Cover image © Drazen Zigic / Shutterstock

Pearson Level 3 Alternative Academic Qualification

BTEC National in

Information Technology (Extended Certificate)

L3

Planning and Teaching Guide

First teaching from September 2025

First certification from 2027

Qualification Number: 610/3960/3

About Pearson

We are the world's leading learning company operating in countries all around the world. We provide content, assessment and digital services to students, educational institutions, employers, governments and other partners globally. We are committed to helping equip students with the skills they need to enhance their employability prospects and to succeed in the changing world of work. We believe that wherever learning flourishes so do people.

References to third-party material made in this Planning and Teaching Guide are made in good faith. Pearson does not endorse, approve or accept responsibility for the content of materials, which may be subject to change, or any opinions expressed therein. (Material may include textbooks, journals, magazines and other publications and websites.)

All information in this Guide is correct at time of publication.

Contents

1. Introduction

This Planning and Teaching Guide complements your Pearson Level 3 Alternative Academic Qualification in Information Technology (Certificate) specification, Pearson Set Assignment Briefs (PSABs), Sample Assessment Materials (SAMs) and the Pearson BTEC Level 3 National Alternative Academic Qualification Administrative Support Guide. This Planning and Teaching Guide provides:

- an overview of dates and deadlines for key events and activities relevant to qualification delivery – from registration to assessment and review of marking – throughout the academic year
- suggestions for planning and delivering your course including induction and unit sequencing
- creative and realistic teaching and learning ideas as well as links to resources for each unit to support and inspire you in creating a dynamic learning environment to keep your learners engaged and motivated to learn.
- wider delivery support such as guidance on study programme planning and descriptions and links to qualification resources and materials.

The guide was designed and written in collaboration with current practitioners to ensure that the planning and delivery suggestions and teaching and learning ideas are feasible, pedagogically sound and appropriate for the vocational area and the purpose of the qualification.

We recognise that delivery contexts will vary from one centre to the next and that practitioners are the best decision-makers for what works best for them and their learners. Therefore, teachers can tailor the suggestions and ideas proposed in this guide to meet the specific needs of their learners and the available resources in their centre. There are, however, requirements that have to be met in relation to assessment plans and to teaching and learning preceding assessment, which will be clarified/covered in this guide.

We hope you will find this guidance relevant and useful, and you enjoy teaching this this qualification!!

What's new

When creating these BTEC Nationals, in addition to ensuring the sector technical content was current and up-to date, we have also focused on developing the skills and personal attributes students need to navigate the future. We have worked with many higher education providers, professional bodies, colleges and schools to ensure these qualifications also meet their needs. Employers are looking for future employees with a thorough grounding in the latest industry requirements and work-ready skills such as critical thinking and problem solving. Higher education needs students who have experience of research, extended writing and meeting deadlines to be successful on their undergraduate programmes.

We have addressed these requirements by:

- Facilitating and guiding the development of transferable skills through the design and delivery of the qualifications, using a holistic and practical framework which is based on recent research into the most critical skills needed to navigate the future. A Transferable Skills framework has been used to embed transferable skills in the qualifications where they naturally occur and to signpost opportunities for delivery and development as a part of the wider BTEC learning experience. Please refer to the BTEC Transferable Skills Guide for Teachers for further information on this framework, its relevance and how it has been implemented in the qualifications.
- Supporting the delivery of Sustainability Education and development of Digital Skills naturally through the content design of the qualifications. Mapping is provided in the specification to identify where these opportunities for teaching and learning exist.
- Updating sector-specific content to ensure it is current, relevant and future-facing.
- Implementing a consistent approach to assessment with a balanced combination of internal and external assessments to better engage students, make the qualifications more accessible for them and more manageable for centres to deliver.

We are providing a wealth of support, both resources and people, to help ensure that you and your learners have the best possible experience during their course. Please see the section on Pearson Qualification Support and resources on page 183 *for* details of the available resources and support with links to access these.

Notes:

The qualification specification provides the content that must be taught and what must be assessed. This planning and teaching guide provides suggestions and ideas for how the content could be delivered. The suggestions given in this guide link with the Pearson Set Assignment Briefs provided by Pearson, which are mandatory for internal assessment and cannot be amended or contextualised by centres.

2. BTEC Calendar of Key Dates

Each academic year there are some key dates and deadlines in the delivery of BTEC qualifications that teachers need to be aware of, and act on appropriately, to ensure:

- the smooth running of learner registration, assessment and the quality assurance process, and
- effective timetable planning to fully prepare students for assessments and ensuring timely completion of administrative tasks.

Here is an overview of the key dates and deadlines for this qualification.

The specific date for each activity or event will vary each academic year and so only the month is provided. For the specific dates for the current academic year, please go to our webpage: https://qualifications.pearson.com/en/qualifications/btec-nationals/information-technology-aaq.html

Month	General related dates	Internal Assessment related dates	External Assessment related dates
September	Student registration		
October		Lead IV registered and completion of team standardisation	Entry deadline for January external assessment
November	Late student registration fee		
December	Late student registration fee Deletion deadline: delete student registrations for any leaner. withdrawn from the qualification		
January		Standards Verification Window opens	January External Assessment Series
February			

March			Restricted release of results to centres Release of results to students Entry deadline for Summer external assessments Review of Marking
April			Review of Marking
May		Standards Verification for first sample closes	Summer External Assessment
June		Standards Verification for second sample closes	
July	Deadline for full qualification claim for summer certification		
August			Restricted release of results to centres Release of results to students Review of marking

3. Planning the Delivery of your Course

Planning your course ensures a coherent and logical approach to teaching that helps learners to connect concepts effectively and build their knowledge progressively.

Effective assessment planning is also essential to allow for timely evaluation of student progress and adjustment of teaching strategies or interventions as needed.

This section offers recommended approaches to support practitioners with planning and implementation of this qualification

Induction

Students

An induction period at the start of the course is recommended to help students understand and prepare for the demands of their chosen course, as well as familiarise them with the BTEC ethos and methodology. This induction aims to not only equip learners with the necessary knowledge and skills but also to create a welcoming environment where they feel safe, supported and gain a sense of belonging as they begin their course in a new setting.

Centres will have their own induction programmes, and to support this, Pearson have provided a range of adaptable resources that can be integrated into this existing programmes. These resources cover areas such as welcome activities and information to include in the induction, with supporting slides. As we believe that every opportunity should be taken to develop transferable skills across the wider BTEC learning experience, we have also provided guidance on which transferable skills could be delivered as a part of the induction process including Managing Own Learning, Continuous Learning, goal setting and personal strength and resilience. The resources are designed to help students develop the relevant transferable skills through learning how to manage their course workload, completing their assessments successfully and meeting deadlines whilst also building their confidence and ability to thrive on their BTEC journey.

Tutors/Teachers

In addition to the annual standardisation training that all BTEC teaching staff are required to complete at the beginning of each academic year using the Pearson provided materials, an induction period for new tutors is also recommended. This will help new tutors familiarise themselves with the specific demands and expectations of the BTEC curriculum, equipping them with the necessary knowledge and skills to effectively plan and support their learners from the outset.

Overview of Assessment Availability

Internal Assessments

Pearson Set Assignments (PSABs) are provided by Pearson for all internally assessed units and must only be used for summative assessment.

These are available for the lifetime of the qualification and are accessible through our website. Teachers with a Pearson online account can log in through the sign-in portal to access them. Any teacher with learners registered for this qualification can create a Pearson online account.

The PSAB's for Information Technology are expected to be changed by the centre each year and guidance on the PSAB's will be availble through our website

External Assessments

External assessments are available in two series each academic year as shown below:

Dates	Jan	Mar	May/June	Aug
Assessment	External Assessments Series 1 *Not available in Jan 2026	External assessment Series 1 Results	External assessment Series 2	External Assessment Series 2 Results

Delivery and Assessment Planning

Clear unit planning and understanding is essential for a successful qualification delivery. This helps students to build on prior learning and reinforce concepts to develop a deeper understanding of the unit content and progressively develop their knowledge, understanding and skills throughout the course delivery.

We have produced a sample delivery plan showing how the **BTEC National Information Technology could** be delivered over **two** years, highlighting ordering of units and assessment milestones.

This plan is intended to be used as guidance.

Key

Del = Unit content delivery

PSAB = Pearson Set Assignment Brief

Rev = Revision for External assessment

Ext = External assessment

Resit Ext = Resit External assessment opportunity

Sequence of delivery

Year One

Unit	Unit Title	GLH	Assessment method	Term 1	January exam series	Term 2	Term 3	Summer exam series
1	Information Technology Systems	120	Ext	Del (Topic A, B & C)	-	Del (Topic D, E & F)	Rev	Ext
3	Website Development	60	Int	Del (Learning Aim A)	-	Del (Learning Aim B & C)	PSAB (15 hours)	

Unit 1 Information Technology Systems: This unit is an externally assessed mandatory unit that lays the foundation for the entire course. This unit provides essential underpinning knowledge of information technology systems, terminology, concepts and processes. There are many opportunities for learners to apply the knowledge gained in this unit to other units. For example, Topic B2 introduces learners to various types of networks, such as PANs, LANs, WANs, and VPNs. This knowledge can then be utilised in Unit 2, where learners will demonstrate their understanding of the cybersecurity risks associated with these networks. Topic E1 introduces learners to a range of online services, which they can later apply in Unit 3 when designing and developing a website in response to a brief. Similarly, Topic E2 familiarises learners with different data sources, collection methods, and techniques for improving data accuracy. This knowledge will be relevant in Unit 4, where learners will design and develop a database to meet a client's requirements.
As this is the first external assessment students will undertake, it is scheduled for the summer exam season. This approach provides centres with sufficient time to teach the unit content and allows students to develop their understanding of the command words used in assessments. It also ensures that students have the opportunity to resit the assessment in the second year of study, if necessary.

Unit 3 Website Development: This unit is internally assessed via a 15-hour PSAB, which is marked by centres and verified by Pearson. Learners will explore the fundamental principles of website development and then design and develop a website in response to a client brief.
Learners will build on the knowledge, understanding, and skills developed in Unit 1, where they gained a broad understanding of information technology systems that can be applied in this unit. For example, their knowledge of Topic C1: Online Systems, C2: Online

Communities, F1: Moral and Ethical Issues, and F2: Legal Issues will support them in designing and developing an effective website that meets the client's requirements.

Year Two

Unit	Unit Title	GLH	Assessment method	Term 1	January exam series	Term 2	Term 3	Summer exam series
2	Cyber Security and Incident Management	120	Ext	Del (Topic A, B, C and D)	Ext			Resit Ext
4	Relational Database Development	60	Int			Del (Learning Aim A, B, C)	PSAB (15 hours)	

Unit 2 Cyber Security and Incident Management: This mandatory unit is externally assessed and provides learners with the knowledge and understanding of cybersecurity terminology, security threats, system vulnerabilities, protection methods, forensic procedures, and the implications of cyber threats.
In Unit 1, learners developed an understanding of various digital devices, computer systems used in IT, emerging technologies, connections, networks, and online communities. Building on this foundation, Unit 2 will enable learners to identify and address the cybersecurity risks associated with these different aspects of IT systems. Learners will also be able to build on their familiarity with command words used in the external assessment for unit 1 such as "describe," "explain," and "evaluate," as these remain consistent across assessments. This unit's assessment is scheduled for the January window, providing students with the option to resit during the summer exam series if necessary.

Unit 4 Relational Database Development**:** This unit is internally assessed through a 15-hour PSAB, which will be marked by centres and verified by Pearson. Learners will examine relational database development principles and apply their skills to design and develop data storage solutions to meet a client's requirements.

Learners will build on the knowledge gained in Unit 1. For example, they learned about different sources of data, collection methods, the importance of ensuring data accuracy, methods for achieving data accuracy, and the legislation governing data use. This understanding will support them in designing and developing an effective database that meets client requirements.

Centres may deliver the qualification over a one-year period if required to provide flexibility to meet student or centre qualification planning needs.

4. Qualification Unit Delivery Guides

This section contains support for delivery of all the units in this qualification. The focus of these guides is on structuring and supporting the teaching and learning process. You will find ideas for activities and guidance on how best to use the activities to develop learners understanding of the topics in each unit. This section also includes activities and information on how to deliver transferable skills which are embedded or signposted in the qualification.

Unit 1: Information Technology Systems

Unit 1: Programming Fundamentals	
Assessment type: External	
Content Area	**Topics**
A: Explore the concepts and implications of the use of, and relationships among devices that form IT systems	A1 Functions and use of digital devices, and the notation used to represent the design of IT systems A2 Peripheral devices and media A3 Computer software in an IT system A4 Choosing IT systems A5 Emerging technologies
B: Transmitting data	B1 Connectivity B2 Networks B3 Issues relating to transmission of data
C: Operating online	C1 Online systems C2 Online communities
D: Protecting data and information	D1 Threats to data, information, and systems D2 Protecting data
E: Impact of using IT systems	E1 Online services E2 Using and manipulating data
F: Issues	F1 Moral and ethical issues F2 Legal issues
Assessment overview The unit will be assessed through one examination of 90 marks lasting 2 hours. Students will be assessed through a number of short- and long-answer questions. The questions will assess knowledge and understanding of IT systems and the implications of their use in personal and professional situations. The assessment availability is twice a year in January and May/June. The first assessment availability is May/June 2026. Sample assessment materials will be available to help centres prepare students for assessment	

Common misconceptions

There are no common misconceptions for this unit

Learning Activities and Resources

This section offers a starting point for delivering the unit by outlining a logical sequence through the unit topics and suggesting practical activities and teacher guidance for covering the main areas of content during guided learning time. Transferable skills are integrated into various activities, with those embedded in a unit indicated by an acronym in square brackets. The acronym combines the letters from the broad skill area and the specific transferable skill, e.g., [IS-WC].

Please note the activities provided below are suggestions and not mandatory. Pearson is not responsible for the content of any external internet sites. It is essential that you preview each website before using it to ensure the URL is still accurate, relevant, and appropriate.

Learning Topic	Activities and guidance for unit content delivery	Resources
A1 Functions and use of digital devices, and the notation used to represent the design of IT systems	• **Whole Class Teaching and Learning – Introduction To Digital Devices:** ○ Start with a comprehensive presentation that explores various digital devices integral to IT systems, such as personal computers, multifunctional devices, mobile devices, servers, entertainment systems, digital cameras, navigation systems, communication devices, and embedded systems. ○ Utilise visual aids and real-world case studies to illustrate the features and practical applications of each device. ○ Foster a dynamic discussion where students share their experiences with these devices, focusing on their roles in personal, educational, and professional contexts. ○ Split students into small groups and assign each group a specific type of digital device (e.g., personal computers, mobile devices, etc.). ○ Task each group with researching the technical features, benefits, and limitations of their assigned device, considering its use in various fields such as education, healthcare, and business.	**Digital Divide Council** - provides insights into the digital divide and the importance of technology in education. It includes case studies and discussions on how digital devices are impacting various fields. Blog | Digital Divide Council **Techopedia -** offers articles that explain the technical features, benefits, and limitations of various digital devices. Techopedia **idebate -** used to promote and facilitate debate education and competition, providing resources and support for students and

	○ Groups will prepare a concise presentation, emphasising how their device addresses the needs of individuals and organisations in modern society. • **Paired Activity - Case Study Analysis:** ○ Have students pair up to analyse real-world case studies that demonstrate the application of digital devices in various sectors (e.g., healthcare innovations, retail technology). ○ Each pair will select a case study to investigate how specific devices are utilised and their impact on efficiency and outcomes. ○ Students will prepare a report or presentation summarising their findings, emphasising the role of technology in driving progress and addressing challenges in their chosen sector. • **Whole Class and Individual Activity - Flowchart Creation:** ○ Introduce flowcharts as an essential form of notation used in designing IT systems. Discuss their importance in visualising processes. Explain the symbols that are used and general good practices that should be observed when drawing flowcharts. ○ Provide examples of flowcharts relevant to IT systems, such as workflows for troubleshooting a device or outlining the steps for connecting devices to a network. ○ Assign students to create a flowchart that details a specific task involving a digital device (e.g., setting up a server or configuring a smart device). ○ Students will present their flowcharts to the class, highlighting the clarity and effectiveness of using proper notation in IT design.	educators to enhance their debating skills and critical thinking. International Debate Education Association (IDEA) **Creately -** offers online diagramming tools, including templates for flowcharts and various system diagrams. Creately

	• **Peer Teaching – Developing System Diagrams**
	  ○ Begin with a brief overview of system diagrams, explaining their purpose in visualising the functionality and processes of IT systems. Discuss how they are different to flowcharts and the importance of notation in effectively communicating how systems operate and interact.
	  ○ Have students pair up with a partner. Encourage them to choose someone they haven't worked closely with before to enhance collaborative learning.
	  ○ Once research is complete, each pair will take turns teaching each other about their chosen system diagram. Encourage students to ask questions and discuss how these diagrams can enhance understanding of IT systems.
	  ○ Each pair will collaboratively create a simple system diagram that illustrates a basic IT system (e.g., a library management system, an online shopping system). They should apply appropriate notation and clearly label the components of the diagram to reflect the system's functionality.
	  ○ Facilitate a discussion about the various notations used and how they contribute to designing effective IT systems.	

A2
Peripheral Devices and Media
	• **Whole Class Teaching and Learning - Introduction to Peripheral Devices:**
	  ○ Introduce students to different types of peripheral devices.
	  ○ Use visual aids (images/videos) to present various input, output, and storage devices. Discuss their functions and importance in IT systems.
	  ○ Encourage students to share experiences of using different devices in their daily lives, highlighting their features and uses. Encourage groups to delve deeper into their research by considering different critical thinking questions
	  ○ They will create a presentation to share their findings with the class, incorporating illustrating their ability to analyse and evaluate the information.
		TechTerms - provides clear definitions and explanations of various technology terms, including peripheral devices, input/output devices, and storage media characteristics. TechTerms
		
		HowStuffWorks - offers detailed articles and explanations about how different technologies work,

	• **Individual Activity - Assistive Technologies Exploration:**
	  ○ Understand the importance of assistive technologies for individuals with disabilities.
	  ○ Each student will select one assistive technology (e.g., adaptive keyboards, screen readers) to research.
	  ○ Students will write a report detailing how their chosen technology works, its features, and its impact on users. They will present their findings in a class discussion.
	  ○ Set up stations with different assistive technologies (e.g., screen magnifiers, text-to-speech software).
	  Students rotate through the stations, trying out each technology and reflecting on its usability and impact on accessibility in IT.
	
	• **Whole Class Activity - Characteristics and Implications of Storage Media:**
	  ○ Analyse the characteristics of various storage media.
	  ○ Facilitate a discussion on storage media, focusing on capacity, cost, speed, and compatibility. Use real-life examples, such as comparing USB drives and cloud storage.
	  ○ Students will complete a chart comparing different storage media based on the discussed characteristics.
	
	• **Paired Activity - Data Processing Methods:**
	  ○ Differentiate between manual and automatic data processing.
	  ○ Pair students and assign them to investigate examples of manual and automatic data processing within an IT system.
	  ○ Instruct each pair to investigate examples of manual and automatic data processing within an IT system.
	  ○ Students to present their findings to the class, explaining their findings and the significance of the differences between manual and automatic processing.
		including peripheral devices and assistive technologies. HowStuffWorks
		
		WebAIM - focuses on web accessibility and provides information about assistive technologies, including screen readers and text-to-speech software. WebAIM

A3 Computer Software in an IT System	• **Whole Class Teaching and Group Activity - Operating Systems:**
	  ○ Begin with a presentation on the various types of operating systems, including batch, distributed, multitasking, network OS, real-time OS, mobile OS, single-use, and multi-user.
	  ○ Divide students into small groups and assign each group a specific type of operating system.
	  ○ Students will research their assigned OS, focusing on its features, applications, and impact on individuals and organisations.
	  ○ Each group will present their findings to the class, encouraging critical thinking about the implications of their OS. **[SP-CT]**
	  ○ Conduct a lecture on the role of operating systems in managing networking, security, memory management, multi-tasking, device drivers, and user accounts.
	  ○ Follow up with an individual assignment where students analyse an operating system of their choice and write a report on how it manages these aspects.
	
	Peer Teaching - User Interface Types:
	
	  ○ Assign students different types of user interfaces (command line, menu-driven, graphical user, touchscreen graphical user)
	  ○ Have them prepare a short lesson to teach their peers about the features and factors influencing their choice.
	  ○ This promotes collaboration and reinforces understanding.
	
	• **Whole Class Activity - Open Source vs. Proprietary Software:**
	  ○ In a computer lab, students will explore common file types and formats for images, audio, video, and application software.
	  ○ They will practice converting files between formats and understanding the features and limitations of each type.
		GCFGlobal - offers free tutorials on various technology topics, including operating systems and software types.
		
		GCFGlobal
		
		Microsoft Learn - provides resources and tutorials for understanding operating systems, user interfaces, and software applications. Microsoft Learn
		
		Codecademy - offers interactive coding lessons that include information about software types and user interfaces. Codecademy
		
		Quizlet - allows users to create and access quizzes and flashcards on various topics, including software concepts and operating systems. Quizlet

A4
 	
Choosing IT Systems
	• **Whole Class Teaching and Learning - Introduction to IT Systems:**
	  ○ Begin with a presentation that outlines the various IT systems and their features. Use visual aids to illustrate how different systems can impact performance.
	  ○ Discuss the factors affecting the choice of IT systems, such as user needs and specifications. Encourage students to share their insights and experiences with different IT systems.
	
	• **Whole Class Teaching and Learning – Factors affecting Choice of IT systems:**
	  ○ Discuss the different factors that affect the choice of IT systems including user needs, specifications, compatibility etc. as outlined in the specification.
	  ○ Provide students with information about different types of users (e.g., office workers, general users) and ask them to identify which factors are most important for each user type, explaining their reasoning.
	
	• **Individual Activity - Case Study on Automation:**
	  ○ Assign students to research a case study on automation within an organisation, focusing on the impact of IT systems on productivity and working practices.
	  ○ Students will prepare a brief presentation on their findings, discussing how automation has changed the work environment.
		CIO.com - provides articles and resources focused on IT management, including user needs analysis, cost-benefit analysis, and security implications of IT systems. CIO.com
		
		Gartner - provides research and analysis on IT systems and emerging technologies. Gartner
		
		ComputerWeekly - offers news, analysis, and best practice guides on IT systems, including implementation plans and security implications. ComputerWeekly

A5
 	
Emerging Technologies
	• **Whole Class Teaching and Small Group Activity - Emerging Technologies**
	  ○ Begin with an overview of emerging technologies, using visual aids and examples (e.g., AI, IoT, blockchain).
	  ○ Discuss the potential benefits and challenges associated with these technologies.
	  ○ Encourage students to share their thoughts on technologies they find interesting or impactful.
		TechCrunch - provides the latest news on emerging technologies, startups, and trends in the tech industry. TechCrunch
		
		MIT Technology Review - offers in-depth articles and insights into

	○ Divide students into small groups (3-5 members). ○ Assign each group a specific emerging technology (e.g., AI, IoT, virtual reality). ○ Groups will conduct research on the assigned technology, focusing on its implications for personal use and organisational performance. ○ Each group will prepare a presentation to share their findings with the class, highlighting key insights and potential future trends. • **Whole Class and Individual Activity - Exploring IT Systems Performance** ○ Discuss the concepts of IT systems performance and how emerging technologies impact efficiency and effectiveness. ○ Assign students to research a case study of an organisation that successfully implemented an emerging technology to improve IT systems performance. ○ Students will write a reflective essay on the implications of this technology on the organisation's operations. • **Project-Based Learning - Designing a Technology Implementation Plan** ○ Students will work on a project in pairs, where they design an implementation plan for an emerging technology within a chosen organisation (real or hypothetical). ○ The plan should include an analysis of the technology's impact on organisational performance and potential challenges in its adoption. ○ Students will present their plans to the class, simulating a pitch to the organisation's stakeholders. • **Formative Assessment - Mock Assessments:** ○ Conduct mock assessments that prepare students, focusing on key concepts related to Aim A Explore the concepts and implications of the use of, and relationships among devices that form IT systems. ○ Use quizzes and interactive activities to consolidate learning and assess understanding of the material covered in the unit.	emerging technologies and their implications for society and business. MIT Technology Review **Pew Research Center** - conducts studies on technology trends and public perceptions of emerging technologies. Pew Research Center **IBM Watson -** provides resources and case studies on artificial intelligence and other emerging technologies. IBM Watson **Future of Privacy Forum -** addresses the ethical implications of emerging technologies, particularly regarding privacy. Future of Privacy Forum

B1
Connectivity
	• **Whole Class Teaching and Learning - Introduction to Data Transmission:**
	  ○ Begin with a presentation on the importance of data transmission in IT systems, covering both wired and wireless methods.
	  ○ Use visual aids to illustrate how data is transmitted and the roles of different connection types (Bluetooth, USB, Wi-Fi, Ethernet).
	  ○ Facilitate a discussion on how data transmission affects everyday technology use and organisational operations.
	
