedules 222–3
 reports 89, 223, 229, 291
 reproducibility 33
 reputation 51, 53–4, 57, 151, 161, 240,
 264
 Request for Comments (RFC) 209
 research 21
 resilience 53, 143, 146–51
 resources 24, 29, 31, 43–4, 87, 219,
 229–30
 response times 46–7, 50
 responsibility 34
 responsible, accountable, consulted or
 informed (RACI) 234
 restructuring 35
 retention 192, 193
 return on investment (ROI) 221
 reviews 52, 229
 rights to practise, withdrawal 54
 risk 30–1, 52–5, 147, 161, 190, 231
 analysis 227, 286
 assessment 190, 223, 226
 management 225–7, 268
 mitigation 62, 190, 227, 249–62, 268,
 298–9, 303
 rollback planning 32–3

root cause analysis (RCA) 274–5, 312
 routers 120–1, 141
 routing protocols 132
 sales 11–14, 74, 280–1
 sales revenue 238
 sanctions 6
 scalability 19, 25, 61
 scheduling 222–3
 scope 217–18, 231–2
 screen input boxes 84–5
 Scrum 283–4, 285
 searches 127, 290
 sector/industry data 76
 Secure Sockets Layer (SSL) 131–2, 266–77
 security 50, 52–3, 131, 150, 236–69, 256
 and cloud storage 292–3
 and confidential information 237–41
 effective 268
 internet security assurance 262–7
 and remote working 38–9
 and resilience 146, 149–51
 and risk mitigation 298–9, 303
 and virtualisation 140, 144
 see also cyber attacks
 segregation (segmentation) 263
 selection 101, 107–8
 self, curated 65
 self-exclusion 71–2
 sensors 127–9
 sequences 101, 107, 108
 Serial Advanced Technology Attachment (SATA) 117
 servers 124, 140–2
 service range 21
 session layers 133, 135
 shareholders 4
 sharing 140
 shoulder surfing 245
 Simple Mail Transfer Protocol (SMTP) 131
 skills 49, 64, 92, 155, 219
 core 295–317
 shortages 63, 66, 299, 301
 sleep disturbances 70–1
 Small Computer System Interface (SCSI) 116, 117
 small or medium enterprises 2
 smart devices 127–30, 171
 SMART objectives 217
 SMARTER objectives 30
 smishing 244
 social engineering 242–3, 245–6, 265, 277
 social factors 7–9, 37–8
 social integration 47

social isolation 65–6, 68, 164
 social media 12, 67, 69, 72, 290
 social mobility 7–8
 social skills 64
 social trends 37
 society 63–7
 socioeconomic factors 8–9, 38, 48
 software 44, 48, 124–7, 250–1
 automation 62
 copying 200
 and data encryption 252–3
 legacy 147, 244, 246–7, 259
 licences 200
 maintenance 259–60
 malicious 242–3, 249–51, 264
 metrics 94
 monitoring 94
 open source 124–6
 and project planning 220
 proprietary 124
 testing 272–3
 training 150
 updates 146–7, 249–50, 259
 versions 271
 see also specific software
 software development kit (SDK) 184
 software as a service (SaaS) 26, 80, 144–5
 solid state drives 116
 sound 89–90
 sources 297–8
 spam, malicious 244
 spiral methodology 286
 sprints 283–4, 285
 spyware 243
 SQL injection 242, 266
 stakeholder power–Interest matrix 289
 stakeholders 2–5, 43–4, 217–18, 220, 238, 297, 299–302
 status reports 223
 storage 77–81, 83, 87, 116, 145–6, 149, 151, 168, 174, 292
 storage area network 79
 strategy 23, 36, 219
 stress 69–70, 276
 subjectivity 186
 subsidies 6
 supervisory control and data acquisition system (SCADA) 128
 suppliers 76, 185
 support 42, 46, 47–8
 surveillance 61, 63–4, 93–4, 205
 sustainability 40, 147
 switches 120, 141
 SWOT analysis 290–1
 system failure 26

system maintenance 259–60
 tables 306
 tailgating/piggybacking 245
 tariffs 6
 tasks 104, 306–17
 taxation 6–7, 16
 teams 24, 30–1, 45, 223, 229, 231
 technological factors 9, 39, 53–4
 test environments (sandboxes) 33–4
 test scripts 273
 testing 143, 270–8, 297–8, 302, 311–17
 threats 241–62, 268, 299
 time issues 43, 47, 146–7, 222–3, 230, 293
 Time to Live (TTL) 138
 timelines 218, 223
 tools 279–94, 297, 299–302, 308
 top-down approaches 103
 touchscreens 118
 trace tables 108
 traceability 33–4
 trade marks 40
 trade secrets 238
 trailers 139
 training 14, 35, 49–50, 143–4, 150, 191, 280
 training needs analysis (TNA) 42–3
 transactions 174
 transmission control protocol 137–9
 Transport Layer Security 131, 266, 267
 transport layers 133, 135, 137
 transportation, smart 129
 trends 8, 37–8, 93–4, 281
 Trojan 243
 troubleshooting 311–12, 314–15
 trusts 51
 unboxing 52
 under-resourced 229–30
 Uniform Resource Identifier (URI) 127
 unique identifiers 65
 unique selling points (USPs) 20
 universal serial bus network cards 121
 Universal Service Obligation (USO) 163, 196–7
 Unix 126
 usability 50, 271, 276
 user interface testing 271
 usernames 254
 users 87, 217, 265
 utility meters, smart 129
 validation 85–6
 value 27
 values 56
 variables 107, 108
 venues 219
 verification 85