	• **Small Group Activity - Connection Type Comparison:**
	  ○ Divide students into small groups (4-6 members) and assign each group one of the following connection types: Bluetooth, USB, Wi-Fi, or Ethernet.
	  ○ Each group will research their assigned connection type, focusing on its features, advantages, disadvantages, and practical applications.
	  ○ Groups will create a comparison chart to present their findings, highlighting how each connection type meets the needs of individuals and organisations. This activity encourages critical thinking as students analyse the implications of each connection type. **[SP-CT]**
	
	Project-Based Learning - Designing a Data Transmission Plan:
	  ○ In pairs, students will choose a hypothetical organisation and design a data transmission plan that includes a combination of connection types.
	  ○ The plan should consider the organisation's needs, the implications of each connection type, and how to optimise performance.
		Cisco Networking Academy - offers resources and courses about different types of network connections, including their performance implications. Cisco Networking Academy
		
		Network World - covers news, analysis, and insights on networking technologies, including connection types and their impacts on IT performance. Network World
		
		CompTIA - offers educational resources on IT and networking, including information on different connection types and their effects on performance. CompTIA
		
		IEEE Xplore Digital Library - provides access to research papers and articles on networking technologies and their performance implications. IEEE Xplore

	○ Each pair will present their plan to the class, simulating a pitch to the organisation's management. This will enhance their critical thinking and problem-solving skills. • **Whole Class and Individual Activity - Impact of Connection Types on Performance:** ○ Discuss how different connection types can affect the performance of IT systems. ○ Assign students to research the impact of a specific connection type on either personal or organisational IT performance. They should consider factors such as speed, reliability, and security. ○ Students will present their findings through a written report or presentation, encouraging them to critically evaluate the implications of their chosen connection type. **[SP-CT]**	**How-To Geek -** offers articles and tutorials on various tech topics, including connection types and their performance impacts. How-To Geek **Lifewire -** provides clear explanations and practical advice on technology topics, including networking and connection types. Lifewire
B2 Networks	• **Whole Class Teaching and Learning - Introduction to Networks:** ○ Start with a presentation explaining the importance of networks in IT systems. ○ Introduce different network topologies (star, ring, bus) and types of networks (PAN, LAN, WAN, VPN) using visual aids. ○ Facilitate a discussion on the impact of networks on individuals and organisations, encouraging students to share their experiences with different network types. • **Small Group Activity - Network Topology Analysis:** ○ Divide students into small groups (4-6 members) and assign each group one of the following network topologies: star, ring, or bus. ○ Each group will research their assigned topology, focusing on its structure, advantages, disadvantages, and practical applications.	**Cisco Networking Academy -** offers resources and courses about different types of network connections, including their performance implications. This site can provide foundational knowledge for students. Cisco Networking Academy **CompTIA -** offers educational resources on IT and networking, including information on different connection types and their effects on performance. CompTIA

	○ Groups will create a poster or digital presentation to showcase their findings, promoting critical thinking as they analyse the implications of using their assigned topology in real-world scenarios. **[SP-CT]** **Whole Class and Individual Activity - Impact of Network Features on Performance:** ○ Discuss how different features of a network (topology, type, connectivity) can affect the performance of an IT system. ○ Assign students to research a specific network feature (e.g., security, connectivity) and its impact on performance. They should consider factors such as productivity and downtime. ○ Students will present their research findings through a written report or a presentation, encouraging them to critically evaluate the implications of their chosen feature. **[SP-CT]**	**IEEE Xplore Digital Library -** provides access to research papers and articles on networking technologies and their performance implications. IEEE Xplore **How-To Geek -** offers articles and tutorials on various tech topics, including connection types and their performance impacts. How-To Geek **Lifewire -** provides clear explanations and practical advice on technology topics, including networking and connection types. Lifewire
B3 Issues relating to transmission of data	• **Whole Class Teaching and Learning - Introduction to Data Transmission:** ○ Begin with a presentation outlining the key concepts of data transmission, including the importance of protocols (SMTP, HTTP, etc.) and their roles in tasks such as email, web pages, and secure payment systems. ○ Use visual aids to illustrate how data is transmitted across different types of networks and the implications of security, bandwidth, and latency. ○ Encourage students to share their own experiences with data transmission in everyday applications, fostering engagement and relatability.	**Tuts+ (Envato) -** provides tutorials and articles on video production, including how different codecs affect video quality and file sizes. Codecs Tutorial **Digital Trends -** Digital Trends provides insights into various codecs, their characteristics, and how they influence user experience in streaming and

	• **Small Group Activity - Protocol Exploration:**
	  ○ Divide students into small groups (4-5 members) and assign each group a specific protocol to research (e.g., SMTP, HTTP, HTTPS, etc.).
	  ○ Each group will create a presentation detailing how their assigned protocol works, its applications, advantages, and potential issues related to security, students analyse real-life applications and consider the consequences of protocol failures. **[SP-CT]**
	• **Individual Activity - File Type Implications:**
	  ○ Provide students with a list of common file types (images, audio, video, application software) and their formats.
	  ○ Students will research and write a brief report on the features and implications of each file type, focusing on how file type affects data transmission and performance. Encourage independent research to support the understanding of file management in IT systems.
	• **Whole Class Activity - Compression Types Workshop:**
	  ○ Conduct a workshop demonstrating the differences between lossy and lossless compression types.
	  ○ Provide students with examples of each type and engage them in a discussion about when to use each type based on factors such as quality and file size.
	  ○ Students can participate in an interactive exercise where they compare compressed and uncompressed files, analysing the trade-offs involved.
	  ○ Lead a discussion on the importance of codecs in transmitting audio and video in digital formats.
	  ○ Explore various codecs and their implications for quality and file size.
	  ○ Encourage students to consider how codec choice impacts user experience in different scenarios (streaming, downloading, etc.) and to share any personal experiences related to codecs.
		playback scenarios.
		Understanding Audio Codecs

	Formative Assessment - Mock Assessments: ○ Conduct mock assessments that prepare students, focusing on key concepts related to Aim B Transmitting Data. ○ Use quizzes and interactive activities to consolidate learning and assess understanding of the material covered in the unit.	
C1 Online Systems	• **Whole Class Teaching and Group Activity - Introduction to Online IT Systems:** ○ Begin with a presentation that outlines the features of online IT systems, including an overview of cloud computing models (private, public, hybrid, IaaS, SaaS, and PaaS). Use visual aids to illustrate these concepts. ○ Clearly define each model and discuss how they differ in terms of data storage and task performance. ○ Divide the class into small groups, assigning each group one cloud computing model (e.g., private cloud, public cloud, etc.). ○ Each group will research their assigned model, focusing on features, benefits, and potential drawbacks. • **Whole Class and Individual Activity - Exploring Remote Working Technologies.** ○ Introduce the concept of remote working technologies, including VPNs and remote desktop technologies, through a teacher-led discussion. ○ After the introduction, assign students to write a reflective piece on how these technologies enable remote work and their potential benefits and challenges for individuals and organisations. This task integrates individual reflection with whole-class learning.	**IBM Cloud Learn Hub:** provides comprehensive resources on cloud computing models, including detailed explanations of IaaS, PaaS, and SaaS, as well as private, public, and hybrid clouds. IBM Cloud Learn Hub **Amazon Web Services (AWS) -** provides an extensive library of resources about cloud computing, including detailed descriptions of their cloud services and models, as well as case studies showcasing real-world applications. AWS Cloud Computing

	• **Paired Activity - Evaluating Online Systems Selection Factors:**
	  ○ Pair students and have them create a checklist of factors that affect the selection of online systems, such as security, cost, ease of use, features, connectivity, and scalability.
	  ○ Each pair will then evaluate a specific online system based on their checklist and present their evaluations to the class.
	  ○ This encourages critical analysis of technology choices and collaborative learning. **[SP-CT]**
	
	• **Whole Class Activity - Cultural and Ethical Considerations in Online Systems:**
	  ○ Lead a discussion on the ethical considerations and cultural biases associated with online systems and cloud computing.
	  ○ Encourage students to reflect on how different populations may have varying access to technology and how this can impact their participation in digital environments.
	  ○ Students can share examples or scenarios they have encountered, fostering a deeper understanding of inclusivity in tech.	

C2
 	
Online Communities
	• **Whole Class Teaching and Small Group - Introduction to Online Communities:**
	  ○ Begin with a presentation that outlines the different features of online communities, including social media, blogs, wikis, chatrooms, instant messaging, podcasts, and forums.
	
	  ○ Discuss the implications of widespread online community use for individuals and organisations.
	  ○ Encourage students to share their own experiences with these platforms to foster engagement.
		Common Sense Media - offers resources on digital citizenship, including guides on various online platforms, privacy, and security. Common Sense Media
		
		Digital Citizen - provides articles and resources focused on digital literacy, online communities, and

	○ Divide students into small groups and assign each group one method of communication (e.g., social media, blogs, forums). ○ Each group will research their assigned method, focusing on its features, advantages, and disadvantages. • **Whole Class Activity - User Experience Evaluation:** ○ Conduct a workshop where students evaluate different online community platforms based on user experience factors (ease of use, performance, availability, accessibility). ○ Provide students with criteria for evaluation and encourage them to share their assessments and recommendations for improvements. ○ Discuss how user experience impacts individuals and organisations. • **Project-Based Learning - Assessing Privacy and Security:** ○ Assign students to work in pairs to choose an online community platform and assess its privacy and security measures. ○ Students will prepare a report detailing their findings, including potential risks and suggestions for enhancing security and privacy, reinforce critical thinking and encourage students to consider real-world implications. **[SP-CT]** • **Whole Class Discussion - Cost and Productivity Considerations:** ○ Lead a discussion on the costs associated with using online community platforms, including subscription fees, training costs, and integration with current systems. ○ Engage students in exploring how these costs impact productivity and overall organisational effectiveness.	safe internet use, which can support discussions about user experience and security. Digital Citizen **Buffer Blog -** discusses social media strategies, user experience, and productivity tips related to online communities. Buffer Blog **Sprout Social -** offers insights and resources about social media platforms, user engagement, and analytics. Sprout Social **Podcast Insights -** offers resources on creating and marketing podcasts. Podcast Insights

	○ Encourage students to consider how different organisations might approach these costs differently. • **Formative Assessment - Mock Assessments:** ○ Conduct mock assessments that prepare students, focusing on key concepts related to Aim C Operating Online. ○ Use quizzes and interactive activities to consolidate learning and assess understanding of the material covered in the unit.	
D1 Threats to Data, Information, and Systems	• **Whole Class Teaching and Small Group Activity - Threats:** ○ Begin with a presentation that outlines the different types of threats to data, information, and systems. Use visual aids and examples of each threat type (e.g., viruses, hacking). ○ Discuss the importance of data security and the consequences of these threats for individuals and organisations. ○ Encourage students to share any personal experiences with data breaches or security incidents. ○ Divide students into small groups and assign each group a specific type of threat (e.g., viruses, social engineering). Each group will research their assigned threat and create a poster or digital presentation. • **Whole Class and Individual Activity - Case Study Discussion:** ○ Present a case study of a well-known data breach (e.g., Equifax, Target). Students will work in pairs to discuss the impact of the breach on the organisation and its customers. ○ Prompt students to consider the financial loss, legal ramifications, and damage to public image. Each pair will summarise their findings and present them to the class, fostering critical thinking about the consequences of data threats. **[SP-CT]**	**Cybersecurity & Infrastructure Security Agency (CISA) -** provides resources and information on various cybersecurity threats, including guides on how to recognise and mitigate risks associated with data breaches and attacks. CISA - Cybersecurity Threats **Kaspersky -** provides comprehensive information on various cybersecurity threats, including articles on data breaches, malware, and social engineering tactics. Kaspersky - Cybersecurity Threats

	• **Individual Activity - Security Policies Proposal:**
	  ○ Have students draft a proposal for a data security policy for a fictional organisation. They should identify potential threats and outline strategies to mitigate these risks.
	  ○ Encourage students to think critically about how to balance security with usability. They should consider internal threats and how to educate employees on data security best practices. **[SP-CT]**
	
	• **Whole Class Activity - Role Play: Social Engineering Awareness:**
	  ○ Conduct a role-play exercise where some students act as "hackers" attempting to gather information using social engineering tactics, while others play employees of a company.
	  ○ After the role play, facilitate a discussion on the tactics used and how they can recognise and respond to such attempts in real life.
	
	• **Whole Class Teaching and Learning - Natural Disasters and Data Security:**
	  ○ Discuss the impact of natural disasters on data integrity and security. Use examples such as floods or fires that have affected businesses.
	  ○ Encourage students to reflect on how organisations can prepare for such events and the importance of data backups and disaster recovery plans.
		Verizon Data Breach Investigations Report (DBIR) - This annual report analyses data breaches and security incidents, providing real-world case studies. Verizon DBIR
		
		Privacy Rights Clearinghouse - offers resources on data breaches, including case studies and their impacts on individuals and organisations. Privacy Rights Clearinghouse - Data Breaches
		
		Infosec Institute - provides educational resources on various cybersecurity topics, including threat analysis and security policies. Infosec Institute
		
		The Hacker News - covers the latest cybersecurity news, including incidents of data breaches and analyses of various threats. The Hacker News

		National Cyber Security Centre (NCSC) - provides guidance on various cyber threats and best practices for organisations to protect their data and systems. NCSC - Cyber Threats
D2 Protecting data	• **Whole Class Teaching and Small Group Activity - Data Protection:** ○ Begin with a presentation on the importance of data protection, outlining various types of data - divide students into small groups and assign each group one of the data protection techniques (e.g., file permissions, multi-factor authentication, encryption methods). ○ Each group researches their assigned technique, focusing on its features, functions, and real-life applications. They should prepare a short presentation to share with the class, highlighting critical analysis of how their technique protects data and potential weaknesses. **[SP-CT]** ○ Ask groups to brainstorm scenarios where their technique might fail and discuss how those failures could be mitigated. **[SP-CT]** • **Whole Class Activity - Antivirus Software and Firewall Features Discussion:** ○ Facilitate a class discussion on the features and functions of antivirus software and firewalls. Use examples of popular software and their reviews. ○ Encourage students to research and present on how different antivirus solutions protect data from various threats. Discuss the pros and cons of using firewalls at home and in organisations.	**Data Protection Commission (DPC) -** provides resources on data protection legislation, principles, and guidelines for both individuals and organisations. Data Protection Commission **International Association of Privacy Professionals (IAPP) -** offers comprehensive resources on data protection, privacy laws, and best practices. IAPP - Resource Center **Kaspersky -** features articles on various data protection techniques, including antivirus and firewall solutions. It also

	○ Challenge students to debate the effectiveness of free antivirus software versus paid options, considering factors like updates, customer support, and features. **[SP-CT]** • **Paired Activity - Encryption Methods Comparison:** ○ In pairs, students will compare different encryption methods used to protect stored data, transmitted data, and data in secure websites (HTTPS). ○ Provide a chart for students to fill out detailing each method's advantages and disadvantages. Discuss how these methods apply to real-world situations, such as online banking or secure communications. ○ Ask students to evaluate which encryption method they believe is the most secure for a specific scenario and defend their reasoning. **[SP-CT]** • **Whole Class and Individual Activity - Case Studies on Data Breaches:** ○ Analyse case studies of notable data breaches (e.g., Target, Equifax) as a class, then assign individuals to research additional cases. ○ Discuss the implications of these breaches on data protection practices and the lessons learned. Students should focus on what went wrong and how proper techniques could have prevented the breaches. ○ Prompt students to propose a comprehensive data protection strategy that could have been implemented to avoid the breaches discussed. **[SP-CT]** • **Formative Assessment - Mock Assessments:** ○ Conduct mock assessments that prepare students, focusing on key concepts related to Aim D Protecting Data and Information ○ Use quizzes and interactive activities to consolidate learning and assess understanding of the material covered in the unit.	provides insights on the effectiveness of free versus paid antivirus options. Kaspersky - Data Protection

E1
 	
Online services
	• **Whole Class and Small Group Activity - Exploring Online Retail Services:**
	  ○ Present different online retail platforms (e.g., Amazon, eBay) using visual aids. Discuss key features such as user reviews, return policies, and personalised recommendations.
	  ○ Divide students into groups and ask them to conduct a survey on their peers' online shopping habits, focusing on preferred platforms, motivations for choosing these platforms and experiences with customer service.
	  ○ Groups will analyse the data collected, identify trends, and prepare a presentation to share their insights with the class.
	
	Project-Based Learning - Online Education and Collaborative Learning:
	
	  ○ Students will work in pairs to select an online learning platform (e.g., Coursera, Khan Academy) and evaluate its features, accessibility, and effectiveness in promoting learning.
	  ○ Each pair will explore how collaborative tools (like Google Docs or discussion forums) enhance the learning experience.
	  ○ Pairs will present their findings to the class, highlighting both the strengths and weaknesses of the platform they studied.
	
	• **Whole Class and Individual Activity - The Impact of Transactional Data and Targeted Marketing:**
	  ○ Introduce the concept of transactional data and how companies use this information for targeted marketing. Use real-world examples to illustrate the points.
	  ○ Assign students to research a specific company and analyse how it utilises transactional data to inform its marketing strategies.
		Online Retail Services - provides insights into different online retail platforms, their features, and consumer behaviours, making it a great resource for understanding online shopping habits. Statista - Online Retail
		
		EdSurge - features articles about online education platforms, tools, and collaborative learning methods. EdSurge - Online Learning
		
		Coursera - offers a variety of online courses and resources that students can explore to understand the features and effectiveness of online education platforms. Coursera
		
		Google Scholar - is a research database where students can find academic papers on various topics, including online services and consumer behaviour. Google Scholar

	○ Students will write a short reflection on the ethical implications of using personal data for marketing purposes and how it affects consumer choices.	**Khan Academy -** is a widely recognised online learning platform that offers a variety of free courses, lessons, and practice exercises across multiple subjects, including math, science, arts, and computer programming. Khan Academy
E2 Using and manipulating data	• **Small Group Activity - Exploring Sources of Data:** ○ Begin with a discussion on the importance of data in today's digital world. Present real-life examples of how organisations use data to make decisions. ○ Divide students into small groups and assign them to research and present on different sources of data: • Primary Data: Methods of collection (interviews, surveys). • Secondary Data: Types of secondary sources (research papers, online databases). ○ After presentations, facilitate a group discussion on the pros and cons of each data source, focusing on reliability and potential bias. **[SP-CT]** • **Whole Class Activity - Data Reliability Discussion:** ○ Introduce methods of ensuring the reliability of information. Discuss examples of unreliable sources versus reliable sources in news media and academic research. ○ Encourage students to debate the importance of data reliability and how it can affect decision-making in real-world scenarios.	**Data.gov -** is the U.S. government's open data portal, providing access to a vast array of datasets from various government agencies.Data.gov **Statista -** offers statistics and data on a wide range of industries and topics. It serves as an excellent resource for students to find both primary and secondary data, enhancing their understanding of data manipulation and its applications in business and research. Statista **SurveyMonkey -** is a digital survey tool that allows users to

	• **Individual Activity - Data Collection Method Design:**
	  ○ Students will choose one method of collecting data (survey, questionnaire, focus group, interview) and design their own data collection instrument.
	  ○ Provide them with guidelines on how to create effective questions. Additionally, they should reflect on how their chosen method impacts the data collected.
	  ○ Ask students to consider what types of bias could emerge from their selected method and how they might minimise this bias. **[SP-CT]**
	
	• **Whole Class and Individual Activity - Accuracy in Data:**
	  ○ Discuss the importance of ensuring data accuracy. Introduce methods like verification and validation.
	  ○ Provide case studies where data inaccuracies led to significant consequences in organisations.
	  ○ Have students analyse a case study and propose solutions to enhance data accuracy. **[SP-CT]**
	
	• **Paired Activity - User Interface Evaluation:**
	  ○ Activity: In pairs, students will evaluate a digital data collection tool (e.g., a survey platform) based on characteristics of user interfaces as outlined in the specification.
	  • Provide criteria for evaluation and have them present their findings.
	  ○ Encourage students to suggest improvements based on their evaluations and discuss the impact these changes could have on data quality.
		create and distribute surveys easily. SurveyMonkey
		
		The Data Warehouse Institute (TDWI) - offers resources and articles on data management, analytics, and the importance of data accuracy. TDWI

	• **Formative Assessment - Mock Assessments:**
	  ○ Conduct mock assessments that prepare students, focusing on key concepts related to Aim E Impact of using IT systems.
	  ○ Use quizzes and interactive activities to consolidate learning and assess understanding of the material covered in the unit.	

F1
 	
Moral and ethical issues
	• **Whole Class Teaching and Learning - Introduction to Moral and Ethical Issues:**
	  ○ Begin with a presentation that outlines the key moral and ethical factors related to information technology, focusing on privacy, environmental impact, unequal access to technology, access to assistive technology, online behaviour and netiquette, and acceptable use policies.
	  ○ Encourage students to share their initial thoughts and experiences regarding these issues.
	
	• **Small Group Activity - Privacy Debate:**
	  ○ Divide students into small groups and assign each group a specific aspect of privacy (e.g., data collection, surveillance, user consent).
	  ○ Each group will prepare arguments for and against the use of technology in relation to privacy, fostering critical thinking and discussion. **[SP-CT]**
	  ○ Groups will present their arguments to the class, followed by an open discussion.
	
	• **Individual Activity - Research on Environmental Impact:**
	  ○ Assign students to research the environmental impact of information technology, including e-waste and energy consumption.
		Electronic Frontier Foundation (EFF) - is a nonprofit organisation that focuses on defending civil liberties in the digital world. They provide resources on privacy, surveillance, and ethical considerations surrounding technology use. Electronic Frontier Foundation
		
		Privacy International - is an advocacy organisation that promotes and defends the right to privacy across the globe. Their website includes articles, reports, and case studies on privacy issues related to technology. Privacy International

	○ Students will create a brief report or presentation summarising their findings and suggesting ways to minimise this impact. ○ Encourage critical thinking by asking them to consider the balance between technological advancement and environmental sustainability. **[SP-CT]** • **Paired Activity - Online Behaviour and Netiquette Role-Playing:** ○ In pairs, students will create scenarios that depict positive and negative online behaviour. ○ They will role-play these scenarios in front of the class, highlighting the importance of netiquette. ○ After each role-play, engage the class in a discussion about the implications of online behaviour on individuals and communities.	**World Economic Forum (WEF) -** publishes articles and reports on the impact of technology on society, including environmental issues and access to technology. World Economic Forum **World Economic Forum (WEF) -** publishes articles and reports on the impact of technology on society, including environmental issues and access to technology. World Economic Forum **Environmental Protection Agency (EPA) -** offers information on the environmental impact of technology, including e-waste and energy consumption. EPA
F2 Legal issues	• **Whole Class Teaching and Learning - Introduction to Legal Issues in IT:** ○ Begin with a presentation that outlines the key legal issues surrounding IT systems, including computer misuse legislation, copyright laws, health and safety regulations, and data protection legislation. ○ Facilitate a discussion on why these laws are necessary for protecting users and their data.	**UK Government - Data Protection and Privacy –** the official government site provides information on data protection laws in the UK, including the General Data Protection Regulation (GDPR) and the Data

	• **Small Group Activity - Case Studies on Computer Misuse:**
	  ○ Divide students into small groups and assign each group a case study related to computer misuse (e.g., hacking, phishing, identity theft).
	  ○ Each group will analyse the case, identify the legal implications, and present their findings to the class, encouraging critical thinking about the consequences of such actions. **[SP-CT]**
	
	• **Individual Activity - Copyright Analysis:**
	  ○ Assign students to research the different types of copyright legislation, including copyright regulations for computer programs.
	  ○ Students will create a brief report or infographic highlighting important points and the implications for individuals and businesses in the IT sector.
	
	• **Whole Class and Individual Activity - Health and Safety Regulations:**
	  ○ Present an overview of health and safety regulations related to display screen equipment and the importance of ergonomics in IT environments.
	  ○ Engage students in a discussion about best practices for maintaining a safe workspace. Then, have students create a checklist of ergonomic practices for using IT equipment.
	
	• **Whole Class Teaching and Learning - The Role of Legislation:**
	  ○ Discuss the role of different legislation in protecting IT systems and users, focusing on how these laws impact organisations' operations.
	  ○ Encourage students to think critically about the balance between security and privacy, and how organisations navigate these challenges.
		Protection Act. It is an essential resource for understanding legal implications related to data protection. UK Government - Data Protection and Privacy
		
		Copyright.gov - The U.S. Copyright Office offers comprehensive resources on copyright law, including details on different types of copyright and their implications for individuals and businesses. Copyright.gov
		
		Computer Misuse Act (UK) - This page outlines the Computer Misuse Act 1990 in the UK, detailing the various offenses and legal implications of computer misuse. Computer Misuse Act
		
		Health and Safety Executive (HSE) - provides guidelines and regulations related to health and safety in the workplace, including ergonomic practices for display

	○ Formative Assessment - Mock Assessments: ○ Conduct mock assessments that prepare students, focusing on key concepts related to Aim F: Issues ○ Use quizzes and interactive activities to consolidate learning and assess understanding of the material covered in the unit.	screen equipment. Health and Safety Executive **Information Commissioner's Office (ICO) -** is the UK's independent authority set up to uphold information rights. Their website contains resources on data protection legislation and the implications for organisations Information Commissioner's Office **European Union – GDPR -** The official EU website provides detailed information about the General Data Protection Regulation (GDPR), including its principles, rights, and obligations. European Union - GDPR **Cybercrime.gov -** provides resources and information on various aspects of cybercrime, including legal definitions and case studies. Cybercrime.gov

Delivering signposted transferable skills

Signposted transferable skills are not mandatory for the delivery of the unit, and it is therefore your decision to deliver these skills as a part of the qualification. Below we have provided some ideas of teaching and learning activities that you could use to deliver these skills if you chose to.

Transferable skills	Ideas for delivery
[SP-CT] Solving Problems – Critical thinking	**Case Study Analysis:** Utilise real-world case studies related to IT systems, such as data breaches or the selection of technology in organisations. Students can analyse the problems presented in the case studies, identify root causes, and propose solutions. **Debates:** Organise structured debates on topics such as the advantages and disadvantages of emerging technologies or the implications of online privacy. This encourages students to critically evaluate different perspectives and formulate reasoned arguments. **Group Problem-Solving Workshops:** Divide students into small groups and present them with complex, real-world problems related to technology, such as cybersecurity threats or system design challenges. Each group collaborates to brainstorm potential solutions and presents their findings to the class. **Role-Playing Scenarios**: Create scenarios where students assume different roles within an organisation (e.g., IT manager, end-user, security analyst) facing a specific problem, like a software failure. This activity encourages students to understand varying perspectives and the impact of decisions.

	Research Projects: Assign students to research a current technological challenge (e.g., AI ethics, data privacy issues) and prepare a presentation or report. This encourages them to gather evidence, analyse data, and articulate their findings clearly. **Problem-Based Learning (PBL):** Implement PBL by presenting students with an open-ended problem related to IT systems. For example, they could work on optimising a system for a fictional company. Students engage in inquiry, research solutions, and develop a proposal. **Journaling Reflections**: Encourage students to keep a reflective journal where they document problems they encounter in their studies or personal experiences. They can analyse these problems, reflect on their thought processes, and outline possible solutions. **Technology Impact Analysis**: Have students choose a specific technology (e.g., social media, cloud computing) and analyse its positive and negative impacts on society. This promotes critical evaluation of technology's role in modern life. **Expert Interviews:** Invite IT professionals to discuss real-world problems they face in their work. Afterward, students can engage in discussions or write reflections on how they would approach similar issues.

Resources

This section has been created to provide a range of links and resources that are publicly available that you might find helpful in supporting your teaching and delivery of this unit in the qualification. We leave it to you, as a professional educator, to decide if any of these resources are right for you and your students, and how best to use them.

Pearson is not responsible for the content of any external internet sites. It is essential that you preview each website before using it to ensure the URL is still accurate, relevant, and appropriate. We'd also suggest that you bookmark useful websites and consider enabling students to access them through the school/college intranet.

Websites

https://aws.amazon.com/what-is-cloud-computing/
Amazon Web Services (AWS) - provides an extensive library of resources about cloud computing, including detailed descriptions of their cloud services and models, as well as case studies showcasing real-world applications.

https://buffer.com/resources
Buffer Blog - discusses social media strategies, user experience, and productivity tips related to online communities.

https://www.cio.com/
CIO.com - provides articles and resources focused on IT management, including user needs analysis, cost-benefit analysis, and security implications of IT systems.

https://www.netacad.com/
Cisco Networking Academy - offers resources and courses about different types of network connections, including their performance implications. This site can provide foundational knowledge for students.

https://www.codecademy.com/
Codecademy - offers interactive coding lessons that include information about software types and user interfaces.

https://www.commonsense.org/education
Common Sense Media - offers resources on digital citizenship, including guides on various online platforms, privacy, and security.

https://www.comptia.org/
CompTIA - offers educational resources on IT and networking, including information on different connection types and their effects on performance.

https://www.legislation.gov.uk/ukpga/1990/18/contents

Computer Misuse Act (UK) - This page outlines the Computer Misuse Act 1990 in the UK, detailing the various offenses and legal implications of computer misuse.

https://www.computerweekly.com/
ComputerWeekly - offers news, analysis, and best practice guides on IT systems, including implementation plans and security implications.

https://www.coursera.org/
Coursera - offers a variety of online courses and resources that students can explore to understand the features and effectiveness of online education platforms.

https://creately.com/
Creately - offers online diagramming tools, including templates for flowcharts and various system diagrams.

https://www.cybercrime.gov/
Cybercrime.gov - provides resources and information on various aspects of cybercrime, including legal definitions and case studies.

https://www.cisa.gov/cybersecurity
Cybersecurity & Infrastructure Security Agency (CISA) - provides resources and information on various cybersecurity threats, including guides on how to recognise and mitigate risks associated with data breaches and attacks.

https://www.data.gov/
Data.gov - is the U.S. government's open data portal, providing access to a vast array of datasets from various government agencies.

https://www.digitalcitizen.life/
Digital Citizen - provides articles and resources focused on digital literacy, online communities, and safe internet use, which can support discussions about user experience and security.

http://www.digitaldividecouncil.com/
Digital Divide Council - provides insights into the digital divide and the importance of technology in education. It includes case studies and discussions on how digital devices are impacting various fields.

https://www.digitaltrends.com/home-theater/what-is-audio-codec-explained/
Digital Trends - Digital Trends provides insights into various codecs, their characteristics, and how they influence user experience in streaming and playback scenarios.

https://www.edsurge.com/

EdSurge - features articles about online education platforms, tools, and collaborative learning methods.

https://www.eff.org/
Electronic Frontier Foundation (EFF) - is a nonprofit organisation that focuses on defending civil liberties in the digital world. They provide resources on privacy, surveillance, and ethical considerations surrounding technology use.

https://www.epa.gov/
Environmental Protection Agency (EPA) - offers information on the environmental impact of technology, including e-waste and energy consumption.

https://ec.europa.eu/info/law/law-topic/data-protection_en
European Union – GDPR - The official EU website provides detailed information about the General Data Protection Regulation (GDPR), including its principles, rights, and obligations.

https://fpf.org/
Future of Privacy Forum - addresses the ethical implications of emerging technologies, particularly regarding privacy.

https://www.gartner.com/
Gartner - provides extensive research and analysis on IT systems and emerging technologies. Their reports can be valuable for understanding market trends and making informed choices about IT systems.

https://edu.gcfglobal.org/en/
GCFGlobal - offers free tutorials on various technology topics, including operating systems and software types. https://edu.gcfglobal.org/en/

https://scholar.google.com/
Google Scholar - is a research database where students can find academic papers on various topics, including online services and consumer behaviour.

https://hbr.org/store/case-studies
Harvard Business Review - Case Studies - provides insights into real-world case studies across various sectors, including technology's impact on efficiency and outcomes.

https://www.hse.gov.uk/
Health and Safety Executive (HSE) - provides guidelines and regulations related to health and safety in the workplace, including ergonomic practices for display screen equipment.

https://www.howstuffworks.com/

HowStuffWorks - offers detailed articles and explanations about how different technologies work, including peripheral devices and assistive technologies.

https://www.howtogeek.com/
How-To Geek - offers articles and tutorials on various tech topics, including connection types and their performance impacts.

https://www.ibm.com/cloud/learn
IBM Cloud Learn Hub: provides comprehensive resources on cloud computing models, including detailed explanations of IaaS, PaaS, and SaaS, as well as private, public, and hybrid clouds.

https://www.ibm.com/watson
IBM Watson - provides resources and case studies on artificial intelligence and other emerging technologies.

https://idebate.net/
idebate - used to promote and facilitate debate education and competition, providing resources and support for students and educators to enhance their debating skills and critical thinking.

https://ieeexplore.ieee.org/
IEEE Xplore Digital Library - provides access to research papers and articles on networking technologies and their performance implications.

https://ico.org.uk/
Information Commissioner's Office (ICO) - is the UK's independent authority set up to uphold information rights. Their website contains resources on data protection legislation and the implications for organisations

https://www.infosecinstitute.com/
Infosec Institute - provides educational resources on various cybersecurity topics, including threat analysis and security policies.

https://iapp.org/resources/
International Association of Privacy Professionals (IAPP) - offers comprehensive resources on data protection, privacy laws, and best practices.

https://www.kaspersky.com/resource-center
Kaspersky - features articles on various data protection techniques, including antivirus and firewall solutions. It also provides insights on the effectiveness of free versus paid antivirus options.

https://www.kaspersky.com/resource-center/threats

Kaspersky - provides comprehensive information on various cybersecurity threats, including articles on data breaches, malware, and social engineering tactics.

https://www.khanacademy.org/
Khan Academy - is a widely recognised online learning platform that offers a variety of free courses, lessons, and practice exercises across multiple subjects, including math, science, arts, and computer programming.

https://www.lifewire.com/
Lifewire - provides clear explanations and practical advice on technology topics, including networking and connection types.

https://learn.microsoft.com/en-us/
Microsoft Learn - provides resources and tutorials for understanding operating systems, user interfaces, and software applications.

https://www.technologyreview.com/
MIT Technology Review - offers in-depth articles and insights into emerging technologies and their implications for society and business.

https://www.ncsc.gov.uk/
National Cyber Security Centre (NCSC) - provides guidance on various cyber threats and best practices for organisations to protect their data and systems.

https://www.networkworld.com/
Network World - covers news, analysis, and insights on networking technologies, including connection types and their impacts on IT performance.

https://www.statista.com/topics/871/online-shopping/
Online Retail Services - provides insights into different online retail platforms, their features, and consumer behaviours, making it a great resource for understanding online shopping habits.

https://www.pewresearch.org/
Pew Research Center - conducts studies on technology trends and public perceptions of emerging technologies.

https://www.podcastinsights.com/
Podcast Insights - offers resources on creating and marketing podcasts.

https://privacyinternational.org/
Privacy International - is an advocacy organisation that promotes and defends the right to privacy across the globe. Their website includes articles, reports, and case studies on privacy issues related to technology.

https://privacyrights.org/data-breach
Privacy Rights Clearinghouse - offers resources on data breaches, including case studies and their impacts on individuals and organisations.

https://quizlet.com/
Quizlet - allows users to create and access quizzes and flashcards on various topics, including software concepts and operating systems.

https://www.security.org/
Security.org - provides articles on online privacy, security measures, and risks associated with different online platforms.

https://sproutsocial.com/insights/
Sprout Social - offers insights and resources about social media platforms, user engagement, and analytics.

https://www.statista.com/
Statista - offers statistics and data on a wide range of industries and topics. It serves as an excellent resource for students to find both primary and secondary data, enhancing their understanding of data manipulation and its applications in business and research.

https://www.surveymonkey.com/
SurveyMonkey - is a digital survey tool that allows users to create and distribute surveys easily.

https://techcrunch.com/
TechCrunch - provides the latest news on emerging technologies, startups, and trends in the tech industry.

https://www.techopedia.com/
Techopedia - offers articles that explain the technical features, benefits, and limitations of various digital devices.

https://techterms.com/
TechTerms - provides clear definitions and explanations of various technology terms, including peripheral devices, input/output devices, and storage media characteristics.

https://tdwi.org/
The Data Warehouse Institute (TDWI) - offers resources and articles on data management, analytics, and the importance of data accuracy.

https://thehackernews.com/
The Hacker News - covers the latest cybersecurity news, including incidents of data breaches and analyses of various threats.

https://www.nist.gov/
The National Institute of Standards and Technology (NIST) - provides guidelines and resources related to IT system security and standards. Their publications can enhance discussions on security implications and best practices in IT system management.

https://tutsplus.com/tutorials/video-codecs-explained--cms-25412
Tuts+ (Envato) - provides tutorials and articles on video production, including how different codecs affect video quality and file sizes.

https://www.gov.uk/data-protection
UK Government - Data Protection and Privacy – the official government site provides information on data protection laws in the UK, including the General Data Protection Regulation (GDPR) and the Data Protection Act. It is an essential resource for understanding legal implications related to data protection.

https://enterprise.verizon.com/resources/reports/dbir/
Verizon Data Breach Investigations Report (DBIR) - This annual report analyses data breaches and security incidents, providing real-world case studies.

https://webaim.org/
WebAIM - focuses on web accessibility and provides information about assistive technologies, including screen readers and text-to-speech software.

https://www.weforum.org/
World Economic Forum (WEF) - publishes articles and reports on the impact of technology on society, including environmental issues and access to technology.

Textbooks

Laudon, K. C. & Laudon, J. P., Management Information Systems: Managing the Digital Firm, Pearson, 2018 (ISBN 978-0-13-480157-0)

O'Brien, J. A. & Marakas, G. M., Management Information Systems, McGraw-Hill Education, 2016 (ISBN 978-0-07-337683-1)

Rainer, R. K. & Turban, E., Introduction to Information Systems: Supporting and Transforming Business, Wiley, 2018 (ISBN 978-1-118-03868-0)

Shelly, G. B. & Vermaat, M. E., Discovering Computers: Digital Technology, Data, and Devices, Cengage Learning, 2018 (ISBN 978-1-305-25800-0)

Stair, R. & Reynolds, G. W., Principles of Information Systems, Cengage Learning, 2017 (ISBN 978-1-305-24845-2)

Turban, E., Volonino, L., & Wood, G., Information Technology for Management: On-Demand Strategies for Performance, Growth and Sustainability, Wiley, 2015 (ISBN 978-1-119-07488-1)

Pearson paid resources also available

- Pearson Student book
- ActiveBook (a digital version of the Student Book, via ActiveLearn Digital Service)
- Digital Teacher Pack (via ActiveLearn Digital Service)

Unit 2: Cyber Security and Incident Management

Unit overview

Unit 2: Computer Network Security and Encryption	
Assessment type: External	
Content Area	**Topics**
A: Cyber security threats, system vulnerabilities and security protection methods	A1 Cyber security threats A2 System vulnerabilities A3 Legal responsibilities A4 Software and hardware security measures
B: Use of networking architectures and principles for security	B1 Network types B2 Network components B3 Networking infrastructure services and resources
C: Cyber security documentation	C1 Internal policies
D: Forensic procedures	D1Forensic collection of evidence D2 Systematic forensic analysis of a suspect system
Assessment overview The unit will be assessed through one examination of 90 marks lasting 2 hours 15 minutes. Students will be assessed through a number of short- and long-answer questions. Students will need to explore and relate to contexts and data presented. The questions will assess understanding of cyber security threats, the methods used to counter them and the forensics used to investigate an attack. The assessment availability is twice a year in January and May/June. The first assessment availability is May/June 2026. Sample assessment materials will be available to help centres prepare students for assessment.	

Common misconceptions

Below are some common misconceptions related to the content of this unit by students and ideas for how you can help your learners to avoid and overcome these.

What is the misconception?	How to help learners overcome it
Cyber security is primarily about technical controls.	Demonstrate how human behaviour affects security. Have learners develop both technical and non-technical controls.
Backup and disaster recovery are the same thing.	Create clear comparisons between backup and disaster recovery. Have learners develop both backup and disaster recovery plans.
Small organisations don't need comprehensive security policies.	Use case studies of small business security breaches. Help learners develop scaled-appropriate policies.
If we have antivirus software installed, our system is completely secure.	Demonstrate through case studies how systems with antivirus were still compromised. Show how security requires multiple layers (defences in depth).
Security policies are just documents that nobody reads.	Show how policies prevent incidents and allow organisations to discipline users for unsafe practices.
GDPR only applies to large organisations.	Clarify GDPR scope and requirements. Show examples of small business compliance.
MAC addresses can't be spoofed	Show practical examples of MAC spoofing; Demonstrate why MAC filtering isn't sufficient security; Explain proper network access controls
Updates only add features and aren't security critical	Share examples of major breaches due to missing patches; Demonstrate vulnerability exploitation; Show how patches address security flaws

Learning Activities and Resources

This section offers a starting point for delivering the unit by outlining a logical sequence through the unit topics and suggesting practical activities and teacher guidance for covering the main areas of content during guided learning time. Transferable skills are integrated into various activities, with those embedded in a unit indicated by an acronym in square brackets. The acronym combines the letters from the broad skill area and the specific transferable skill, e.g., [IS-WC].

Please note the activities provided below are suggestions and not mandatory. Pearson is not responsible for the content of any external internet sites. It is essential that you preview each website before using it to ensure the URL is still accurate, relevant, and appropriate.

Learning Topic	Activities and guidance for unit content delivery	Resources
A1 Cyber security threats A1.1.1 Employee sabotage, deliberate and accidental	**Whole class teaching and learning – Introduction** ○ Introduce the concept of cyber security threats by explaining the difference between internal and external threats. ○ Encourage learners to consider how different threats, such as employee sabotage or accidental errors, affect data security and business operations. ○ Use case studies to show real-life examples of companies that have faced security breaches due to internal threats. ○ Encourage a class discussion about how internal threats might differ in terms of intent (deliberate or accidental) and how they can manifest within a company. Learners can share their thoughts on how organisations can protect themselves from such risks. **Small group activity – Employee sabotage, deliberate damage and accidental damage** ○ Each group will be given a scenario where internal threats could occur e.g. employee sabotage, accidental mistakes, theft of physical equipment, loss of data). Their task is to:	National Cyber Security Centre (NCSC): Provides guidance on managing insider threats and safeguarding data within the UK. https://www.ncsc.gov.uk/ Get Safe Online: Offers practical advice for preventing internal cybercrime through user education and policy enforcement in the UK. https://www.getsafeonline.org/ Talk Talk cyber attack. You can use this case to highlight how internal threats (e.g., poor internal security management) and external cyber-attacks overlap. Learners can discuss the legal, financial, and operational impacts.

	○ analyse the scenario ○ pinpoint potential internal threats ○ outline the possible consequences for the organisation. ○ After analysis, groups will present their findings, including suggestions on how to mitigate these threats. **Whole class teaching and learning – Unauthorised software and its impact** ○ Explain the impact of using unauthorised software within an organisation. ○ Discuss the legal and liability implications of software use, especially in cases where the software is unlicensed or incompatible with the company's systems. ○ Use examples of software that could interfere with the running of the network or other critical software and explore how such unauthorised programs might be used for illegal activities, spying, or avoiding monitoring. ○ Encourage learners to reflect on the importance of legal compliance in the use of software, and how unauthorised software could pose significant security risks. **Paired activity – Legal and liability issues in software use** ○ Learners will research a specific case where a company faced legal or security issues due to the use of unauthorised software. ○ Each pair will summarise the situation and outline the legal consequences faced by the organisation. Pairs will present their case study to the class, discussing how these issues relate to the broader topic of internal threats in cyber security.	https://ico.org.uk/about-the-ico/media-centre/talktalk-cyber-attack-how-the-ico-investigation-unfolded/ FAST is a UK organisation that campaigns against software piracy and provides support for organisations to remain compliant with software licensing laws. https://fast.org/

A1.1.2 Accidental or deliberate damage	**Whole class instruction teaching and learning – Introduction to accidental and deliberate damage** ○ Introduce the topic of accidental and deliberate damage within organisations by explaining the different types of incidents that can lead to system damage. ○ Emphasise how incidents like fires, floods, power loss, and acts of terrorism can either happen by accident or be caused deliberately. ○ Discuss how such events can lead to data loss, operational downtime, and financial repercussions for companies. Use case studies to illustrate real-world examples where companies faced substantial losses due to accidental or deliberate damage and discuss the differences between the two types of damage. ○ **Small group – Scenario analysis: Identifying risk and impact** ○ Provide each group with a scenario where accidental or deliberate damage has affected an organisation's IT infrastructure (e.g., power loss due to equipment failure, or intentional damage through an act of sabotage). ○ Ask groups to: ○ Identify the type of damage (accidental or deliberate) in the scenario ○ Discuss the immediate and long-term impact on the organisation ○ Propose strategies the organisation could implement to mitigate these risks ○ Have each group present their scenario and analysis to the class, promoting active engagement and critical thinking. ○ **Pair activity – Exploring disaster recovery strategies** ○ In pairs, learners will research different disaster recovery strategies used to prepare for accidental or deliberate damage, such as offsite backups, redundancy systems, and emergency response protocols.	This a link that includes UK-specific guidance and real examples. It's freely accessible and includes sections on backing up data, protection from malware, and keeping devices safe - all relevant to accidental and deliberate damage. https://www.ncsc.gov.uk/collection/small-business-guide This ICO link provides real examples of UK data breaches and incidents. https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/personal-data-breaches-a-guide/

	○ Each pair will choose one strategy to summarise and discuss its effectiveness in protecting data and reducing downtime. ○ Afterward, each pair will present their strategy, explaining its relevance to the scenario and its potential limitations.	
A1.1.3 Weak cyber security measures and unsafe practices	**Whole class instruction teaching and learning - Introduction** ○ Introduce the concept of weak cyber security measures and unsafe practices by discussing their impact on organisations, including risks of data breaches and compromised systems. **Small group activity - Identifying weak practices** ○ In small groups, learners will be given a scenario that includes weak cyber security practices, such as unvetted visitor access or accessing untrustworthy websites on company devices. Groups should: ○ Identify weak practices in the scenario. ○ Discuss potential risks and consequences. ○ Propose steps the organisation could take to improve security practices. Each group will present their findings to the class, explaining how their recommendations could reduce vulnerabilities. **Pair activity - Evaluating security measures** ○ Assign each pair a different cyber security measure (e.g., equipment security, visitor screening). ○ Have learners research the importance of their assigned measure and examine real-world cases where weaknesses in this area led to security incidents. Each pair will then present a summary to the rest of the class.	UK Government Security Policy Framework - Real examples of security measures and practices used in government organisations. https://www.gov.uk/government/publications/security-policy-framework

A1.1.4 Accidental loss or disclosure of data/credentials	**Whole class instruction teaching and learning - Introduction** ○ Introduce the concept of accidental data loss or disclosure by discussing common causes, such as human error, negligence, and inadequate training. ○ Discuss the potential consequences for organisations, including financial, reputational, and legal impacts. Invite learners to think about how simple mistakes could have significant effects on data security. **Small group activity - Case study analysis** ○ Divide learners into small groups and provide each group with a case study involving accidental data loss or disclosure (e.g., an employee sending private customer data to an unintended recipient). Each group should: ○ Identify the cause(s) of the data loss in the case. ○ Analyse the impact on the organisation and affected individuals. ○ Suggest preventive measures that could have reduced the risk of accidental data loss. **Pair activity - Assessing human factors** ○ In pairs, learners will explore how human factors contribute to data loss or disclosure. ○ Each pair will choose one factor (e.g., poor training, inadequate monitoring, weak security culture) to research further. ○ They will provide a brief summary on how this factor can lead to accidental data breaches and propose solutions to address it. ○ Each pair will present their findings to the rest of the class.	Case study: https://www.itgovernance.co.uk/blog/public-health-wales-accidentally-publishes-18000-coronavirus-patients-data

A1.2.1 Malicious software (malware)	**Whole class instruction teaching and learning - Introduction** ○ Introduce malware by explaining its different types, including viruses, worms, trojans, spyware, and ransomware. Engage learners in discussing recent malware attacks in the news and their impacts on businesses and individuals. **Small group activity - Malware matching game** ○ Divide learners into small groups and provide each group with a set of cards. ○ Each card features either a type of malware, a characteristic, a symptom, or a real-world example of a malware attack. ○ Learners will work together to match the malware type with its characteristics, symptoms, and example. ○ After completing the activity, groups will present one matched set to the class and briefly explain it. **Pair activity - Malware prevention research** ○ In pairs, assign learners a specific type of malware (e.g., ransomware, spyware, trojans) and ask them to research current methods to prevent or mitigate that malware type. ○ Each pair will summarise their findings, focusing on practical actions such as using antivirus software, updating software regularly, or avoiding suspicious downloads. ○ Pairs will then share their findings with another pair, promoting peer-to-peer learning and reinforcing malware prevention strategies.	Crowdstrike global threat report. https://go.crowdstrike.com/global-threat-report-2024.html CompariTech UK Ransomware Stats - Regular updates on UK malware incidents with detailed analysis of attack patterns and costs to businesses. https://www.comparitech.com/blog/information-security/
A1.2.2 Hacking – commercial, government, individuals	**Whole class instruction teaching and learning - Introduction** ○ Begin with an overview of hacking, including its different motivations and targets (e.g., commercial, government, and individuals).	Motivations of a Hacker: This article explores the different reasons behind hacking activities, such as financial gain, political motives, and personal satisfaction. It provides