version control 35
viability 29, 221
victimisation 157
video 89–90
video conferencing 61, 293–4
virtual assistants 13–14
virtual client computing (VCC) 141
virtual computing systems 139–44
virtual local area network (VLAN) 263
virtual private network (VPN) 120, 261
virtual reality (VR) 89, 173–4
virtual workspaces/workstations 292
virtualisation 18–19
viruses 243
vishing 244

visualisation 173, 291
voluntary sector 2
vulnerabilities 25, 97, 151, 246–9,
 265–6, 268, 299
war 36
warrants 192, 193
waste 10, 41, 129, 200–1, 284
Waste Electrical and Electronic
 Equipment Directive 2012 200–1
Waterfall methodology 285–6
web browsers 127, 130, 271
Web Content Accessibility Guide
 (WCAG) 154, 155, 164, 204
web protocols 130–1
webinars 89

webmarking 197
website traffic 75
white box testing 266, 278
white papers 185
whiteboards, electronic 293
Wide Area Network (WAN) 119–20
wireless connection 119–20, 123, 211
Work at Height Regulations 2005 189
work breakdown structure (WBS) 228,
 233
workflow impedance 31
working practice 56, 61–2
workstations 71, 190–1, 291–2
World Wide Web (WWW) 183
worms 243



Digital T Level: Digital Support Services and Digital Business Services (Core): Boost eBook

Boost eBooks are interactive, accessible and flexible. They use the latest research and technology to provide the very best experience for students and teachers.

- **Personalise.** Easily navigate the eBook with search, zoom and an image gallery. Make it your own with notes, bookmarks and highlights.
- **Revise.** Select key facts and definitions in the text and save them as flash cards for revision.
- **Listen.** Use text-to-speech to make the content more accessible to students and to improve comprehension and pronunciation.
- **Switch.** Seamlessly move between the printed view for front-of-class teaching and the interactive view for independent study.
- **Download.** Access the eBook offline on any device – in college, at home or on the move – with the Boost eBooks app (available on Android and iOS).

To subscribe or register for a free trial, visit
www.hoddereducation.co.uk/t-levels-digital

The Digital Support Services and Digital Business Services route core elements are covered in this Student Textbook. We have released the Digital Support Services pathway core elements online, for free.
Visit www.hoddereducation.co.uk/digitalsupportservices/pathwaycore to learn more.

‘T-LEVELS’ is a registered trade mark of the Department for Education.

‘T Level’ is a registered trade mark of the Institute for Apprenticeships and Technical Education

The T Level Technical Qualification is a qualification approved and managed by the Institute for Apprenticeships and Technical Education.

DIGITAL

DIGITAL SUPPORT SERVICES: CORE DIGITAL BUSINESS SERVICES: CORE

Tackle the core elements of your Digital Support Services or Digital Business Services T Level with this comprehensive resource, endorsed by NCFE.

Written by highly respected authors, Mo Everett and Sonia Stuart, this clear, accessible and thorough textbook will guide you through the key principles, concepts and terminology, as well as providing the inside track into what it takes to kick-start a career in the Digital world.

- Simplify complex topics with summary tables, diagrams, key term definitions and a glossary.
- Track and strengthen knowledge by using learning outcomes at the beginning of every unit and 'Test Yourself' questions.
- Apply your knowledge and understanding across 100s of engaging activities and research tasks.
- Prepare for your exams and the employer-set project using practice questions and project practice exercises.
- Get ready for the workplace with industry tips and real-world examples.
- Be guided through your course by expert authors Mo Everett and Sonia Stuart, who draw on their extensive industry and teaching experience.

This Student Textbook covers the T Levels' 12 route core elements. The Digital Support Services pathway core elements are covered online and available for free on the Hodder Education website. Find out more by turning to the inside back cover.



This title is also available as an **eBook** with **learning support**.

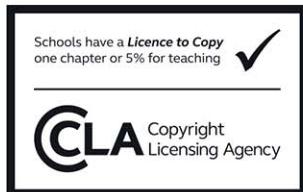
Visit hoddereducation.co.uk/boost to find out more.

HODDER EDUCATION

t: 01235 827827

e: education@hachette.co.uk

w: hoddereducation.co.uk



ISBN 978-1-3983-4679-6