	○ Use real-life examples, such as notable commercial data breaches, government espionage cases, and personal identity theft incidents, to illustrate the scope of hacking. ○ Lead a class discussion on how the goals of hackers might vary by target, and introduce common techniques like phishing, DoS/DDoS attacks, and database breaches. **Small group activity - Hacker profile analysis** ○ Divide learners into small groups and assign each group a "hacker profile" (e.g., hacktivist, cybercriminal, state-sponsored hacker, insider). ○ Each group will research and create a profile, identifying the hacker's motivations, common methods, and typical targets. ○ Groups will present their profiles to the class, helping learners understand the diverse types of hackers and the specific threats each poses to different entities.	insights into how these motivations influence the choice of targets, including commercial entities, governments, and individuals. https://focusgroup.co.uk/resources/blog/motivations-of-a-hacker
A1.2.3 Sabotage – commercial, government, individuals, terrorism	**Whole class instruction teaching and learning - Introduction** ○ Introduce the concept of sabotage, explaining how it differs from other forms of cyber threats. ○ Discuss types of sabotage that target commercial entities, government infrastructures, individuals, and critical systems in terrorism-related attacks. ○ Use visual aids to outline different sabotage techniques (e.g., data tampering, system destruction, malware insertion) and illustrate the potential impacts on society, business continuity, and national security. ○ Prompt learners to consider how motives for sabotage may vary depending on the target.	Sabotage: National Security Bill Factsheet This UK government factsheet outlines the growing threat of sabotage, including cyber sabotage, and the legislative measures being introduced to counter such threats. It provides insights into the legal framework and the importance of safeguarding national security. https://www.gov.uk/government/publications/national-security-bill-factsheets/sabotage-national-security-bill-factsheet

	Small group activity - Sabotage scenario analysis ○ In small groups, assign each group a different type of sabotage scenario (e.g., corporate espionage in a commercial context, infrastructure attacks targeting government, personal data sabotage, and terrorist-driven attacks on critical systems). ○ Groups should: ○ Analyse the potential impact of their assigned scenario. ○ Identify vulnerabilities that made the sabotage possible. ○ Suggest protective measures to prevent similar incidents. Each group will present their findings, explaining both the immediate and broader implications of their sabotage scenario. **Individual activity - Sabotage defence planning** ○ For this activity, learners will act as security advisors tasked with drafting a basic defence plan for a specific sector (commercial, government, individual, or counterterrorism). ○ Each learner will choose one type of target and outline a simple plan detailing key security measures to prevent sabotage (e.g., access controls, network monitoring, staff training).	Great-Power Offensive Cyber Campaigns: Experiments in Strategy This research paper from the International Institute for Strategic Studies examines offensive cyber operations by major powers, including case studies of cyber sabotage. It offers an in-depth analysis of strategies and their implications for national security. https://www.iiss.org/research-paper/2022/02/great-power-offensive-cyber-campaigns/
A1.2.4 Social-engineering techniques used to obtain secure information by deception.	**Whole class instruction teaching and learning - Introduction** ○ Begin by explaining social-engineering techniques in general, focusing on the psychological tactics used to deceive people into providing secure information. ○ Describe common methods such as phishing, smishing, pretexting, and baiting. ○ Use visual aids or diagrams to show how each technique operates and the typical steps involved in a social-engineering attack. ○ Discuss the importance of awareness and vigilance as primary defences against these tactics.	10 Types of Social Engineering Attacks https://www.crowdstrike.com/en-us/cybersecurity-101/social-engineering/types-of-social-engineering-attacks/ Social Engineering Awareness Kit https://www.terranovasecurity.com/resources/guides/social-engineering-training-kit

	Individual activity - Creating a warning infographic ○ Learners will choose one social-engineering technique (e.g., phishing or pretexting) and create a simple infographic that explains the technique, signs to watch out for, and ways to avoid it. ○ They can outline steps for recognising and responding to the method, aiming to make their infographic both clear and informative. ○ After completion, each pair can display their infographic in the classroom or submit it for feedback.	
A1.2.5 Physical security	**Whole class instruction teaching and learning - Introduction** ○ Introduce learners to physical security in cyber security. Discuss the importance of protecting physical assets like hardware, secure areas, and devices from unauthorised access and theft. ○ Explain common physical security breaches, such as tailgating, forced entry, and device theft, and the potential impacts on organisational security. **Whole class activity - Physical security walk-through** ○ Take learners on a guided walk around the school or organisation, examining physical security measures like fences, gates, locks on doors, and surveillance cameras. ○ Instruct learners to observe how each feature could either prevent or enable unauthorised access. ○ Encourage them to consider what improvements might be necessary to increase physical security.	Physical Security and Cybersecurity: How They Work Together This article discusses the integration of physical security and cybersecurity measures, highlighting the importance of a holistic approach to protect sensitive assets. It provides insights into how physical security controls, such as access control systems and surveillance cameras, complement cybersecurity protocols. https://www.lenels2.com/en/news/insights/Physical_and_Cybersecurity.html Physical Security video series: https://www.youtube.com/watch?v=j9MQMVn3FV4

	Pair activity - Think-pair-share on security measures ○ Learners pair up to discuss and evaluate various physical security methods (e.g., CCTV, biometric systems, secure cabling) and their effectiveness. Each pair will: ○ Identify two physical security measures from the previous activities. ○ Evaluate the pros and cons of these methods for securing devices and areas. ○ After discussing, each pair will share their evaluations with the class. **Individual activity - Security improvement proposal** ○ Learners will write a brief report reflecting on the security walk-through and the small group discussions. Each learner will: ○ Identify two physical security improvements they believe are necessary. ○ Justify their selections by describing how these improvements could reduce specific security risks. ○ Propose steps for implementing each improvement.	
A1.3.1 Operational loss	**Whole class instruction teaching and learning - Introduction** ○ Introduce the concept of operational loss in the context of cyber security. ○ Explain how operational losses affect an organisation's ability to function, often resulting from security incidents that disrupt manufacturing output, service availability, and data access. ○ Use examples like system downtime, service interruptions, and productivity impacts to illustrate operational losses.	Cyber Case Study: Colonial Pipeline Ransomware Attack This case study examines the Colonial Pipeline breach, highlighting its impact on supply chains and critical infrastructure. It underscores the necessity of robust cybersecurity systems and protocols to prevent and respond to such attacks. https://coverlink.com/case-study/cyber-

	Whole class activity - Case study analysis ○ Present a real-world case study where an organisation experienced operational loss due to a cyber security incident (e.g., ransomware attack, DoS attack on service availability). Lead a class discussion on: ○ The causes of the operational loss. ○ The types of operations impacted (e.g., data unavailability, service outages). ○ How the organisation responded and recovered. Encourage learners to consider how different sectors (e.g., healthcare, finance) may experience unique impacts from operational loss.	case-study-colonial-pipeline-ransomware-attack/
A1.3.2 Financial loss	**Whole class instruction teaching and learning - Introduction** ○ Introduce the topic of financial loss as a result of cyber security incidents, covering both direct and indirect financial impacts. ○ Discuss how financial loss can stem from causes such as service disruption, data breaches, theft, and fines. ○ Explain specific types of financial impacts, including loss of profits, increased insurance costs, compensation to affected customers, and legal penalties. **Individual activity - Risk assessment and reflection** ○ Learners will complete a risk assessment exercise and write a reflection on financial loss prevention. Each learner will: ○ Identify a potential cyber threat and its associated financial risks. ○ Assess the financial impact this threat could have on a hypothetical organisation. ○ Propose two proactive strategies for reducing or managing financial loss from this threat.	Financial Loss Exposure of Cyber Risks Across Industries This article from the World Economic Forum discusses the economic drivers and impacts of cyber risks. https://www.weforum.org/stories/2023/03/how-does-your-industry-compare-when-it-comes-to-the-financial-impact-of-cyber-threats/ Rising Cyber Threats Pose Serious Concerns for Financial Stability The International Monetary Fund explores the increasing risk of extreme losses from cyber incidents. https://www.imf.org/en/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability

	○ Reflect on the importance of financial loss mitigation as part of a comprehensive cyber security strategy.	
A1.3.3 Reputational loss	**Whole class instruction teaching and learning - Introduction** ○ Introduce learners to reputational loss, explaining how cyber incidents can damage an organisation's public image, customer trust, and overall credibility. Discuss the importance of reputation for businesses and the long-term impacts of reputational damage, such as reduced customer loyalty, negative media coverage, and declining market share. **Individual activity - Reputational recovery plan** ○ Learners will develop a brief reputational recovery plan based on a hypothetical cyber incident. Each learner will: ○ Describe a potential cyber incident and its likely reputational impact on the organisation. ○ Outline at least two actions the organisation could take to recover its reputation (e.g., issuing public apologies, improving cyber defences). ○ Reflect on the importance of maintaining a positive reputation and consider how strong cyber practices can contribute to trustworthiness.	Cyber claims case study: Reputational repercussions This case study explores the reputational harm and financial loss experienced by a small online retailer following a data breach, highlighting the challenges even smaller companies face in maintaining customer loyalty after such incidents. https://www.cfc.com/en-gb/knowledge/resources/case-studies/uk-cyber-claims-case-studies/cyber-claims-case-study-reputational-repercussions-uk/
A1.3.4 Intellectual property loss	**Whole class instruction teaching and learning - Interactive modelling** ○ Introduce intellectual property (IP) and discuss how it can be targeted by cyber threats. ○ Use an interactive modelling approach where learners participate in mapping out a "threat model" for a mock organisation. ○ Invite learners to brainstorm different types of intellectual property (e.g., software code, product designs) and potential	Teaching Intellectual Property Through Interactive Methods: This article suggests engaging strategies for teaching IP concepts, such as competitions and creative projects, to help students grasp the importance of IP protection. https://www.tes.com/magazine/sponsored/intellectual-property-office/7-

	threats (e.g., hacking, employee theft, accidental leaks). This helps learners visualise the different types of IP, the threat landscape, and methods of protection. **Whole class activity - Gallery walk on IP protection methods** ○ Set up several stations around the room, each featuring a different IP protection method (e.g., encryption, restricted access, employee NDAs, IP tracking technology). ○ Include information on how each method works, its benefits, and any limitations. Have learners rotate between stations, reading and taking notes on each method. ○ Conclude with a class discussion where learners share insights and discuss which methods they found most effective and why.	unexpected-ways-teach-intellectual-property
A1.4.1 National Cyber Security Centre (NCSC) UK	**Whole class instruction teaching and learning - Introduction** ○ Introduce the National Cyber Security Centre (NCSC) and explain its role in protecting UK organisations, public services, and individuals from cyber threats. ○ Discuss how the NCSC provides resources, updates, and guidance to improve national cyber resilience. Emphasise the importance of foundational cyber security knowledge for all staff and how the NCSC training can build awareness and practical skills. **Whole class activity - Overview and training setup** ○ Walk the learners through an overview of the NCSC Cyber Security Training for Staff by showing them the website and introducing the key topics it covers, such as passwords, phishing, and device security. ○ Ensure learners know the objectives of the training, which are to understand basic cyber security practices and recognise common security threats in professional settings. ○ Provide learners with the training link:	

	https://www.ncsc.gov.uk/training/v4/Top+tips/Web+package/content/index.html#/ ○ Explain the expectations: each learner should complete the training independently, taking notes on key practices and tips they learn. **Individual activity - NCSC cyber security training completion** ○ Learners will independently complete the NCSC Cyber Security Training online. They should take notes on: ○ Key tips for securing information and devices. ○ Methods to identify phishing attempts and suspicious communications. ○ Strategies for creating and managing strong passwords. ○ Encourage learners to reflect on how these principles apply not only to organisational settings but also to personal cyber security.	
A1.4.2 National Institute of Standards and Technology (NIST) USA	**Whole class instruction teaching and learning - Introduction** ○ Introduce learners to the National Institute of Standards and Technology (NIST), explaining its role in developing standards and guidelines to enhance cyber security, especially within the USA. ○ Highlight the significance of NIST frameworks in guiding organisations on best practices for managing cyber risks and establishing resilient cyber defences. ○ Mention key publications, such as the NIST Cybersecurity Framework (CSF), and discuss how it is used internationally to improve security practices.	The National Institute of Standards and Technology (NIST) is a U.S. agency that develops standards and guidelines to enhance cybersecurity across various sectors. A key publication is the NIST Cybersecurity Framework (CSF), which outlines five core functions: Identify, Protect, Detect, Respond, and Recover. https://www.nist.gov/cyberframework

	Whole class activity - Interactive modelling of the NIST Cybersecurity Framework o Guide learners through the five core functions of the NIST Cybersecurity Framework (Identify, Protect, Detect, Respond, Recover). o Create an interactive session where learners help model these functions for a hypothetical organisation, identifying the key actions and practices each function entails (e.g., identifying assets, protecting data, detecting threats). o Use real-world examples to show how each function applies to organisational security practices. **Individual activity - Research task on NIST resources** o Assign learners an independent research task to explore a specific NIST resource or publication (e.g., NIST's guidelines on IoT security, password management, or incident response planning). Each learner will: o Write a brief summary of the resource, including its main recommendations. o Identify one practical tip or recommendation that could be beneficial for daily or organisational use. o Reflect on how international frameworks like NIST can influence cyber security practices worldwide. **Whole class discussion - NIST vs. UK Cybersecurity Standards** o Conclude with a class discussion comparing NIST's guidelines to UK cyber security standards, such as those promoted by the National Cyber Security Centre (NCSC). Discuss questions like: o What similarities and differences exist between NIST and UK guidelines?	

	○ How can UK organisations benefit from international standards like those provided by NIST? ○ Why is it beneficial for organisations globally to reference multiple cyber security frameworks? ○ Encourage learners to consider the importance of international collaboration in cyber security.	
A1.4.3 Open Web Application Security Project (OWASP)	**Whole class instruction teaching and learning - Introduction** ○ Introduce learners to the Open Web Application Security Project (OWASP), explaining its mission to improve software security worldwide by providing freely accessible resources. ○ Highlight the significance of the OWASP Top 10, which identifies the most critical security risks to web applications and explain how it serves as a foundational tool for developers and security professionals. **Whole class activity - OWASP Top 10 overview and interactive discussion** ○ Present the OWASP Top 10 risks (such as injection attacks, broken authentication, and security misconfigurations). Divide the class into groups and assign each group one of the OWASP Top 10 risks to research briefly and explain in simple terms. As each group presents their assigned risk to the class, discuss: ○ Why each risk poses a threat to web security. ○ Real-life examples of these vulnerabilities, if applicable. ○ This collaborative introduction will provide learners with a baseline understanding of common web application vulnerabilities.	OWASP Official Website: Offers an overview of OWASP's mission to enhance software security globally through freely accessible resources. https://owasp.org/ OWASP Top 10 Project: Details the most critical web application security risks, serving as a foundational tool for developers and security professionals. https://owasp.org/Top10/

A2 System vulnerabilities A2.1.1 Network (vulnerabilities)	**Whole class instruction teaching and learning - Demonstration and interactive modelling** ○ Introduce the concept of network vulnerabilities and discuss why identifying and addressing these weaknesses is essential to cyber security. ○ Explain common vulnerabilities such as open ports, weak firewall settings, and unpatched software. ○ Use a network diagram to model potential vulnerabilities in a typical organisation's network, such as exposed devices or insufficient access controls. **Pair activity - Think-pair-share on network vulnerability mitigation** ○ In pairs, learners will brainstorm ways to mitigate the network vulnerabilities discussed in class. Each pair will: ○ Choose one common network vulnerability, such as open ports or weak access controls. ○ Identify two or three security measures that could address or prevent this vulnerability (e.g., closing unused ports, implementing strong firewall rules, regular software updates). ○ Share their findings with the class, explaining how their chosen mitigation techniques would protect the network. **Individual activity - Research and report on a network vulnerability** ○ Learners will select a specific network vulnerability (e.g., Denial of Service (DoS) risks, weak encryption protocols, or unpatched software) and conduct research to deepen their understanding. Each learner will: ○ Write a summary explaining the vulnerability, how it occurs, and its potential impacts on a network.	Common Network Vulnerabilities: This resource outlines prevalent network vulnerabilities, such as unpatched software flaws, weak passwords, and open ports, and discusses their implications for businesses. https://heimdalsecurity.com/blog/common-network-vulnerabilities/ Network Security Threats and Vulnerabilities: Provides insights into various network security threats, including phishing and malware, and explains how these vulnerabilities can be exploited. https://www.eccouncil.org/cybersecurity-exchange/network-security/network-security-threats-vulnerabilities/

	○ Provide a real-world example of an attack or incident involving this vulnerability. ○ Recommend at least two practical mitigation strategies that organisations could use to address this vulnerability.	
A2.1.2 Organisational (vulnerabilities)	**Whole class instruction teaching and learning - Introduction** ○ Begin by explaining organisational vulnerabilities, highlighting risks that arise from internal processes, policies, and human factors. ○ Discuss examples such as inadequate access controls, weak password policies, insufficient training, and poor security culture. Use examples of real-world incidents where internal vulnerabilities led to security breaches, underscoring the importance of addressing these risks within an organisation. **Small group activity - Problem-solving task on access control issues** ○ Divide learners into small groups and present a scenario where an organisation's access control policy is weak (e.g., employees have excessive permissions, no distinction between user roles, or a lack of two-factor authentication). ○ Each group will: ○ Identify specific security risks that could arise from these weak access controls. ○ Discuss the potential consequences of unauthorised access to sensitive information or systems. ○ Develop a revised access control policy to address these risks, incorporating measures such as role-based access, least privilege, and multi-factor authentication.	Weak Security Controls and Practices Routinely Exploited for Initial Access: This advisory highlights common internal vulnerabilities, such as inadequate access controls and unpatched software, that have been exploited in real-world incidents, underscoring the need for robust internal security measures. https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-137a

A2.1.3 Software (vulnerabilities)	**Whole class instruction teaching and learning – Introduction** ○ Introduce software vulnerabilities by discussing the risks of untrustworthy software sources, malware-laden installers, and security gaps in unpatched systems. ○ Use a real-world example of a recent software vulnerability (e.g., zero-day exploit in a popular application) to demonstrate how software issues can expose organisations to security threats. **Pair activity – Exploring zero-day exploits** ○ Pairs will research a famous zero-day exploit, such as the WannaCry ransomware attack or a high-profile SQL injection incident. ○ Each pair will create a short summary of the exploit, its effects, and how it could have been mitigated with better software practices. **Individual activity – vulnerability tracking journal** ○ Learners will start a journal to track current software vulnerabilities reported by organisations like the National Cyber Security Centre (NCSC) or Open Web Application Security Project (OWASP). ○ Each entry should summarise a new vulnerability, its potential risks, and mitigation advice. ○ Learners will review their journals periodically, discussing trends they observe in software vulnerabilities and learning to stay updated with evolving threats.	Risks and Vulnerabilities of Unpatched Software: This article discusses the dangers of unpatched software, including malware infections and compliance violations, highlighting the importance of regular updates. https://www.splashtop.com/blog/risks-and-vulnerabilities-of-unpatched-software Zero-Day Exploit Examples (2024): The 10 Worst Attacks Ever: Lists significant zero-day exploits, including the Code Red Worm, detailing their impact and lessons learned. https://softwarelab.org/blog/zero-day-exploit-examples
A2.1.4 Operating system, Graphical User Interface (GUI) and Command Line Interface (CLI) (vulnerabilities)	**Whole class instruction teaching and learning - Introduction** ○ Introduce the concept of vulnerabilities associated with operating systems, focusing on GUI and CLI aspects. Discuss how outdated operating systems, missing patches, or incorrect security settings can expose systems to risks.	Operating System Vulnerabilities: Understanding and Mitigating the Risk: This article provides an overview of common operating system vulnerabilities, including those associated with GUIs and CLIs, and

	○ Highlight the differences between GUI and CLI in terms of user access and control, noting how each interface type may introduce unique vulnerabilities. **Individual activity - Vulnerability awareness poster** ○ Ask learners to create a poster on an OS vulnerability of their choice (such as missing patches, end-of-life OS versions, or misconfigured security settings). ○ They should design the poster to educate others on what the vulnerability is, why it's dangerous, and how to protect against it. ○ Encourage creativity—learners can use drawings, catchy slogans, or quick safety tips. ○ Display the posters around the classroom or school as a fun and visible reminder of key cyber security concepts.	offers strategies for mitigation. https://sternumiot.com/iot-blog/operating-system-vulnerabilities-understanding-and-mitigating-the-risk/
A2.1.5 Mobile devices reliant on Original Equipment Manufacturers (OEMs) to update system software (vulnerabilities)	**Whole class instruction – Introduction** ○ Introduce the topic by explaining how OEMs control software updates for mobile devices and the risks associated with delayed or unsupported updates (e.g., increased vulnerability to malware). ○ Use a "lifecycle timeline" on the board or wall, marking stages from device release, active updates, end-of-support, and potential risks as updates stop. **Small group activity - "update or upgrade?" debate** ○ Divide learners into small groups and assign each group a scenario with a mobile device that is near end-of-support. ○ Their task is to debate whether to update the device as long as updates are available, upgrade to a newer device, or continue using the outdated version despite the risks. ○ Each group should consider factors like cost, security, and usability. Afterward, groups present their decisions, and the class discusses the pros and cons of each choice.	Phone Update Policies from Every Major Company: Offers an overview of various manufacturers' update policies, highlighting the differences in support duration and frequency. https://www.androidauthority.com/phone-update-policies-1658633/

A2.1.6 Physical (vulnerabilities)	**Whole class instruction - "Guess the vulnerability" classroom tour** ○ Create mock stations around the classroom, each representing a physical vulnerability related to device security (e.g., an unlocked device left unattended, a USB device lying around, or a mobile phone without a case in a crowded space). ○ As a class, take a tour to each station and ask learners to guess the physical vulnerability and discuss potential security implications. **Individual activity - Design a physical security "quick guide" card** ○ Each learner creates a small "quick guide" card listing practical tips for avoiding physical vulnerabilities (e.g., never leave devices unattended, use locks for laptops, be mindful of shoulder surfers). ○ After designing, learners can swap cards to see each other's ideas and combine them into a class set of best practices.	Physical Security Threats & Vulnerabilities: This article discusses common physical security threats, such as unauthorized access and theft, and their implications for device security. https://www.charter-global.com/common-physical-security-threats/
A2.1.7 Process of how people use the system (vulnerabilities)	**Whole class instruction - "Spot the vulnerability" scenarios** ○ Begin with a few short, relatable scenarios on the board where improper use of a system could lead to vulnerabilities. ○ Examples might include sharing passwords, leaving devices logged in and unattended, or clicking on unknown links. ○ As a class, discuss each scenario, asking learners to identify the vulnerability and suggest ways to avoid it. **Pair activity - "Think before you click" checklist** ○ In pairs, have learners brainstorm situations where users might accidentally create vulnerabilities, such as responding to phishing emails, accessing suspicious links, or plugging in unknown USBs. ○ Each pair creates a checklist of questions users should ask themselves before taking these actions, like "Is this email from a trusted source?" and "Do I know where this USB came from?"	Security Awareness and Behaviour Explained in 5 Minutes: Offers a concise overview of security awareness and behaviour, including practical tips for users to enhance their security practices. https://apmg-international.com/article/security-awareness-and-behaviour-explained-5-minutes

	○ They can exchange checklists with other pairs to gather additional ideas. **Individual activity - "Day in the life" vulnerability journal** ○ Ask each learner to keep a journal for a day, noting moments where they interact with devices or systems (e.g., logging in to a computer, using Wi-Fi, or saving passwords). ○ They should identify any actions that might pose security risks and write suggestions on how to handle these situations more securely. ○ This self-reflective activity helps learners become more aware of their own habits and promotes responsibility in safe system use.	
A2.1.8 Security implications of cloud computing and of the Internet of Things (IoT) devices	**Whole class instruction teaching and learning - Introduction** ○ Introduce the topic of security implications in cloud computing and IoT by discussing how these technologies have transformed data storage, device management, and connectivity. ○ Explain the risks associated with these advancements, such as weak encryption, data interception, and dependence on third-party providers. ○ Use examples to illustrate potential vulnerabilities in each area and encourage learners to consider the ways these issues affect personal privacy and organisational security. **Small group activity - Cloud and IoT risk analysis** ○ In small groups, learners will analyse assigned scenarios that involve either cloud computing or IoT devices, focusing on vulnerabilities such as data movement over public networks, insecure default settings, and lack of patch management. ○ Each group will identify specific security risks in their scenario, discuss potential impacts, and propose solutions to enhance security.	Top IoT Device Vulnerabilities: How To Secure IoT Devices: This resource outlines common IoT vulnerabilities, including limited computational abilities and lack of built-in security, and provides recommendations for securing IoT devices. https://www.fortinet.com/resources/cyberglossary/iot-device-vulnerabilities

	○ Groups will then present their findings to the class, taking part in a collective discussion on best practices for cloud and IoT security.	
A2.2 Where to find up-to-date sources of information on specific known hardware and software vulnerabilities.	**Whole class instruction teaching and learning - Introduction** ○ Introduce the importance of staying informed about current hardware and software vulnerabilities. ○ Discuss how new vulnerabilities are discovered frequently and how organisations and IT professionals rely on authoritative sources to maintain security. ○ Explain the role of well-known organisations such as the National Cyber Security Centre (NCSC), National Institute of Standards and Technology (NIST), and industry-specific forums. ○ Provide examples of the types of vulnerabilities these sources report, such as zero-day exploits or newly patched security issues. **Pair activity - Comparing vulnerability resources** ○ In pairs, learners will compare two vulnerability resources (e.g., NIST vs. OWASP). ○ They will consider factors such as update frequency, accessibility, focus areas, and reliability. ○ Each pair will outline the strengths and limitations of each resource and discuss scenarios where one resource might be preferred over the other. ○ Pairs will then share their comparisons with the class to generate a discussion on which resources are most useful in different security contexts.	National Vulnerability Database (NVD): Managed by the National Institute of Standards and Technology (NIST), the NVD is the U.S. government's repository of standards-based vulnerability management data. https://nvd.nist.gov/ Common Vulnerabilities and Exposures (CVE) List: The CVE system provides a reference method for publicly known information-security vulnerabilities and exposures. https://www.cve.org/
A2.3.1 Attack vectors: Wireless	**Whole class instruction teaching and learning - Introduction** ○ Begin with an overview of wireless networks, including Wi-Fi, Bluetooth, and other wireless protocols.	Wireless Attacks: This article provides an overview of common wireless attacks, including rogue access points, Wi-Fi denial-of-service attacks, and jamming, highlighting their

	○ Explain how these networks differ from wired connections and introduce common wireless attack vectors, such as eavesdropping, man-in-the-middle attacks, Evil Twin attacks, and wireless sniffing. ○ Use examples to illustrate how attackers exploit these vulnerabilities and discuss the potential consequences for individuals and organisations. **Small group activity - Identifying wireless attack scenarios** ○ Divide learners into small groups and provide each group with a specific wireless attack vector (e.g., Evil Twin attack, Bluetooth eavesdropping, Wi-Fi sniffing). ○ Each group will analyse a scenario where their assigned attack could occur, identify the conditions that make the attack possible, and discuss the potential security impact. ○ Groups will then present their scenarios and findings to the class, explaining how each type of attack compromises data or network security. **Pair activity - Securing wireless networks** ○ In pairs, learners will research security measures to protect against wireless attack vectors, such as using WPA3 encryption, disabling unused network protocols, and setting up Virtual Private Networks (VPNs). ○ Each pair will create a list of recommended security practices for organisations or individuals to prevent wireless attacks. ○ Pairs will share their recommendations with the class, contributing to a collaborative list of best practices for wireless security.	mechanisms and potential impacts. https://www.codecademy.com/article/wireless-attacks Ensuring Wireless Network Security: Tips and Best Practices: Offers practical advice on securing both residential and business Wi-Fi networks, emphasizing the importance of strong passwords, network segmentation, and the use of Virtual Private Networks (VPNs). https://dig8ital.com/post/wireless-security-101/

A2.3.2 Attack vectors: Internet Connection	**Whole class instruction teaching and learning – introduction** ○ Introduce the concept of internet connection vulnerabilities by explaining how different internet connection types (e.g., copper cable, optical fibre, Wi-Fi, cellular/5G) can become potential attack vectors for cyber threats. ○ Use examples to illustrate how each type can be exploited, such as Wi-Fi eavesdropping, or vulnerabilities within 5G networks. ○ Facilitate a class discussion on why internet connections are common targets for cyber attacks, touching on risks associated with various connection devices like modems and routers. **Small group activity – threat mapping exercise** ○ Organise learners into small groups and assign each group an internet connection type or device (e.g., Wi-Fi routers, 5G networks). ○ Their task is to create a "threat map" by identifying specific attack vectors and threats for their connection type, such as packet sniffing for Wi-Fi or spoofing for routers. ○ Each group will then devise a visual diagram or map showing how these threats connect and potential mitigation strategies. ○ Groups will present their threat maps to the class, discussing the risks and protections for each connection.	Potential Threat Vectors to 5G Infrastructure: This report by the Cybersecurity and Infrastructure Security Agency (CISA) explores and prioritizes potential threat vectors associated with 5G networks, providing insights into vulnerabilities and mitigation strategies. https://www.cisa.gov/sites/default/files/publications/potential-threat-vectors-5G-infrastructure_508_v2_0%20%281%29.pdf
A2.3.3 Attack vectors: Internal network access devices	**Whole class instruction teaching and learning – Demonstration and discussion** ○ Start with a demonstration of different internal network access devices (e.g., routers, switches, wireless access points) and explain how they can become entry points for cyber attacks. ○ Use visual aids or a live demo to illustrate common attack vectors such as unauthorised access through misconfigured routers, exploiting outdated firmware on switches, or eavesdropping on traffic via insecure wireless access points.	What are Attack Vectors: Definition & Vulnerabilities: This article defines attack vectors and discusses how cybercriminals exploit vulnerabilities in network devices to infiltrate systems. https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/attack-vector/

	○ Facilitate a discussion on why internal network security is crucial, especially in protecting sensitive organisational data. **Pair activity – Network device hardening plan** ○ In pairs, learners will select a network device, such as a wireless access point or router, and create a "hardening" plan. ○ Their plan should include steps to secure the device (e.g., changing default passwords, enabling WPA3 encryption, disabling unused ports). ○ Each pair will summarise their plan in a brief report, highlighting which vulnerabilities their measures address and how these steps would protect against potential attacks.	Network Hardening: Best Practices & Techniques: Offers guidance on implementing security protocols and measures to fortify network defences, including securing open ports and conducting vulnerability assessments. https://www.businesstechweekly.com/cybersecurity/network-security/network-hardening/
A2.4 Types and uses of tools and methods to assess the vulnerabilities in computer systems	**Whole class instruction teaching and learning – Introduction** ○ Introduce learners to vulnerability assessment concepts by discussing how tools like port scanners, network mappers, website vulnerability scanners, and vulnerability detection software function. ○ Use screenshots, videos, or simulations (such as YouTube demonstrations) to show each tool's interface and how it identifies vulnerabilities, covering common findings like open ports, unpatched software, and weak configurations. ○ Discuss the types of threats these vulnerabilities expose systems to, emphasising the ethical and legal considerations around using these tools. **Small group activity – Vulnerability tool research project** ○ Divide learners into small groups, assigning each group one vulnerability assessment tool (e.g., port scanner, network mapper, registry checker). ○ Each group will research their assigned tool's purpose, common uses, and any specific threats it helps mitigate.	Vulnerability Assessment Tools: Key Features and 5 Tools You Should Know: This article provides an overview of essential features in vulnerability assessment tools and highlights five notable examples, discussing their purposes and functionalities. https://brightsec.com/blog/vulnerability-assessment-tools-key-features-and-5-tools-you-should-know/

	○ They should also investigate a real-life example where the tool was used to prevent or respond to an attack. ○ Groups will then create a short presentation to teach their classmates about their tool, including visuals or case study summaries. **Pair activity – Vulnerability assessment tools presentation** ○ In pairs, learners will research and create a presentation on different types of vulnerability assessment tools, focusing on each tool's purpose, functionality, and application in identifying security risks. ○ Learners will present to the whole class and ask/answer questions.	
A2.5 Use of independent third-party review of a system and network designs before implementation	**Whole class instruction teaching and learning - Introduction** ○ Directly introduce the concept of independent third-party review in system and network security. ○ Explain the importance of third-party assessments in verifying the robustness of security designs before implementation, emphasising due diligence and third-party certification. ○ Use examples of well-known certifications (e.g., ISO/IEC 27001) and discuss their role in building trust for customers and stakeholders by meeting industry standards. **Pair activity - Research task: certification standards** ○ Learners will work in pairs to research and summarise the key requirements and benefits of a security certification standard (such as ISO/IEC 27001 or SOC 2). ○ Each pair will outline how these certifications help in achieving secure designs and the steps organisations must take to be certified. ○ Pairs will then share a short summary with the class, promoting a broader understanding of various certification options.	Pivot Point Security provides network architecture reviews and security assessments. Their services aim to minimise risks by verifying the design and operation of key architectural and operational controls intended to secure systems, applications, and data. https://www.pivotpointsecurity.com/services/network-architecture-review/

	Individual activity - Reflection exercise ○ Learners will write a short reflection on the importance of third-party security reviews in safeguarding against risks. ○ They should consider how these reviews can prevent oversights in system design and their role in overall cyber security strategy, particularly in risk management and trust-building.	
A2.6 Applications and features of penetration testing for common threats, those in the Open Web Application Security Project (OWASP) top 10.	**Whole class instruction teaching and learning - Introduction** ○ Introduce the concept of penetration testing as a method for proactively identifying vulnerabilities in network and system security. ○ Explain the difference between penetration testing and vulnerability scanning and discuss how penetration testing aligns with industry standards like the OWASP Top 10. ○ Highlight specific OWASP Top 10 threats, such as injection flaws, broken authentication, and cross-site scripting, and describe how they are commonly tested. **Small group activity - Simulated penetration test planning** ○ Divide learners into small groups and assign each group a hypothetical company with a unique set of potential vulnerabilities. ○ Their task is to create a basic penetration testing plan to address threats relevant to their assigned company, referencing at least three OWASP Top 10 vulnerabilities. ○ Groups will outline specific testing methods they would use (e.g., SQL injection tests, cross-site scripting checks) and detail the types of reports and findings they would expect. ○ Groups will then present their plans to the class, encouraging peer feedback.	OWASP Top 10 for WebApp Penetration Testing: This article discusses how the OWASP Top 10 can be effectively leveraged in penetration testing, providing a roadmap to understanding and mitigating web applications' most critical security risks. https://www.stationx.net/owasp-top-10-penetration-testing/

A2.7 Passive risk management measures	**Whole class instruction teaching and learning - Introduction** ○ Introduce the concept of passive risk management measures, explaining how these strategies allow organisations to mitigate risks without active intervention. ○ Cover the three main approaches: risk transfer (e.g., insurance or outsourcing), risk avoidance (e.g., stopping risky activities), and risk acceptance (deciding to bear the cost or impact of certain risks). ○ Provide real-world examples, such as using cyber insurance to transfer risk or stopping the use of unsupported software to avoid risk. **Pair activity - Cost-benefit analysis of passive measures** ○ Each pair of learners will choose one passive risk management strategy and research its potential costs and benefits. ○ For example, a pair studying risk transfer might analyse the cost of cyber insurance premiums versus the financial impact of a potential data breach. ○ Pairs will then present their analysis, focusing on how businesses decide between passive strategies and their importance in a broader risk management framework. **Individual activity - Reflection on organisational risk tolerance** ○ Learners will individually write a reflection on how an organisation's tolerance for risk impacts its choice of passive risk management measures. ○ They should consider questions like: When might it be acceptable to "accept" a risk? When might an organisation decide that transferring or avoiding risk is the best approach?	Risk Response Strategies: Mitigation, Transfer, Avoidance, Acceptance: This article provides an overview of various risk response strategies, including passive measures such as risk transfer, avoidance, and acceptance, with practical examples. https://twproject.com/blog/risk-response-strategies-mitigation-transfer-avoidance-acceptance/
A3 Legal responsibilities	**Whole class instruction teaching and learning - Introduction** ○ Begin with an overview of the main legislation governing cyber security and data protection, focusing on the General Data	Data Protection and Cybersecurity Laws in the UK | CMS Expert Guide: Provides an overview of data protection and

A3.1 Current legislation A3.2 Areas the legislation applies to	Protection Regulation (GDPR) and the Computer Misuse Act 1990. ○ Explain key principles of GDPR, such as data processing consent, data minimisation, and individuals' rights to access and erase personal data. Introduce the Computer Misuse Act, covering unauthorised access, modification, and its implications for cyber security professionals. ○ Discuss how compliance with these laws affects day-to-day operations and responsibilities in organisations. **Pair activity - Legislation comparison** ○ In pairs, learners will compare GDPR and the Computer Misuse Act. Each pair will outline the main objectives and coverage of both laws and explore the differences in scope, focus, and penalties. ○ For instance, GDPR emphasises data protection and privacy rights, while the Computer Misuse Act focuses on preventing unauthorised access and tampering. ○ Pairs will share their comparisons with the class, promoting a deeper understanding of the legislation landscape.	cybersecurity laws in the UK, detailing the scope and application areas of GDPR and the Computer Misuse Act. https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/united-kingdom Data Protection Self Assessment | ICO: The Information Commissioner's Office offers checklists to assess compliance with data protection laws, helping organisations ensure they are keeping personal data secure. https://ico.org.uk/for-organisations/advice-for-small-organisations/checklists/data-protection-self-assessment
A3.3.1 General Data Protection Regulation (GDPR)	**Whole class instruction teaching and learning - Introduction** ○ Introduce GDPR and its core purpose of protecting personal data and privacy rights within the European Union. ○ Explain key GDPR principles, including lawfulness, fairness, and transparency in data processing; data minimisation; accuracy; storage limitation; and integrity and confidentiality. ○ Discuss legal bases for data processing, such as consent, legitimate interest, and contractual obligation. ○ Use examples of real-world GDPR violations and consequences to emphasise the importance of compliance, both financially and reputationally.	Case studies and examples | ICO: A collection of case studies illustrating various data protection scenarios, including GDPR compliance challenges and resolutions. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/case-studies-and-examples/

	Pair activity - GDPR case studies ○ Provide each pair with a GDPR-related case study in which a company faced fines or sanctions due to non-compliance (e.g., data breach or inadequate consent procedures). ○ Each pair will analyse the case, identify specific GDPR violations, and discuss what the organisation could have done to avoid non-compliance. ○ Pairs will then share their insights with the class, encouraging learners to think critically about GDPR requirements and common compliance challenges.	
A4 Software and hardware security measures A4.1.1 Physical security measures	**Whole class instruction teaching and learning - Introduction** ○ Introduce the concept of physical security measures and their importance in protecting an organisation's resources from unauthorised access, theft, or damage. ○ Use visual aids to demonstrate different physical security tools, such as locks, biometric scanners, and CCTV. Highlight the different types of physical security tools like card entry systems, biometrics, and protected cabling, explaining how each offers specific levels of protection suited to different organisational needs. ○ Facilitate a class discussion on why physical security is essential for organisations and encourage learners to consider potential risks in areas without these protections. **Small group activity - Identifying security needs** ○ Each group will receive a scenario, such as a company office, a data centre, or a public-access network hub. ○ In their groups, learners will identify physical security needs for their assigned location and select appropriate security tools (e.g., RFID badges, CCTV, locked storage). ○ Each group will present their security plan to the class, explaining their reasoning.	A Guide to Physical Security: Controls, Tools, and Examples: This resource explores various physical security controls and tools, providing examples to enhance understanding of their application in different scenarios. https://www.lenels2.com/en/news/insights/the-ultimate-guide-to-physical-security.html Physical Security: Planning, Measures & Examples An in-depth guide covering the fundamentals of physical security, including planning strategies, various measures, and practical examples. https://www.avigilon.com/blog/physical-security-guide

	○ After each presentation, allow time for peer feedback and discussion of alternative solutions, including the strengths and weaknesses of each approach. **Pair activity - Security measure research** ○ Each pair will research a specific physical security technology, such as biometric authentication or magnetic stripe readers. ○ They will investigate how the technology functions, its advantages, and any potential limitations. ○ Each pair will prepare a short summary of their findings to present to the class, discussing how their assigned measure would protect against specific physical security threats (e.g., tailgating, forced entry). **Individual activity - Reflective journal** ○ Learners will write a reflective journal entry about the impact of physical security measures on overall cybersecurity. ○ They should consider questions such as: ○ Which physical security measures do they think are most effective, and why? ○ How might they apply these insights in future cybersecurity planning? ○ Encourage learners to explore how physical security complements IT security measures in protecting organisational assets and access control.	
A4.1.2 Data storage, data protection and backup, and recovery procedures	**Whole class instruction teaching and learning - Introduction** ○ Introduce the importance of data storage, data protection, and backup and recovery procedures in ensuring data security and continuity of operations. ○ Explain different types of backups (e.g., full, differential, incremental) and strategies (e.g., onsite, offsite, cloud).	Incremental vs. Differential vs. Full Backup - A Comparison Guide An analytical comparison of the three primary backup methods, discussing their advantages, disadvantages, and suitable applications to aid in selecting the most appropriate strategy for

	○ Demonstrate how backup and recovery procedures function, using visual aids or case studies of organisations that successfully recovered from data loss due to robust backup strategies. ○ Facilitate a class discussion on the potential risks of inadequate backup procedures, including data loss and business disruption. **Small group activity - Backup strategy planning** ○ Each group will be given a specific organisational scenario (e.g., small business, large enterprise, healthcare provider). ○ Their task is to design a backup and recovery plan that includes backup types, storage locations, and recovery methods suitable for their assigned organisation. ○ Groups should consider factors such as data sensitivity, frequency of updates, and storage capacity. ○ Each group will present their backup plan to the class, explaining the reasoning behind their choices. ○ Encourage questions and peer feedback on the practicality and security of each approach.	different organisational needs. https://www.acronis.com/en-us/blog/posts/incremental-differential-backups Incremental, full and differential backups explained. https://www.youtube.com/watch?v=o-83E6levzM
A4.1.3 Antivirus software and detection techniques	**Whole class instruction teaching and learning - Introduction** ○ Introduce the role of antivirus software in cybersecurity, explaining how it detects, quarantines, and removes malware. ○ Cover key detection techniques, such as signature-based detection, heuristics, and file integrity checks. ○ Use examples to show how antivirus software operates and its limitations, particularly with newer or evolving malware. ○ Facilitate a class discussion about the importance of keeping antivirus software up-to-date and the potential consequences of unaddressed malware threats in an organisation.	How Antivirus Works? | 6 Methods Antivirus Software Used to Work A comprehensive guide on the various methods antivirus software utilises to detect and prevent malware, including heuristic analysis and automatic updates. https://antivirus.comodo.com/blog/computer-safety/how-antivirus-works/ Advanced Technologies at the Core of Microsoft Defender Antivirus

	Pair activity - Research on antivirus software features ○ Each pair will research a specific feature or capability of antivirus software (e.g., real-time scanning, sandboxing, automatic updates). ○ They will investigate how this feature contributes to malware detection and prevention, as well as any limitations it might have. ○ Each pair will prepare a short summary to share with the class, discussing how this feature would be useful in an organisational context and why organisations might choose antivirus solutions with these specific capabilities. **Individual activity - Reflective journal** ○ Learners will write a reflective journal entry on the importance of antivirus software in protecting organisational assets. ○ They should consider questions such as: ○ Which detection techniques do they think are most effective, and why? ○ How would they ensure that an organisation's antivirus software remains effective over time? ○ Encourage learners to reflect on the evolving nature of malware and the importance of adapting antivirus strategies to meet new threats.	This technical documentation explores the sophisticated technologies underpinning Microsoft Defender Antivirus, including machine learning models, behaviour monitoring, and cloud-based protection. https://learn.microsoft.com/en-us/defender-endpoint/adv-tech-of-mdav
A4.1.4 Software and hardware firewalls and the filtering techniques they use	**Whole class instruction teaching and learning - Introduction** ○ Introduce firewalls as a fundamental aspect of network security and highlight the differences between software and hardware firewalls. ○ Use a diagram to explain core filtering techniques, such as packet filtering, stateful inspection, and application layer filtering, showing how each technique controls data flow.	Types of Firewalls Defined and Explained This resource provides an overview of various firewall types, including software and hardware firewalls, and details filtering techniques such as packet filtering, stateful inspection, and application-layer filtering.

	○ Discuss examples of real-world firewall breaches and their impact, encouraging learners to consider why effective firewall configurations are essential for organisations. **Pair activity - Firewall rule-making exercise** ○ In pairs, learners will create a set of firewall rules to protect a fictional small business network from specific threats (e.g., unauthorised access, malware infiltration, data theft). ○ They will need to decide which filtering techniques to apply and justify their choices. Pairs will exchange their firewall rules with another pair to review and offer feedback. ○ After receiving peer input, each pair will revise their rules to improve security measures. **Individual activity - Firewall quiz and self-assessment** ○ Learners will complete an interactive quiz or assessment on firewall concepts, types, and filtering techniques, testing their knowledge on packet filtering, stateful inspection, and real-world application of firewall rules. ○ After completing the quiz, they will review and analyse their answers to identify any areas where they need further understanding. ○ Learners write a brief reflection on how they could apply what they learned to a real-world setting.	https://www.paloaltonetworks.com/cyberpedia/types-of-firewalls Stateless vs Stateful Packet Filtering Firewalls An in-depth comparison between stateless and stateful packet filtering firewalls, explaining their operational differences and implications for network security. https://www.geeksforgeeks.org/stateless-vs-stateful-packet-filtering-firewalls/
A4.1.5 User authentication	**Whole class instruction teaching and learning - Introduction** ○ Introduce the concept of user authentication and its importance in verifying identity to secure network and system access. ○ Explain different authentication factors, such as knowledge (passwords), possession (security tokens), and inherence (biometrics).	Authentication Methods: Choosing the Right Type This guidance from the UK's National Cyber Security Centre (NCSC) explores various authentication methods, including knowledge-based (passwords), possession-based (security tokens), and inherence-based

	○ Demonstrate examples of single-factor and multi-factor authentication (MFA) and discuss the strengths and weaknesses of each method. ○ Lead a discussion about why organisations might require MFA and what considerations are involved in choosing authentication methods. **Individual activity - Creating a personal authentication plan** ○ Learners will develop a personal authentication plan for their own online accounts, choosing secure authentication methods where available (e.g., enabling MFA for email and social media accounts, using a password manager). ○ They will write a reflection on their chosen methods, considering questions like: ○ Why did they choose these methods? ○ How do these choices increase their personal cybersecurity?	(biometrics), providing insights into their strengths and weaknesses. https://www.ncsc.gov.uk/guidance/authentication-methods-choosing-the-right-type
A4.1.6 Access controls and the methods to restrict users' access to resources	**Whole class instruction teaching and learning - Introduction** ○ Introduce the concept of access control as a means of managing and limiting user access to resources within an organisation. ○ Explain different access control models, such as Discretionary Access Control (DAC), Role-Based Access Control (RBAC), and Rule-Based Access Control. ○ Use examples to illustrate how each model restricts access based on user roles, rules, or discretionary permissions, and discuss why organisations implement access controls to protect sensitive data and resources. ○ Facilitate a discussion on how access control is essential in preventing unauthorised access and reducing security risks.	Access Control Models: MAC, DAC, RBAC, & PAM Explained This article provides an overview of various access control models, including Mandatory Access Control (MAC), Discretionary Access Control (DAC), Role-Based Access Control (RBAC), and Privileged Access Management (PAM). It discusses the advantages and disadvantages of each model, aiding in understanding their applications within organisations. https://www.twingate.com/blog/other/access-control-models

	Small group activity - Access control scenario planning ○ Divide learners into small groups, giving each group a unique organisational scenario (e.g., a hospital, a financial institution, an educational institution). ○ Each group will determine the best access control model(s) to implement for their scenario, justifying their choice based on specific needs and security risks. ○ Groups should also outline roles and permissions for different types of users in their scenario (e.g., administrators, employees, guests). ○ Afterward, each group will present their access control plan to the class, allowing time for questions and feedback.	
A4.1.7 Trusted computing	**Whole class instruction teaching and learning - Introduction** ○ Introduce the concept of trusted computing, explaining how it aims to enhance system security by building trust into hardware and software. ○ Cover key components such as the Trusted Platform Module (TPM), secure boot processes, and the role of digital certificates. ○ Discuss the benefits of trusted computing, such as improved security and integrity, alongside its drawbacks, such as reduced user control and potential privacy concerns. ○ Encourage learners to share their initial impressions of the balance between security and control in trusted computing. **Individual activity - Trusted computing infographic creation** ○ Learners will create an infographic on a trusted computing feature (e.g., TPM, secure boot, or digital certificates). ○ They will research and summarise how the feature works, its benefits for security, and any common concerns or limitations.	Trusted Platform Module (TPM) Summary This summary offers insights into the TPM's functionality, including its ability to securely store artefacts used for platform authentication, such as passwords, certificates, and encryption keys. https://trustedcomputinggroup.org/resource/trusted-platform-module-tpm-summary

	○ Each learner will share their infographic with the class in a gallery walk, allowing peers to view and ask questions about each feature. ○ This activity reinforces understanding and encourages creativity in summarising technical information visually.	
A4.1.8 Finding lost or stolen devices	**Whole class instruction teaching and learning - Introduction** ○ Introduce methods and tools used to locate and secure lost or stolen devices, such as GPS tracking, remote lock/wipe functions, and "phone home" software. ○ Demonstrate how these tools work and explain the importance of device location and security features in protecting sensitive data. ○ Discuss real-life examples where organisations successfully used these technologies to recover devices or prevent data breaches, emphasising the risks involved if security features are not activated. **Small group activity - Scenario analysis: lost laptop with military information** ○ Divide learners into small groups and present them with the following scenario: ○ *A government employee has lost a laptop that contains classified military information. The laptop was left unattended in a public place and is now missing. The organisation must respond quickly to secure the data and mitigate potential risks.* ○ Each group will develop a response plan, addressing the following key points: ○ Discuss the steps the employee and organisation should take to report the missing laptop, including notifying supervisors, IT security, and relevant government authorities. ○ Determine the steps to remotely wipe or lock the laptop to prevent unauthorised access. The group should identify any pre-	Remote Wipe Data Protection: How It Works This article explains the concept of remote wipe, detailing how it functions across various operating systems like Android, iOS, and Windows through Mobile Device Management (MDM) tools or built-in features. https://preyproject.com/blog/what-is-remote-wipe-and-why-you-might-need-it Selective Wipe for Corporate Data: In scenarios where it's necessary to remove only corporate data while preserving personal information, Intune provides a selective wipe option. This action targets company data within managed apps, leaving personal data intact. Selective wipe is particularly useful for Bring Your Own Device (BYOD) policies, ensuring that corporate information is protected without affecting personal content. https://learn.microsoft.com/en-us/mem/intune/apps/apps-selective-wipe

	configured security measures (e.g., remote wipe software, two-factor authentication) that would be activated in this situation. o Consider and discuss the potential consequences of the loss, including: o Delays or changes in military operations due to compromised plans or intelligence. o Possible exposure of classified data to adversaries and the risks of espionage. o Potential legal impacts, public relations challenges, and the effect on public trust in government security practices. o Each group will present their response plan, explaining their choices and highlighting the importance of each step. o Following the presentations, encourage a class discussion on how the response plan could be improved and how organisations can better prepare for such incidents. **Pair activity - Security feature analysis** o Each pair will investigate the security features of a particular device type or operating system (e.g., iOS, Android, Windows, MacOS) with a focus on options for tracking, locking, and wiping devices. o Pairs will create a short guide outlining the steps for enabling and using these features, highlighting any advantages and limitations. o They will then exchange guides with another pair to review and provide feedback.	
A4.1.9 Device based security	**Whole class instruction teaching and learning - Introduction** o Introduce the concept of device-based security measures designed to protect individual devices from unauthorised access.	Face, Iris, Fingerprint, Password, or PIN: Which Is Most Secure? This article compares different authentication methods—biometric

	○ Discuss common security features such as screen timeouts, timed lockouts, and memory wipe after failed login attempts. ○ Highlight the importance of these features for protecting sensitive data on devices, especially in scenarios where devices are lost or stolen. ○ Use examples to illustrate how these security features work in different environments, such as corporate settings or personal devices. **Pair activity - Security feature research and comparison** ○ In pairs, learners will research two different security features or configurations commonly available on devices (e.g., biometric authentication vs. PIN, screen lock vs. timed auto-wipe). ○ Each pair will compare the strengths, weaknesses, and ideal applications of each feature and create a summary table or poster illustrating their findings. **Individual activity - Security habits assessment** ○ Learners will assess their own device security habits, such as the type of lock screen they use, password complexity, and backup routines. ○ In a reflective journal entry, they will evaluate the effectiveness of their current device security practices and identify at least two changes they could implement to improve their security. ○ Encourage them to think about potential risks, such as device theft or unauthorised access, and how their habits could reduce those risks. **Whole class wrap-up - Best practices discussion** ○ Conclude with a class discussion on the best practices for device-based security. ○ Ask learners to share insights from their activities and summarise the most effective security measures they identified.	and traditional—discussing their strengths, weaknesses, and suitable applications to help users make informed security choices. https://www.makeuseof.com/face-iris-fingerprint-password-pin-most-secure/ PIN or Biometrics, Which Is Most Secure? This resource analyses the security aspects of PINs versus biometric authentication, providing insights into their effectiveness and potential vulnerabilities. https://www.nextauth.com/pin-or-biometrics-which-is-most-secure/

A4.2.1 Storage encryption	**Whole class instruction teaching and learning - Introduction** ○ Introduce storage encryption, explaining how it secures data by converting it into an unreadable format that can only be accessed with an encryption key. ○ Discuss different types of storage encryption, such as file-level, disk-level, and database encryption, and the importance of encryption standards like AES (Advanced Encryption Standard). ○ Use examples to show how encryption protects data at rest on devices, drives, and in cloud storage environments. ○ Discuss real-life situations where encryption protected data after device loss or theft. **Individual activity - encryption features comparison table** ○ Learners will independently create a table comparing different storage encryption methods (e.g., AES, RSA, file-level encryption, full-disk encryption). The table should include columns for: ○ Encryption Method ○ Description ○ Strengths ○ Limitations ○ Typical Use Cases ○ Encourage learners to refer to classroom resources or research online to complete the table.	Cryptographic Storage Cheat Sheet - OWASP This resource provides guidelines on implementing cryptographic storage solutions, covering encryption algorithms, key management, and best practices. https://cheatsheetseries.owasp.org/cheatsheets/Cryptographic_Storage_Cheat_Sheet.html Everything You Need to Know About File Encryption | Veritas An overview of file encryption, discussing different encryption approaches, algorithms like AES and RSA, and their applications in securing data. https://www.veritas.com/en/aa/information-center/file-encryption
A4.2.2 Communications encryption	**Whole class instruction teaching and learning - Introduction** ○ Introduce communications encryption, focusing on its role in protecting data in transit. Explain the importance of securing communication channels and discuss common encryption protocols and technologies, such as Transport Layer Security	What is end-to-end encryption (E2EE)? - Cloudflare This resource explains end-to-end encryption, how it works, and its importance in securing communications.

	(TLS), Secure Sockets Layer (SSL), Virtual Private Networks (VPNs), and end-to-end encryption in messaging apps. ○ Use examples, like HTTPS for secure web browsing, to show how communications encryption protects data from interception or tampering. **Individual activity - Communications encryption methods comparison table** ○ Learners will create a table comparing various communications encryption methods, including TLS, SSL, VPNs, and end-to-end encryption. The table should include columns for: ○ Encryption Method ○ Description ○ Purpose ○ Strengths ○ Common Applications **Small group activity - Encrypted communication scenario planning** ○ In small groups, learners will be given different scenarios (e.g., a remote worker connecting to a company server, a team exchanging sensitive emails, a person using a public Wi-Fi network). ○ Each group will choose an appropriate communications encryption method for their scenario and explain why it is suitable. ○ They will outline how the method protects data in transit and address any potential limitations. ○ After the discussion, each group will present their scenario and encryption solution to the class.	https://www.cloudflare.com/en-gb/learning/privacy/what-is-end-to-end-encryption/ Encryption Types, Methods, and Use Cases Explained - Enterprise Networking Planet This article explores different encryption types and methods, including their use cases in securing communications. https://www.enterprisenetworkingplanet.com/security/encryption-types/

A4.3.1 Media Access Control (MAC) address filtering and hiding the Service Set Identifier (SSID)	**Whole class instruction teaching and learning - Introduction** ○ Introduce MAC address filtering and SSID hiding as key techniques in securing wireless networks. ○ Explain the function of each method: MAC address filtering limits network access to specified devices by recognising their unique MAC addresses, while hiding the SSID makes the network name invisible to general scans. ○ Highlight the potential importance of these methods in preventing unauthorised access and reducing the risk of Wi-Fi attacks. ○ Explain the limitations of the methods against a persistent or technical attacker. **Pair activity - Writing a short report with peer review** ○ Each pair will write a short report on the effectiveness of MAC address filtering and SSID hiding in enhancing Wi-Fi security. The report should cover: ○ A brief overview of each method and how it improves security ○ Advantages and potential limitations in practical settings ○ At least one real-world example or case study where these methods were applied, if available ○ After completing the report, pairs will exchange reports with another pair for peer review, focusing on clarity, completeness, and depth of analysis. Each pair will revise their report based on feedback received.	MAC Address Filtering and Hiding SSID Won't Protect Your Wi-Fi Network This article explains why MAC address filtering and SSID hiding are not effective security measures for Wi-Fi networks. https://smallstep.com/blog/mac-address-filtering-and-hiding-ssid-dont-work/ 5 Wi-Fi Security Myths You Must Abandon Now An article that addresses common misconceptions about Wi-Fi security, including the use of MAC address filtering and SSID hiding. https://www.pcworld.com/article/447974/5-wi-fi-security-myths-you-must-abandon-now.html
A4.3.2 Wireless encryption	**Whole class instruction teaching and learning – Introduction** ○ Begin by introducing wireless encryption and its importance in securing wireless networks from unauthorised access.	WEP, WPA, WPA2 and WPA3: Differences and Explanation - Kaspersky This article provides an overview of different Wi-Fi encryption protocols,

	○ Explain the types of encryption methods, with a focus on WPA2 and WPA3, and briefly cover other security measures like Wi-Fi Protected Setup (WPS) and the risks of unsecured access points. ○ Use examples of recent network security breaches to illustrate the potential impact of inadequate wireless security. **Small group activity – Jigsaw Activity** ○ Divide the class into small groups and assign each group a specific aspect of wireless encryption (e.g., WPA2, WPA3, WPS, vulnerabilities of unsecured access points). ○ Each group will research their topic and create a short summary. ○ After the initial research, reorganise the groups so that each new group has a representative from each topic area. ○ Each learner will then teach their topic to the other group members, ensuring everyone gains a comprehensive understanding of wireless encryption methods and vulnerabilities.	including WPA2 and WPA3, explaining their differences and security features. https://www.kaspersky.com/resource-center/definitions/wep-vs-wpa
A4.4 Security issues during network and system design to ensure security is built-in	**Whole class instruction teaching and learning - Introduction** ○ Begin with a lecture on the importance of designing security into network systems from the outset. Introduce principles such as "expect attacks to happen and plan for them" and "design the system to run on the fewest privileges." ○ Explain the risks of relying on secrecy and the benefits of following information security standards, such as ISO 27000. ○ Use examples of well-known data breaches to illustrate how proactive design could have reduced risks. **Small group activity - Security design challenge** ○ Divide learners into small groups and assign each group a hypothetical organisation (e.g., healthcare, finance, or education). ○ Each group will create a network design with built-in security, considering factors like access control, encryption, and compliance standards.	Case Studies: Notable Breaches – Codecademy An analysis of significant data breaches, exploring what happened before, during, and after the attacks, and discussing key takeaways and lessons. https://www.codecademy.com/article/case-studies-notable-breaches Network Security Architecture: Best Practices & Tools – eSecurity Planet This article explores network security architecture, focusing on network configuration and best practices. https://www.esecurityplanet.com/networks/network-security-architecture/

	○ After designing, groups will share their designs with the class and discuss potential strengths and weaknesses. **Pair activity - Podcast on security design principles** ○ In pairs, learners will create a podcast episode explaining how to integrate security into network design. ○ They should cover essential principles such as "expecting attacks" and "compliance with security standards." ○ Encourage pairs to use real-life examples and include advice on avoiding common security pitfalls. **Individual activity - Reflection journal** ○ Learners will complete a journal entry reflecting on the importance of designing security into network systems. ○ They should identify three specific principles they feel are most important and explain why, using examples from the lesson.	Network Infrastructure Security Guide – U.S. Department of Defence This guide provides information on secure network design and configuration. https://media.defense.gov/2022/Jun/15/2003018261/-1/-1/0/CTR_NSA_NETWORK_INFRASTRUCTURE_SECURITY_GUIDE_20220615.PDF
B1 Network Types B1.1.1 Network types B1.1.2 Private network types	**Whole class instruction teaching and learning - Introduction** ○ Introduce the concepts of network types and private network types, covering key definitions and their applications (e.g., Local Area Network [LAN], Wireless Local Area Network [WLAN], Wide Area Network [WAN], Storage Area Network [SAN], and Personal Area Network [PAN] as well as private networks like intranets, extranets, and cloud networks). ○ Use diagrams to illustrate these types, showing differences in size, connectivity, and typical use cases. Encourage learners to discuss the importance of each network type in various settings, such as in schools, hospitals, and large corporations. ○ Highlight cyber security implications associated with each network type, such as the risks associated with WLANs compared to LANs.	Types of Computer Networks: Their Features, Advantages, Disadvantages, and Examples This article offers detailed explanations of different computer networks, including their characteristics, benefits, drawbacks, and practical applications. https://tooabstractive.com/networking/types-of-computer-network-with-example/ Types of Computer Networks - GeeksforGeeks This page discusses various computer network types, including their definitions, purposes, and typical use cases.

	Small group activity - Mind map on network types ○ In small groups, have learners create a mind map for network types. Each group will cover a different network types. Ask learners to include: ○ Definition and purpose ○ Typical use cases ○ Advantages and disadvantages ○ Security considerations ○ Afterward, each group will present its mind map to the class, discussing the network's characteristics and potential vulnerabilities.	https://www.geeksforgeeks.org/types-of-computer-networks/
B1.1.3 Wired and wireless integration	**Whole class instruction teaching and learning - Introduction** ○ Introduce wired and wireless integration by explaining the basics of Ethernet standards within the 802 family, covering both wired and wireless connections. ○ Use network diagrams to illustrate compatibility and interoperability issues, such as signal interference and protocol mismatches. ○ Discuss common integration challenges, including signal strength, interference, channel allocation, and IP address management. ○ Encourage learners to think critically about both technical and administrative aspects of network integration. **Small group activity - Analysing integration issues** ○ Divide learners into small groups and provide each with a network integration scenario (e.g., adding wireless networks to a wired LAN in a corporate setting). Groups will:	Advantages and Disadvantages of Wired and Wireless Networks This resource outlines the pros and cons of wired and wireless networks, providing a basis for discussing integration challenges and solutions. https://tooabstractive.com/networking/wired-and-wireless-network-advantages-and-disadvantages Wired and Wireless Networking - GeeksforGeeks This article explains the differences between wired and wireless networking, including their advantages, disadvantages, and typical use cases, which is useful for understanding integration considerations.

	○ Identify potential compatibility issues, including protocol mismatches or signal interference. ○ Propose solutions for technical and administrative challenges, such as channel selection and IP address allocation. ○ Each group will present their findings and solutions to the class, applying knowledge and analysis skills to real-world scenarios. **Pair activity - Exploring security in network integration** ○ In pairs, learners will research potential security vulnerabilities unique to integrated wired and wireless networks (e.g., access point spoofing or man-in-the-middle attacks). Each pair will: ○ Describe a specific security risk. ○ Suggest preventative security measures, such as encryption protocols or MAC address filtering. ○ Pairs will share their findings with the class, encouraging deeper evaluation of network security within integration contexts.	https://www.geeksforgeeks.org/wired-and-wireless-networking/
B1.1.4 Schematic diagrams	**Whole class instruction teaching and learning - Introduction** ○ Introduce the concept of schematic diagrams by explaining the purpose of logical and physical network diagrams in visualising network structure and components. ○ Use examples to show different network layouts, such as a Local Area Network (LAN) with designated IP addresses and port numbers. ○ Discuss how these diagrams help in identifying network design flaws and enhancing security and troubleshooting processes. ○ Encourage learners to consider how these diagrams support network planning and risk management.	How to Create a Network Diagram | Steps and Expert Tips - Miro This guide outlines the process of creating a network diagram, including defining the scope, gathering information, and using Miro's features to build and refine the diagram. https://miro.com/diagramming/how-to-create-a-network-diagram/ Network Diagrams Guide This guide explains the fundamentals of network diagrams, including common

	Small group activity - Creating and analysing network diagrams ○ In small groups, learners will receive a sample network diagram with missing elements. Each group will: ○ Identify and add missing components (e.g., switches, routers, or access points). ○ Ensure accurate placement of components by applying basic network design principles and labelling IP addresses and port numbers. ○ Groups will present their completed diagrams to the class, explaining their choices and how the diagram supports efficient network management. **Pair activity - Troubleshooting with network diagrams** ○ In pairs, learners will be provided with a pre-designed network diagram containing potential issues (e.g., misconfigured IP addresses or incorrectly placed firewalls). Each pair will: ○ Identify the problem areas. ○ Propose solutions for correcting the issues in the diagram. ○ Pairs will present their findings, explaining how their adjustments improve network functionality and security, encouraging evaluation and problem-solving skills. **Individual activity - Designing a network diagram** ○ Learners will individually design a basic network diagram from scratch for a small office setup. The diagram should: ○ Include necessary components (e.g., computers, servers, routers) with accurate placement. ○ Label each component with an appropriate IP address, subnet, and port number.	pitfalls. It serves as a foundation for creating diagrams with intentional faults for educational purposes. https://nulab.com/learn/software-development/network-diagrams-guide/

	○ Learners will submit their diagrams along with a brief written explanation of how their design supports security and connectivity requirements.	
B1.1.5 Features/ requirements of networks (cyber security related)	**Whole class instruction teaching and learning - Introduction** ○ Introduce the essential features and requirements of secure networks, focusing on key aspects such as scalability, compatibility, performance, backup management, security settings, fault tolerance, and reliability. ○ Explain how each feature impacts the cyber security of networked systems and why these requirements are integral to protecting organisational data and communications. ○ Use examples to illustrate how each requirement functions in real-world networks. **Small group activity - Network requirements analysis** ○ In small groups, learners will review a case study describing an organisation's network setup. ○ They will analyse the network for its scalability, compatibility, backup management, and security settings. ○ Each group should identify potential cyber security weaknesses related to these requirements and suggest improvements. ○ Afterward, groups will present their analyses to the class, allowing peers to ask questions and provide additional insights.	What Is Network Security? Definition and Types | Fortinet This resource provides an overview of network security, detailing various types and their significance in protecting data and ensuring compliance. https://www.fortinet.com/resources/cyberglossary/what-is-network-security
B1.2.1 Physical topologies	**Whole class instruction teaching and learning - Introduction** ○ Introduce the concept of physical network topologies (e.g., star, extended star, hierarchical, wireless mesh, ad-hoc). ○ Use diagrams to illustrate each topology, discussing how physical layouts influence network performance, scalability, and cyber security.	6 Network Topologies Explained & Compared - Comparitech This resource explains different network topologies and compares their impact on performance and reliability. It also touches upon how these topologies affect network security,

	○ Highlight the pros and cons of each topology type in terms of fault tolerance, ease of monitoring, and vulnerability to attacks. **Small group activity - Network topology comparison** ○ Divide learners into small groups, assigning each group a specific topology (e.g., one group focuses on star, another on mesh, etc.). ○ Groups will research the cyber security strengths and weaknesses of their assigned topology, considering aspects like fault tolerance, vulnerability to attacks, and ease of isolating network failures. ○ Each group will create a brief presentation or infographic to share with the class, explaining why an organisation might choose (or avoid) their assigned topology for security reasons. **Pair activity - Topology selection and scenario analysis** ○ In pairs, learners will receive a hypothetical business scenario (e.g., a hospital, a university, or a small business) and choose an appropriate topology based on the scenario's needs. ○ They will justify their choice by discussing factors like data sensitivity, fault tolerance requirements, and network performance. ○ Pairs will then present their selected topology to the class, explaining how it addresses both the functional and security needs of their assigned scenario.	offering a comprehensive view of their pros and cons. https://www.comparitech.com/net-admin/network-topologies-advantages-disadvantages/
B1.2.2 Logical topologies	**Whole class instruction teaching and learning - Introduction** ○ Introduce the concept of logical topologies and explain how they differ from physical topologies, using examples of logical bus and logical ring setups. ○ Discuss how data flows within these logical structures and the implications for network security, fault tolerance, and monitoring.	Difference between Physical and Logical Topology - GeeksforGeeks This article explains the distinctions between physical and logical topologies, providing examples of logical bus and ring setups. It discusses how data flows within these structures and the implications for network performance and security.

	○ Use visual aids to demonstrate data paths and point out potential vulnerabilities associated with each topology. **Individual activity - Research and reflection on logical topologies** ○ Each learner will research a real-world example of a network that uses a logical bus or ring topology. ○ They will write a brief reflection on how the logical structure impacts the security and efficiency of that network, considering factors like vulnerability to eavesdropping, ease of monitoring, and fault isolation. ○ Learners should connect this real-world application to concepts learned in class, discussing any potential risks and benefits of the chosen topology.	https://www.geeksforgeeks.org/difference-between-physical-and-logical-topology/
B1.3 Network architecture	**Whole class instruction teaching and learning - Introduction** ○ Introduce learners to the three primary types of network architecture: peer-to-peer, client/server, and thin client. ○ Discuss how each architecture works, its typical uses, and cyber security considerations. ○ Highlight factors such as data access control, vulnerability to attacks, ease of monitoring, and fault tolerance. ○ Use diagrams to illustrate data flow in each architecture and provide examples of typical use cases (e.g., file sharing for peer-to-peer, web services for client/server). **Small group activity - Architecture evaluation and comparison** ○ Organise learners into three groups, each assigned to one network architecture type (peer-to-peer, client/server, or thin client). ○ Each group will research their architecture, focusing on strengths and weaknesses related to security, reliability, and scalability.	Client Server Architecture: Types, Examples, & Benefits This resource explores the client-server model in detail, including its types, real-world examples, benefits, and associated security considerations. https://www.redswitches.com/blog/client-server-architecture/

	○ Groups should also identify common security challenges for their architecture and discuss solutions or best practices to mitigate these risks. ○ Each group will create a presentation or poster and then present their findings to the class, allowing time for questions and discussion.	
B1.4.1 Virtualisation	**Whole class instruction teaching and learning - Introduction** ○ Introduce virtualisation, focusing on its applications in cybersecurity. ○ Explain key concepts, including segmentation, isolation (sandboxing), and containerisation, highlighting how these techniques enhance network security by reducing the attack surface. ○ Use diagrams to demonstrate how virtualisation separates different environments within a system, and discuss common uses, such as virtual machines (VMs) and containers. **Small group activity - Exploring virtualisation use cases** ○ In small groups, learners will analyse case studies that illustrate virtualisation in different industries (e.g., healthcare, finance, education). Each group will: ○ Identify the types of virtualisation used. ○ Describe how segmentation and isolation protect sensitive data. ○ Discuss potential security risks and the benefits provided by each case. ○ Each group will present their findings, fostering a discussion on the advantages of virtualisation in real-world applications. **Pair activity - Virtualisation and risk reduction** ○ Learners will work in pairs to research different types of virtualisation technologies (e.g., VMware, Hyper-V, Docker) and	Containerisation and Cybersecurity This article discusses how containerisation enhances cybersecurity by isolating applications and their dependencies, reducing the attack surface. https://www.comptia.org/blog/containerization-and-cybersecurity Virtualisation vs. Containerisation in System Design This resource compares virtualisation and containerisation, highlighting their differences and respective security implications. https://www.geeksforgeeks.org/virtualization-vs-containerization/

	examine how these technologies support cybersecurity. Each pair will: ○ Select a virtualisation platform and list its security features. ○ Explore any known vulnerabilities or challenges associated with the platform. ○ Summarise their findings and share strategies that help mitigate these risks.	
B1.4.2 Cloud computing	**Whole class instruction teaching and learning - Introduction** ○ Introduce cloud computing by explaining its fundamental concepts, including data storage, accessibility, and scalability. ○ Focus on security issues in cloud computing, such as default access settings, data leaks, and vulnerabilities in APIs. ○ Use a visual diagram to show how data moves through cloud systems and highlight the importance of security measures. **Individual activity - Infographic creation** ○ Each learner will design an infographic that illustrates best practices for cloud security, including elements such as multi-factor authentication, data encryption, regular audits, and secure API management.	Cloud Computing Security Issues and Challenges This article discusses common security issues in cloud computing, such as default access settings, data leaks, and vulnerabilities in APIs. It provides an overview of the challenges and considerations for securing cloud environments. https://www.crowdstrike.com/en-us/cybersecurity-101/cloud-security/cloud-security-risks/
B1.4.3 BYOD	**Whole class instruction teaching and learning - Case example discussion** ○ Begin with an overview of BYOD policies, focusing on both benefits (e.g., convenience, cost savings) and risks (e.g., data security, privacy). ○ Share a recent real-world example of an organisation that faced challenges with BYOD security, highlighting issues such as data leakage, compatibility, and policy enforcement.	BYOD Policies for Organizations (4 Examples) - Dashlane This resource provides examples of BYOD policies, reflecting various ways organisations can implement policies that best suit their preferences and culture. It discusses full BYOD policies and considerations for acceptable use and off boarding practices.

	○ Encourage a class discussion on why BYOD can be both a convenience and a risk, prompting learners to consider their own experiences with personal device use. **Small group activity - Policy creation workshop** ○ In small groups, learners will create a BYOD policy for a hypothetical company. Each group should: ○ Identify potential risks of BYOD for their company type (e.g., healthcare, finance, education). ○ Draft key elements of a BYOD policy, including acceptable device usage, security requirements (e.g., antivirus software, VPN usage), and protocols for lost or stolen devices. ○ Present their BYOD policy to the class, explaining how it addresses specific risks and balances security with accessibility. **Whole class wrap-up activity - Security do's and don'ts brainstorming session** ○ To conclude the lesson on BYOD, lead the class in a brainstorming session to review best practices and common security mistakes related to BYOD policies. ○ Draw two columns on the board and label them "DO's" and "DON'Ts." ○ Ask learners to contribute examples of secure BYOD practices for the DO's column (e.g., "use a secure password" or "enable device encryption") and common security risks for the DON'Ts column (e.g., "don't use public Wi-Fi without a VPN" or "don't share work devices with others"). ○ Once the list is complete, the class agrees the top three DO's and DON'Ts as main takeaways from the lesson.	https://www.dashlane.com/blog/byod-policies-for-organizations

B2 Network components B2.1.1 End-user devices, with connectivity and processing	**Whole class instruction teaching and learning - Introduction** ○ Introduce end-user devices by explaining their role in a networked environment, including connectivity features (e.g., Wi-Fi, Bluetooth, cellular) and processing capabilities. ○ Highlight various types of devices (e.g., smartphones, laptops, tablets, and IoT devices) and discuss the security implications of each. ○ Use visuals to illustrate how these devices interact with other networked components and outline the importance of securing end-user devices. **Small group activity - Device security evaluation** ○ Divide the class into small groups, assigning each group a specific end-user device (e.g., smartphone, tablet, laptop, or wearable). Each group will: ○ Identify key connectivity features and potential vulnerabilities associated with their device. ○ Discuss how processing power impacts the device's ability to handle security applications (e.g., antivirus software). ○ Outline security measures specific to their device (e.g., biometric authentication, encryption). ○ Each group will share their findings with the class, encouraging discussion on the unique security needs of different devices. **Pair activity - Comparison chart: Connectivity and processing** ○ Each pair will create a chart comparing the connectivity and processing capabilities of two assigned devices (e.g., smartphone vs. laptop, or tablet vs. smartwatch). Their chart should include: ○ Connectivity options (e.g., Wi-Fi, cellular, Bluetooth). ○ Processing power and limitations.	End User Device Strategy: Security Framework & Controls This document outlines security frameworks and controls for end-user devices, discussing connectivity features, processing capabilities, and security measures. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/261980/EUD_Security.pdf Device Security Guidance - NCSC This guidance provides advice on managing deployed devices, including connectivity options, processing capabilities, and security considerations. https://www.ncsc.gov.uk/collection/device-security-guidance/managing-deployed-devices/advising-end-users

	○ Security features suited to each device type. ○ Pairs will briefly present their charts, helping learners see the variety and specialisation in device capabilities.	
B2.1.2 Connectivity devices	**Whole class instruction – Introduction to connectivity devices** ○ Introduce the concept of connectivity devices and their role within a network infrastructure. ○ Cover the purpose and features of each device, including switches, routers, modems, access points, and hubs. ○ Use visual aids or a physical demonstration to show how devices interconnect, transmitting data across networks securely. ○ Encourage learners to think about how different devices impact security, performance, and scalability. **Small group activity – Device identification and functionality** ○ Assign each group a different connectivity device (e.g., router, switch, modem). Instruct groups to research and analyse the specific functions, advantages, and security implications of their device. ○ Each group will prepare a short presentation with key features and possible security risks. ○ Afterward, have each group present their findings, fostering an understanding of how each device contributes to network security. **Pair activity – Assessing security in connectivity devices** ○ In pairs, learners will evaluate the security configurations of connectivity devices such as routers and switches. ○ Ask them to explore and recommend ways to secure these devices against threats (e.g., changing default passwords, enabling firewall options, disabling unused ports). ○ Each pair will document their recommendations and discuss the potential security improvements with the class.	Network Devices: Common Types and Their Functions This resource discusses common network devices, such as routers, switches, and hubs, and their functions in managing traffic flow, providing security, and enabling connectivity between network segments or the Internet. https://www.lepide.com/blog/the-most-common-types-of-network-devices/

	Individual activity – Research on multi-functional connectivity devices ○ Learners will research a multi-functional connectivity device that combines functions like a router and switch or modem and access point. ○ They will create a written summary on the pros and cons of such multi-functional devices from a security perspective, particularly regarding vulnerabilities and how these can be mitigated. ○ Encourage learners to reflect on their findings and propose effective security practices.	
B2.1.3 Connection media	**Whole class instruction teaching and learning - Introduction** ○ Introduce the concept of connection media in networking by discussing the variety of physical and wireless media types, including cable, Ethernet, USB, Wi-Fi, NFC, Bluetooth, cellular (5G), and optical fibre. ○ Use visual aids to represent each type and highlight typical uses, advantages, and potential limitations. ○ Discuss how connection media impact network performance and security. ○ Encourage learners to consider why specific media types are chosen for different purposes (e.g., speed, range, or compatibility). ○ Lead a class discussion on security risks associated with each connection type, such as interception risks for Wi-Fi or vulnerabilities in USB devices. **Small group activity - Media comparison analysis** ○ Assign each group a type of connection media to research in-depth (e.g., Ethernet, Wi-Fi, Bluetooth). Each group will: ○ Analyse the media's key characteristics, such as speed, range, and security features.	Network Connected Security Technologies (NCST) Guidance: Guidance on managing risks associated with deploying network-connected security technologies, including considerations for different media types. https://www.npsa.gov.uk/network-connected-security-technologies-ncst-guidance Types of Transmission Media: An overview of various transmission media, including guided (wired) and unguided (wireless) types, with explanations of their characteristics and applications. https://www.geeksforgeeks.org/types-transmission-media/

	○ Evaluate potential vulnerabilities, like physical tampering with Ethernet or eavesdropping on Wi-Fi. ○ Propose methods to secure each type, considering real-world scenarios. ○ Groups will present their findings to the class, fostering peer learning and critical thinking on best practices for securing connection media. **Individual activity - Connection media evaluation task** ○ For individual practice, learners will select one connection media type and create a brief report that: ○ Describes its common uses and security risks. ○ Explains mitigation strategies for securing the chosen media, using real-world examples where possible. ○ Reflects on the impact of unsecure media on network performance and organisational security.	
B2.2 Application and security issues of external media and storage	**Whole class instruction teaching and learning - Introduction** ○ Introduce the topic by discussing the role and common uses of external media in both personal and professional settings, such as USB drives, external hard drives, and SD cards. ○ Explain the associated security issues, emphasising risks like data interception, loss, and malware transmission. ○ Use visual aids to show how security breaches can occur via external media and encourage learners to think about where and how they encounter these media in daily use. ○ Conclude with a discussion on the importance of encryption, secure disposal, and device management to safeguard sensitive information.	Cyber Security and External Storage Devices Risks: An article that explores the security concerns related to external storage devices, such as USB drives, and provides insights into managing these risks. https://www.beyond20.com/blog/external-storage-device-security/ Security Best Practices for Removable Media and Devices: An article that outlines the security risks associated with removable media and provides best practices for mitigating these risks. https://hackernoon.com/security-best-

	Pair activity - Encryption and secure disposal research ○ In pairs, learners will research best practices in encryption and secure disposal for external media. Each pair will: ○ Summarise an encryption method suitable for securing data on external media. ○ Outline a disposal method for preventing data recovery on retired storage devices. ○ Present their findings to the class, explaining the importance of each method and offering examples of tools or techniques. **Individual activity - Evaluating external media security risks** ○ For individual practice, learners will choose an external media device (e.g., SD card, flash drive) and create a risk assessment covering potential threats like malware infection, data interception, and media failure. ○ They should: ○ Identify the specific security risks for their chosen media. ○ Propose two security measures to mitigate these risks. ○ Reflect on how their findings can inform personal and organisational media use.	practices-for-removable-media-and-devices
B2.3.1 Network and device operating systems	**Whole class instruction teaching and learning - Introduction** ○ Begin by explaining the purpose of network and device operating systems, such as managing hardware, supporting applications, and providing user interfaces (GUI and CLI). ○ Use examples of popular operating systems for network devices (e.g., Windows Server, Linux) and end-user devices (e.g., Windows, macOS, Android). ○ Highlight the differences between these systems and the importance of secure configuration to prevent vulnerabilities.	Network Operating System (NOS) – Network Encyclopaedia: This article provides an overview of network operating systems, detailing their functions, types, and examples, which can help illustrate the role of NOS in managing network resources. https://networkencyclopedia.com/network-operating-system-nos

	○ To engage learners, compare GUI and CLI interfaces and discuss their respective roles in device management and security. **Small group activity - Exploring vulnerabilities in operating systems** ○ Divide learners into small groups and assign each group a case study focused on a specific operating system vulnerability (e.g., unpatched software, default settings in IoT devices). Each group will: ○ Analyse the case study to identify the causes of the vulnerability ○ Discuss potential impacts on network or device security ○ Suggest practical methods for mitigating this vulnerability, such as regular updates, configuration changes, or security patches ○ Groups will present their findings to the class, enhancing their understanding of security best practices. **Individual activity - securing an operating system** ○ Individually, learners will choose an operating system they use regularly (e.g., Windows, Android) and create a personal security checklist. The checklist should include: ○ Essential security practices, such as enabling firewalls, installing updates, and configuring user permissions ○ Specific steps to secure common applications on the operating system ○ A note on the impact of each security measure on data protection and device integrity	
B2.3.2 network monitoring, management and troubleshooting tools	**Whole class instruction teaching and learning - Introduction** ○ Introduce network monitoring, management, and troubleshooting tools by explaining their role in maintaining network security, performance, and reliability.	20 Best Network Monitoring Tools for 2024 (Free & Paid): This article provides an extensive list of network monitoring tools, detailing their features and applications, which can help illustrate

	○ Provide an overview of common tools, such as network analysers (e.g., Wireshark), vulnerability scanners, and performance monitors, and explain their purposes (e.g., detecting intrusions, identifying bottlenecks, and troubleshooting connectivity issues). ○ Use real-world examples to illustrate how these tools prevent and resolve network issues. ○ Conclude by discussing the importance of proactive monitoring to anticipate and mitigate potential security threats. **Individual activity - Creating a network troubleshooting plan** ○ For individual practice, learners will create a basic network troubleshooting plan that outlines steps to identify, diagnose, and resolve a common network issue (e.g., connectivity problems or unusual traffic). ○ Each learner should: ○ Choose an issue and describe symptoms that may indicate its occurrence ○ List monitoring and troubleshooting tools they would use to detect and address the issue ○ Summarise key actions to take during troubleshooting, explaining how each step helps to isolate and fix the problem	their roles in maintaining network security, performance, and reliability. https://www.comparitech.com/net-admin/network-monitoring-tools/ Network Troubleshooting Guide for IT Professionals: A comprehensive guide that discusses common network issues and the tools used to troubleshoot them, providing insights into practical actions to take during troubleshooting. https://www.auvik.com/franklyit/blog/network-troubleshooting/
B2.3.3 network applications	**Whole class instruction teaching and learning - Introduction** ○ Begin by introducing network applications and their role in supporting communication, collaboration, and data management across networks. ○ Explain the functionality of various network applications, such as remote working tools (e.g., VPNs, remote desktops), databases, and document management systems. ○ Highlight security considerations for network applications, including access control, encryption, and data integrity. Use examples like email servers, VoIP, and collaboration tools to	What is Application Security?: This resource provides an overview of application security, discussing its importance and various types, which can help illustrate the role of network applications in supporting communication, collaboration, and data management. https://www.imperva.com/learn/application-security/application-security/

	illustrate how these applications contribute to business operations and data security. **Small group activity - Analysing network application scenarios** ○ Divide learners into small groups, assigning each group a specific network application scenario (e.g., remote work access via VPN, data storage on a networked database). Each group will: ○ Identify potential security risks associated with their assigned network application ○ Discuss measures to mitigate these risks, such as implementing access controls, encryption, or regular audits ○ Outline the benefits of using the application securely within an organisation, focusing on productivity and data protection ○ Lead a class discussion on the findings. Correct any misconceptions. **Pair activity - Comparing communication applications** ○ In pairs, learners will research and compare two communication network applications, such as VoIP and email services, focusing on their security features, accessibility, and functionality. Each pair will: ○ Summarise the main features of each application and its use in organisational communication ○ Compare security aspects, such as data encryption, access control, and vulnerability to phishing or malware ○ Present their analysis to the class, offering insights into how different communication applications can meet various organisational needs	Security in Network Design: Key Considerations from a Network Architect: This blog post discusses key security considerations in network design, including the importance of securing network applications through access control, encryption, and data integrity measures. https://blogs.cisco.com/learning/security-in-network-design-key-considerations-from-a-network-architect

B3 Networking infrastructure services and resources B3.1.1 Transmission Control Protocol/Internet Protocol (TCP/IP)	**Whole class instruction teaching and learning - Introduction** ○ Begin by introducing the basics of the TCP/IP protocol suite, its purpose, and its importance in ensuring data is sent and received accurately over networks. ○ Explain the four-layer model (Application, Transport, Internet, and Network Interface) and the function of each layer, highlighting how TCP/IP enables data communication between devices on different networks. ○ Use diagrams to show packet structure and explain key concepts like IP addresses, packets, and error correction. ○ Conclude by discussing common uses of TCP/IP in real-world applications, such as web browsing and email transmission. **Pair activity - Analysing packet structure and data flow** ○ In pairs, learners will examine the structure of a TCP/IP data packet and discuss how data flows through the four layers of the TCP/IP model. Each pair will: ○ Break down the components of a packet (e.g., header, payload) and the information contained in each part, such as source and destination addresses ○ Map out the journey of a packet from sender to receiver, explaining how each layer processes the data ○ Present their analysis, highlighting how the model ensures data integrity and reliability in communication. **Individual activity - Configuring basic TCP/IP settings** ○ For individual practice, learners will conduct a hands-on activity to configure basic TCP/IP settings on a device (or a simulated network environment if available). Each learner should: ○ Set up an IP address, subnet mask, and gateway	TCP/IP Model: This resource explains the four-layer TCP/IP model, detailing each layer's function and how they work together to facilitate network communication. https://www.geeksforgeeks.org/tcp-ip-model/ TCP/IP Packet Format: This resource provides detailed information on the structure of TCP/IP packets, including headers and payloads, and explains key concepts like IP addresses and error correction. https://www.geeksforgeeks.org/tcp-ip-packet-format/

	○ Test the configuration using commands like ping and ipconfig (or equivalent commands) ○ Document each step and reflect on how configuration impacts connectivity and network access	
B3.1.2 Ports	**Whole class instruction teaching and learning - Introduction** ○ Start with an overview of network ports, explaining that ports serve as endpoints for network communication and allow multiple services to run on a single IP address. ○ Describe the difference between well-known, registered, and dynamic/private ports, providing examples like port 80 for HTTP, port 443 for HTTPS, and port 25 for SMTP email services. ○ Use a visual diagram to show how data packets use IP addresses and ports to reach specific applications on a device. ○ Conclude by discussing the importance of secure port management to prevent unauthorised access. **Small group activity - Identifying common ports and their uses** ○ Divide learners into small groups and assign each group a few commonly used ports (e.g., 21 for FTP, 22 for SSH, 53 for DNS, 80 for HTTP). Each group will: ○ Research the function and typical application of each assigned port ○ Identify potential security risks associated with each port (e.g., unauthorised access through open ports) ○ Present their findings to the class, discussing why it's important to secure or monitor these ports in a network environment	What is a Computer Port? | Ports in Networking: This article provides an overview of computer ports, explaining their function as virtual points where network connections start and end, and how they help computers sort network traffic. https://www.cloudflare.com/en-gb/learning/network-layer/what-is-a-computer-port/
B3.1.3 Packet	**Whole class instruction teaching and learning - Introduction** ○ Introduce the concept of data packets, explaining their purpose in network communication.	Exploring the Anatomy of a Data Packet: This article provides an in-depth look at the structure of data packets, including headers, payloads, and

	○ Discuss the basic structure of a packet, including its header (with addressing and control information), payload (the actual data), and trailer (for error checking). ○ Highlight the differences between TCP, IP, and UDP protocols and their specific uses in reliable and non-reliable data transmission. ○ Use diagrams or animations to visually represent packet flow through networks, showing how packets are broken down and reassembled to facilitate communication. **Small group activity - Packet dissection exercise** ○ Divide the class into small groups and assign each group a different packet protocol (TCP, IP, or UDP). ○ Provide sample packet data for each protocol and guide learners to analyse the packet structure, identifying each section (header, payload, trailer) and its purpose. ○ After analysing, each group will present the protocol's structure and discuss why each section is crucial for that protocol's functionality.	trailers, and explains their roles in network communication. https://www.techrepublic.com/article/exploring-the-anatomy-of-a-data-packet/ TCP vs. UDP — What's the Difference and Which Protocol is Faster?: An analysis of TCP and UDP protocols, discussing their functionalities, performance, and suitable applications. https://www.freecodecamp.org/news/tcp-vs-udp/
B3.1.4 Network address translation (NAT)	**Whole class instruction teaching and learning - Introduction** ○ Introduce network address translation (NAT) and discuss its role in network security and IP address management. ○ Explain the different types of NAT: static, dynamic, and Port Address Translation (PAT). ○ Use a diagram to illustrate how NAT hides internal IP addresses when devices communicate over the internet. ○ Encourage learners to reflect on how NAT helps organisations maintain network privacy and security by reducing direct exposure of devices to external networks.	What Is Network Address Translation (NAT)?: This article provides an overview of NAT, explaining its purpose in network security and IP address management. https://www.fortinet.com/resources/cyberglossary/network-address-translation Types of Network Address Translation (NAT): This resource explains the different types of NAT—static, dynamic,

	Small group activity - NAT types Comparison ○ In small groups, learners will analyse and compare static, dynamic, and PAT NAT types by researching each type's specific use cases, benefits, and limitations. ○ Each group will evaluate the scenarios where one NAT type may be more suitable than others, considering factors such as network size, security requirements, and user connectivity. ○ Groups will present their comparisons and explanations to the class, encouraging a discussion on the practical implications of each NAT type in real-world network configurations. **Pair activity - IPv4 vs. IPv6 Addressing formats** ○ In pairs, learners will investigate the structure and format of IPv4 and IPv6 addresses, including an exploration of private IP address ranges (RFC 1918) for IPv4 and the common features of IPv6. ○ Each pair will focus on understanding the characteristics and addressing methods in each protocol, noting differences in notation and address allocation. ○ Afterward, learners will apply their knowledge by converting a set of IP addresses to demonstrate their understanding of IPv4 sub netting and IPv6 prefixing. ○ Pairs will discuss with the class how the transition from IPv4 to IPv6 impacts NAT usage. **Individual activity - RFC 1918 and special IP addresses** ○ For individual practice, learners will identify and list the private IP address ranges for Class A, B, and C (RFC 1918) and the Automatic Private IP Addressing (APIPA) range used during DHCP failures. ○ They will also research the role of reserved IP addresses, such as the 127.0.0.1 loopback address, and create a short summary explaining each category's purpose.	and Port Address Translation (PAT)—including their specific use cases, benefits, and limitations. https://www.geeksforgeeks.org/types-of-network-address-translation-nat What are Special IP Addresses in IPv4?: An informative piece that explains the different types of special IP addresses in IPv4, including their ranges and purposes. https://binaryterms.com/special-ip-addresses-in-ipv4.html

B3.2 Application of domains, sub-domains and segmentation	**Whole class instruction teaching and learning - Introduction** ○ Introduce the concept of domains and sub-domains within network architecture. ○ Discuss the importance of hierarchical organization in networks and how domains and sub-domains are structured to create trust relationships and enhance security. Use diagrams to illustrate a domain hierarchy and show examples of how network segmentation limits unauthorised access and reduces attack surfaces. ○ Encourage learners to reflect on how segmentation benefits organisations by containing security threats and improving control over access to sensitive data and applications. **Small group activity - Exploring trust relationships and access control** ○ In small groups, learners will analyse various trust relationships within a domain hierarchy, including how access control policies are applied across domains and sub-domains. ○ Each group will evaluate how different levels of access within a hierarchy can help manage trust and restrict unauthorised movement within a network. ○ Afterward, groups will discuss scenarios where trust relationships could either support or undermine security if not configured correctly. ○ They will present their insights, focusing on how segmentation affects overall network security. **Pair activity - Segmentation benefits analysis** ○ In pairs, learners will explore the security benefits of network segmentation by studying its impact on limiting lateral movement of malware, reducing attack surfaces, and simplifying damage control.	Network Segmentation: Definition, Benefits, Best Practices: An article that explains network segmentation, its importance in hierarchical organisation, and how it enhances security by creating manageable segments. https://phoenixnap.com/blog/network-segmentation Network Segmentation Cheat Sheet: This cheat sheet from OWASP provides insights into building a secure and maximally isolated service network architecture, focusing on trust relationships and access control. https://cheatsheetseries.owasp.org/cheatsheets/Network_Segmentation_Cheat_Sheet.html 7 Network Segmentation Best Practices to Level-up: This resource offers best practices for implementing network segmentation, focusing on creating a hierarchy that restricts access and minimizes attack surfaces. https://www.strongdm.com/blog/network-segmentation

	○ Each pair will evaluate a case study or scenario where segmentation was used to contain a security breach or to isolate critical assets from the rest of the network. ○ Pairs will present their findings to the class, sharing insights on the advantages and challenges of implementing network segmentation in organisational networks. **Individual activity - Creating a segmented network model** ○ For individual practice, learners will design a simple network model that incorporates domains, sub-domains, and segmented zones. ○ They will identify key access points, apply access control measures, and create a hierarchy showing how devices and data are segmented for security. ○ Learners will submit a short write-up summarising how their model restricts access, minimises attack surfaces, and offers protection against intruders or malware.	
B3.3 Application of network devices to configure networks	**Whole class instruction teaching and learning - Introduction** ○ Introduce network configuration by discussing the essential roles and applications of network devices. ○ Explain how each device (e.g., server, router, switch, WAP, firewall, bridge, and gateway) contributes to network security and connectivity. ○ Use visual diagrams to illustrate basic network setups, showing where each device fits within a network and discussing their configurations. **Individual activity - Network security checklist creation** ○ Each learner will create a security checklist focused on securing network devices, covering routers, switches, firewalls, and other key devices. ○ The checklist should include essential configurations (e.g., password protection, firmware updates, disabling unused ports)	Network Devices (Hub, Repeater, Bridge, Switch, Router, Gateways): This article provides detailed explanations of various network devices, their functions, and how they contribute to network security and connectivity. https://www.geeksforgeeks.org/network-devices-hub-repeater-bridge-switch-router-gateways/

	and a brief explanation of how each step enhances network security. ○ Learners can refer back to this checklist for future activities involving device configuration.	
B3.4.1 Domain Name System (DNS)	**Whole class instruction teaching and learning - Introduction** ○ Introduce the Domain Name System (DNS) by explaining its essential role in translating domain names into IP addresses. ○ Use a simple analogy, like a "phonebook for the internet," to help learners understand the importance of DNS. Cover the basic DNS resolution process, reverse DNS resolution, and the function of DNS caching in speeding up network access. ○ Highlight IPv6 DNS and how it addresses limitations in IPv4. ○ Use a flowchart to illustrate each step in the DNS resolution process. **Pair activity - Investigating DNS and reverse DNS lookup** ○ In pairs, learners will use command-line tools (such as nslookup or dig) or online tools to perform DNS and reverse DNS lookups on various websites. ○ Each pair will record and analyse the results, noting how a domain name resolves to an IP address and how reverse DNS retrieves the domain from an IP address. ○ Pairs will also investigate the effects of DNS caching by performing repeated lookups and noting any differences.	What is DNS? https://www.cloudflare.com/en-gb/learning/dns/what-is-dns/ DNS Lookup https://mxtoolbox.com/DNSLookup.aspx DNS Propagation checker https://www.whatsmydns.net/ Reverse IP lookup https://mxtoolbox.com/ReverseLookup.aspx
B3.4.2 Directory services (DS), identity and access management	**Whole class instruction teaching and learning - Introduction** ○ Begin by introducing directory services and their importance in managing user identities, permissions, and access across networks. ○ Explain the role of directory services in centralising user data and enhancing security through controlled access.	IAM https://www.microsoft.com/en-gb/security/business/security-101/what-is-identity-access-management-iam

	○ Provide an overview of the key directory services: Active Directory (primarily used in Windows environments), Open Directory (for Apple devices), and OpenLDAP (an open-source directory protocol for various systems). ○ Use a visual comparison chart to highlight their distinct features and common uses. **Individual activity - Directory services security best practices guide** ○ Each learner will create a one-page guide on best practices for securing directory services, covering user authentication (e.g., multi-factor authentication), access control (e.g., least privilege principle), and regular auditing. ○ They should include specific practices for securing Active Directory, Open Directory, and OpenLDAP, if applicable, and briefly explain why each practice is crucial to maintaining a secure identity and access management system.	https://learn.microsoft.com/en-us/entra/fundamentals/introduction-identity-access-management
B3.4.3 Authentication services	**Whole class instruction teaching and learning - Introduction** ○ Introduce the concept of authentication services by explaining why different types of authentication (single-factor, two-factor, multi-factor) are used and their roles in protecting systems. Use visuals to illustrate each type and discuss the purpose of single sign-on (SSO) and its advantages for user convenience. ○ Describe common authentication protocols (PAP, CHAP, and EAP) and the relevance of each in network security. **Small group activity - Comparing authentication methods** ○ Each group is assigned a type of authentication (e.g., single-factor, TFA, MFA, SSO) to research. Groups will: ○ Analyse how their assigned authentication method enhances security. ○ Evaluate the pros and cons of their method in terms of user experience and security. Groups will present their findings,	NCSC Authentication methods https://www.ncsc.gov.uk/guidance/authentication-methods-choosing-the-right-type User authentication methods https://www.idrnd.ai/5-authentication-methods-that-can-prevent-the-next-breach/

	discussing the most secure methods and suggesting improvements for specific scenarios. **Pair activity - Protocol investigation** ○ Each pair will explore one authentication protocol (PAP, CHAP, or EAP) in depth. They will: ○ Describe how the protocol operates within network security. ○ Compare it with another protocol, noting how it strengthens (or weakens) security. Pairs will then summarise and share insights with the class, focusing on real-world applications of each protocol. **Individual activity - Reflective report on authentication practices** ○ Learners will write a short report on how they might apply authentication protocols and multi-factor authentication in a business environment. They will include: ○ A summary of one protocol and its application. ○ Suggested improvements to existing authentication processes in their hypothetical organisation.	
B3.4.4 Dynamic Host Configuration Protocol (DHCP)	**Whole class instruction teaching and learning - Introduction** ○ Begin with an introduction to DHCP, explaining the roles of DHCP servers and clients in assigning IP addresses automatically within a network. ○ Use diagrams to illustrate the IP allocation process, emphasising how DHCP simplifies IP management. Cover the importance of DHCP in network efficiency and discuss basic configuration settings, such as address ranges, lease duration, and types of IP allocation (dynamic, static, and automatic).	What is DHCP and how does it work https://www.youtube.com/watch?v=ldtUSSZJCGg https://www.cloudns.net/blog/dhcp-server/ https://learn.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-top

	Small group activity - DHCP configuration simulation ○ Assign each group a scenario where they will configure a DHCP setup with specific requirements, such as setting address ranges and configuring static and dynamic addresses. Each group will: ○ Design a basic DHCP setup based on their scenario requirements. ○ Explain how the chosen settings (e.g., lease time, reservation of specific addresses) meet network needs.	
B3.4.5 Routing	**Whole class instruction teaching and learning - Introduction** ○ Introduce the concept of routing in network communication, explaining the purpose and function of static and dynamic/adaptive routing. ○ Use a network diagram to demonstrate how routers use routing tables to direct traffic. ○ Briefly introduce key routing protocols, distinguishing between Interior Gateway Protocols (IGPs) used within an organisation and Exterior Gateway Protocols (EGPs) for external networks. ○ Emphasise the significance of the Border Gateway Protocol (BGP) in internet routing and how it helps manage data across large networks. **Small group activity - Routing table analysis** ○ Assign each group a simplified routing table for analysis. Groups will: ○ Interpret the routing table to understand which routes are static and which are dynamic. ○ Analyse the impact of each route on network efficiency, discussing factors like shortest paths, speed, and reliability.	What is routing https://aws.amazon.com/what-is/routing/

	○ Each group will then present their analysis, focusing on how routing tables contribute to data flow and network optimisation. **Pair activity - Protocol comparison** ○ In pairs, learners will explore and compare one Interior Gateway Protocol (e.g., RIP or OSPF) and one Exterior Gateway Protocol (e.g., BGP). They will: ○ Explain the purpose and applications of each protocol within and between networks. ○ Evaluate the strengths and limitations of each protocol, especially in large-scale networks. ○ Pairs will share their comparisons, discussing how each protocol contributes to efficient routing.	
B3.4.6 Remote access services	**Whole class instruction teaching and learning - Introduction** ○ Begin by introducing remote access services, discussing why organisations use them to enable secure, remote connections to internal networks and resources. ○ Explain dial-up access through telecommunications services as a legacy method, contrasting it with VPN (Virtual Private Network) connections, which provide more secure access over the internet. ○ Describe the handshake process in establishing remote connections, focusing on the client-host/server interaction that authenticates users and secures data transmission. **Pair activity - Remote access method comparison** ○ In pairs, learners will compare dial-up and VPN remote access methods. They will: ○ Identify the main differences in connection speed, security, and usability.	What is remote access https://www.hpe.com/uk/en/what-is/remote-access.html

	○ Evaluate the suitability of each method for modern organisational needs, particularly focusing on security implications. ○ Pairs will share their findings with the class, emphasising the relevance of VPNs over dial-up in current remote access requirements.	
B3.5.1 File and print services	**Whole class instruction teaching and learning – Introduction** ○ Begin by discussing the core functions of file and print services in a network. ○ Explain concepts such as file servers for centralised storage, print servers for managing printer access, and why effective management of these resources is critical for security, productivity, and efficiency. ○ Highlight file sharing, access control, print queue prioritisation, and printer driver management. ○ Show a flow diagram of how these services work in a typical office setup. **Individual activity - File access policy design** ○ Learners design an access control policy for a fictional company. The activity includes: ○ Choosing access levels for different types of employees (e.g., admins, managers, team members) for various file types (e.g., confidential HR files, shared project files, public documents). ○ Creating a visual access hierarchy (e.g., flowchart or access matrix) to show who can access which files and why. ○ Writing a short policy summary explaining how their design protects data and supports the organisation's workflow.	How does a print server work https://www.papercut.com/blog/print_basics/how-does-a-print-server-work/ Flash cards https://www.brainscape.com/flashcards/lesson-6-file-and-print-services-7687698/packs/12688261

B3.5.2 Web, mail and communications services	**Whole class instruction teaching and learning - Introduction** ○ Introduce learners to web, mail, and communication services, explaining how each service type supports networking infrastructure and business operations. ○ Discuss the protocols involved, such as HTTP, HTTPS, SMTP, and POP, emphasising their roles and limitations, particularly around security and encryption. ○ Use visual aids to illustrate how these services interconnect and facilitate data sharing, application communication, and user collaboration across platforms. **Individual activity - Data sharing and security report** ○ Learners write a summary report on how data sharing and communication services can enhance business operations but also increase exposure to security risks. ○ They should consider concepts like: ○ encryption ○ protocol vulnerabilities ○ the balance between accessibility and security.	https://whatismyipaddress.com/types-internet-protocols
C1 Internal policies C1.1.1 A cyber security policy that uses the Plan-Do-Check-Act loop derived from part of the International Organisation for Standardisation (ISO) 27001:2013	**Whole class instruction teaching and learning - Introduction** ○ Introduce ISO 27001 standards, emphasising its importance in creating and maintaining robust cyber security policies. ○ Use a short video overview of ISO 27001 to introduce key concepts and the PDCA (Plan-Do-Check-Act) cycle. ○ Explain each component of PDCA in relation to cyber security policy implementation, focusing on continual improvement. ○ Discuss how policies on internet and email use, security procedures, and staff responsibilities can be structured within PDCA.	ISO 27001 https://www.youtube.com/watch?v=x792wXSeAhA Case studies https://www.itgovernance.co.uk/resources/iso-27001 Plan Do Check Act https://www.youtube.com/watch?v=n6BW3Tv1vAw

	Small group activity - Designing a PDCA-based policy ○ Assign each group a specific aspect of internet/email security (e.g., handling confidential information, monitoring policies, or password enforcement). ○ Groups will use PDCA to design a security policy for their assigned topic, identifying actions for each cycle stage. ○ Each group presents its policy, explaining how the PDCA cycle promotes compliance and improvement. **Pair activity - Exploring password and security procedures** ○ Each pair will research examples of password policies in real organisations, focusing on aspects like strength requirements, monitoring, and enforcement tools. ○ They will analyse the policies, identifying any strengths and weaknesses and considering how PDCA can improve these areas. ○ Each pair shares insights, discussing potential improvements and challenges in enforcing robust password practices.	https://www.youtube.com/watch?v=bO3GpAjVvD8 https://www.qmii.com/understanding-the-pdca-cycle-in-iso-27001-auditing/ Toolkit https://www.iso27001security.com/html/toolkit.html
C1.1.2 Security audits and their application to check compliance against policies	**Whole class instruction teaching and learning - Introduction** ○ Introduce security audits by explaining their purpose in maintaining compliance with both internal and external requirements. ○ Discuss the main goals of audits, such as identifying weaknesses, verifying adherence to internal policies and external laws, and guiding necessary improvements. ○ Use a visual outline of the auditing process from goal setting to reporting results to help learners conceptualise the steps involved. ○ Encourage a class discussion on why compliance with security policies and regulations is critical to an organisation's success and security.	IT Security Audit - Step-by-Step Guide & Tools: This article provides an overview of IT security audits, discussing their purpose in maintaining compliance with internal and external requirements, and outlining the auditing process from goal setting to reporting results. https://www.comparitech.com/net-admin/it-security-audit/ Free Security Audit Checklist: This resource offers a comprehensive tool used to assess the security measures

	Small group activity: Audit goals brainstorming ○ In small groups, learners brainstorm potential goals for a security audit in different scenarios (e.g., a healthcare organisation, a financial institution, a small business). ○ Each group should focus on setting realistic goals based on their assigned scenario's needs (such as ensuring data privacy or protecting against data breaches). ○ Groups will then share their goals with the class. **Small group activity: Compliance checklist creation** ○ Each group will be assigned a set of basic security policies (e.g., password policies, data access restrictions, physical security). ○ Their task is to create a simple compliance checklist based on these policies that an auditor could use to assess compliance. ○ Groups will then swap checklists and use them to "audit" a fictional organisation with provided scenarios, noting any gaps or issues. **Individual activity: Audit process flowchart** ○ Ask each learner to design a flowchart showing the main steps in a security audit process. The flowchart should cover key stages like defining the audit scope, identifying gaps, comparing with policies, and reporting results. ○ This activity helps learners visualise the audit process and organise their understanding of each stage.	and controls in an organisation's systems, processes, and infrastructure, which can aid in creating compliance checklists. https://safetyculture.com/checklists/security-audit
C1.1.3 Backup policy	**Whole class instruction teaching and learning - Introduction** ○ Introduce the concept of a backup policy by explaining its importance in maintaining data integrity and recovery in case of incidents.	Backup Policy Best Practices: Approaches and Frameworks: This guide discusses best practices for designing backup schedules, considering factors such as data volume, recovery needs, and

	○ Discuss the elements of a robust backup policy, including selecting data for backup, types of backups, scheduling, and storage strategies. ○ Use examples to show different backup types (e.g., full, incremental, differential) and how each fits into different organisational needs. ○ Conclude with a discussion on compliance requirements and the critical role of testing and accountability. **Small group activity - Comparing backup methods** ○ In small groups, learners are assigned different backup methods (e.g., full, differential, incremental, continuous). Each group researches and analyses the pros, cons, and ideal use cases for their assigned method. ○ Groups will present their findings to the class, demonstrating how each method fits within an organisational backup strategy. **Pair activity - Designing a backup schedule** ○ In pairs, learners will create a backup schedule for a hypothetical company, choosing from daily, weekly, and monthly options. ○ They must consider the company's data volume, recovery needs, and scheduling requirements, and justify their chosen frequency. ○ Pairs will then share their schedules and rationale with the class, helping them apply knowledge of backup frequency and evaluate recovery needs. **Individual activity: Creating a backup process flowchart** ○ Each learner will design a flowchart of the backup process, from data selection through to testing and compliance checks. ○ They should include decision points, such as selecting data types and testing intervals, to demonstrate their understanding of the full backup process.	scheduling requirements, and provides guidance on choosing appropriate backup frequencies. https://www.msp360.com/resources/blog/backup-policy-best-practices/ How do I create a backup policy?: An article that discusses the steps involved in creating a backup policy, including defining roles and responsibilities, which can aid in creating infographics highlighting accountability in the backup process. https://darwinsdata.com/how-do-i-create-a-backup-policy/

	Individual activity: Backup responsibility infographic ○ Learners create an infographic highlighting roles and responsibilities in the backup policy, including who oversees backups, who ensures testing, and who is accountable for compliance.	
C1.1.4 Data protection policy to ensure organisational compliance	**Whole class instruction teaching and learning - Introduction** ○ Introduce data protection policies by explaining their purpose in safeguarding organisational and personal data, with emphasis on compliance with laws such as GDPR. ○ Discuss the role of the Data Protection Officer (DPO), the core data protection principles, and the importance of protecting privacy rights. ○ Provide examples of how data protection applies to staff training, system security, and external parties (e.g., contractors and vendors). ○ Conclude with an overview of the responsibilities and accountability for data protection across the organisation. **Individual activity: Staff training module outline** ○ Each learner will create a brief outline for a staff training module on data protection, covering essential concepts like privacy rights, data handling procedures, and compliance. ○ They should also identify topics relevant for different roles (e.g., general employees vs. data handlers).	Who is a Data Protection Officer [Role and responsibilities]: An article that delves into the roles and responsibilities of a DPO, highlighting their importance in facilitating compliance and competitive advantage for businesses. https://dataprivacymanager.net/who-is-a-data-protection-officer-roles-and-responsibilites/
C1.1.5 Cyber security incident response policy	**Whole class teaching and learning – Introduction to incident response policy** ○ Introduce the concept of a cyber security incident response policy, including the roles and responsibilities of team members and essential communication protocols.	Incident Response Plan: Frameworks and Steps: This article provides an overview of incident response plans, discussing the roles and responsibilities of team members and essential communication protocols.

	○ Explain the importance of each contact (e.g., legal, public relations, IT, insurance) in effective incident response. ○ Use real-world examples where incident response teams were critical in managing a breach. **Small group activity – Response team roles and responsibilities** ○ Each group will be assigned specific roles within an incident response team, such as incident response lead, IT specialist, or legal counsel. Groups will: ○ Discuss the responsibilities of each role during an incident. ○ Develop a table outlining their assigned roles, tasks, and key contacts for escalation. ○ Present how each role contributes to an effective response and how the team coordinates internally and with external entities. **Individual activity – Checklist for incident closure and reporting** ○ Each learner will create a checklist for reviewing, reporting, and closing a cyber security incident. The checklist should include: ○ Required post-incident documentation. ○ Key items for the review process, such as lessons learned and recommendations. ○ Details for final reporting to ensure compliance and thorough documentation.	https://www.crowdstrike.com/en-us/cybersecurity-101/incident-response/incident-response-steps Incident Response (IR) Flowchart - tw-Security: This resource provides a sample flowchart representing the stages of incident response, including decision points such as when to escalate an incident to senior management or engage with public relations. https://www.tw-security.com/PDF_UPLOAD/Incident%20Response%20%28IR%29%20Flowchart%20-%20Sample.pdf
C1.1.6 Disaster recovery policy	**Whole class instruction teaching and learning – Introduction** ○ Introduce the concept of disaster recovery in cyber security, explaining its critical role in maintaining business operations during or after a crisis. ○ Define the purpose and scope of a disaster recovery policy, covering key elements such as triage procedures and categorisation of events by severity.	Disaster Recovery Policy: Essential Elements and Best Practices: This article provides an overview of disaster recovery policies, discussing their critical role in maintaining business operations during or after a crisis, and defining their purpose and scope.

	○ Emphasise how effective disaster recovery policies activate protocols like the cyber security incident response, business continuity plan, and disaster recovery plan. ○ Display a process infographic showing the response flow from incident detection to recovery, highlighting roles and responsibilities involved in each stage. ○ Facilitate a class discussion on real-world events, such as data breaches or natural disasters, to help learners visualise the types of incidents covered in a disaster recovery policy. **Small group activity – Event severity and response planning** ○ Provide each group with a different hypothetical disaster scenario (e.g., cyber-attack, fire, system outage). Their task is to: ○ Analyse the severity of the incident. ○ Identify the appropriate response and activate the necessary protocol. ○ Assign roles and responsibilities for key team members in the scenario. ○ Each group will present a flow diagram of their response plan, showing the steps taken from initial detection through recovery. ○ This activity helps learners understand the policy's operational side and encourages teamwork in designing incident responses. **Pair activity – Contact list creation and role allocation** ○ In pairs, learners will develop a contact list for a simulated organisation, identifying key contacts such as IT security team leaders, legal advisors, and public relations representatives. ○ They will then assign responsibilities to each role based on a specific disaster scenario provided by the teacher (e.g., data breach or equipment theft).	https://cloudian.com/guides/disaster-recovery/disaster-recovery-policy-essential-elements-and-best-practices/ What is business continuity and disaster recovery planning? https://www.youtube.com/watch?v=o0xj1JKjjOE

	○ Each pair will use a checklist format to detail contact information, roles, and response duties. **Individual activity – Monitoring and reporting guidelines** ○ Learners will create a template for a log outlining monitoring and reporting requirements for disaster recovery. ○ They should include specific examples of what to monitor (e.g., incident progress, recovery success) and reporting methods for ongoing tracking. ○ This task aims to develop learners' ability to think critically about the importance of maintaining communication during disaster recovery and to self-assess their understanding of monitoring procedures.	
C1.1.7 External services policy	**Whole class instruction teaching and learning – Introduction** ○ Introduce the concept of an external services policy, outlining its role in managing authorisation and access control, regulatory compliance, and incident response procedures for third-party services. ○ Emphasise the importance of accountability in managing external service providers across cloud, hardware, and software solutions. ○ Use examples to discuss real-world situations where weak external service policies led to security vulnerabilities. ○ Present a mind map highlighting each key area of an external services policy, from cloud data protection to vendor support expectations. ○ Guide a discussion on how external services might introduce unique risks and ask learners to brainstorm ways organisations can ensure regulatory compliance when relying on external services.	Engaging Cloud Service Providers: This resource delves into the management of external service providers, discussing authorisation, access control, and compliance, and providing guidance on developing policy statements and incident response steps. https://www.dataprotection.ie/sites/default/files/uploads/2019-10/Guidance%20for%20Engaging%20Cloud%20Service%20Providers_Oct19.pdf Service Level Agreement for Managed IT Service Providers (MSP SLA): This resource discusses the critical elements of an SLA, such as service definitions, performance standards, and remedies for non-compliance, tailored for managed IT services.

	Small group activity – External services policy role-play ○ Assign each group a specific type of external service (e.g., cloud storage, hardware vendors, software providers). Their task is to: ○ Develop a short policy statement covering authorisation, access, and compliance. ○ Outline incident response steps for potential issues with their assigned service. ○ Identify key contact roles and accountability, detailing which personnel or teams should handle particular responsibilities. ○ Each group will create a process map showing the steps they would take to address a service-related incident, including escalation points and timelines. ○ Afterward, groups will share their process maps to compare how policies might vary across different types of external services. **Pair activity – Cloud and data protection standards** ○ Each pair will research specific data protection requirements for a cloud service provider, including acceptable use and the types of resources that require added security measures. ○ They will prepare a comparison table outlining data protection expectations and list potential compliance requirements for organisations relying on cloud services. **Individual activity – Service support plan checklist** ○ Ask learners to create an action plan checklist detailing response times, escalation procedures, and troubleshooting protocols for an external support incident.	https://www.msp360.com/resources/blog/msp-agreement-guide/

	○ Each learner will focus on a particular type of support (e.g., hardware, software) and document steps for contacting support, escalating issues, and tracking completion timelines.	
D1 Forensic collection of evidence D1.1.1 Meeting requirements for forensics	**Whole class instruction teaching and learning – Introduction** ○ Introduce forensic procedures in cyber security by discussing the importance of digital evidence handling and device confiscation. ○ Use visual aids to illustrate protocols, such as isolating devices from networks, retaining device power states, and documenting the chain of custody. ○ Encourage learners to consider the challenges of preserving digital evidence, particularly in mobile devices, and the role of forensic tools in ensuring accuracy. **Small group activity – Device confiscation role-play** ○ Assign groups a scenario where they must act as a forensic team tasked with confiscating and securing devices. Each group will: ○ Plan steps for device isolation, disconnection, and secure packaging. ○ Document their chain of custody and establish legal permissions. ○ Discuss as a team how they would maintain the device's power state and prevent evidence contamination. ○ Groups will present their protocols to the class, showcasing their preparedness for a forensic incident. **Paired activity – Exploring forensic analysis tools** ○ Pairs will research a forensic tool (e.g., disk imaging, malware analysis software) and investigate its features, effectiveness, and use cases in incident investigations. ○ Each pair will create a process infographic outlining how the tool supports forensic analysis steps such as system imaging, log review, and malware detection.	ACPO Good Practice Guide for Digital Evidence: This guide provides comprehensive protocols for handling digital evidence, including device isolation, power state retention, and chain of custody documentation. https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf Best Practices In Digital Evidence Collection: This article discusses evolving evidence handling procedures, highlighting the importance of proper device isolation, disconnection, and secure packaging to prevent evidence contamination. https://www.sans.org/blog/best-practices-in-digital-evidence-collection/

	○ Pairs will present their infographics and discuss any limitations or special considerations of each tool. **Individual activity – Log review analysis** ○ Each learner will review a sample set of system logs (provided or simulated) to identify unusual patterns that could indicate unauthorised access or malware. ○ Learners will document their findings in a data table, noting entries that suggest irregular activity, the type of evidence collected, and its relevance to potential security incidents. ○ This exercise encourages attention to detail and familiarity with reviewing system activity.	
D1.1.2 The challenges of live forensics	**Whole class instruction teaching and learning – Introduction** ○ Introduce the concept of live forensics and its unique challenges. Discuss issues such as in situ data changes, recovering corrupted data, and capturing volatile data in active memory. ○ Use examples to illustrate why handling live systems differs from typical forensic methods and the risks of altering or losing data. ○ Encourage learners to reflect on why live forensics might be essential in ongoing security incidents. **Small group activity – Challenges of data preservation exercise** ○ Groups will receive a simulated case where they must analyse the steps needed to preserve live data on an active system. Each group will: ○ Identify potential risks to data integrity (e.g., data alteration, memory loss). ○ Develop a strategy to minimise these risks while collecting live data. ○ Outline procedures for recovering corrupted or temporary files during a live investigation.	Data Integrity Risks: Interacting with a live system can inadvertently alter or overwrite data, potentially compromising evidence integrity. Careful planning and controlled procedures are essential to minimize this risk. https://www.vaia.com/en-us/explanations/law/forensic-science/live-forensics/

	○ Afterward, groups will present their strategies, explaining how each step helps prevent data loss or corruption.	
D1.1.3 Network forensics	**Whole class instruction teaching and learning – Interactive scenario demonstration** ○ Start with an interactive demonstration where learners observe a simulated network forensics investigation. ○ Use a video to show a step-by-step approach to scanning infrastructure, gaining necessary permissions, and using passive vs. active analysis methods. ○ Highlight how to review logs from different devices and investigate alerts. ○ Pause at key points to quiz learners on next steps or on-the-spot decisions to reinforce learning. **Small group activity – Authority briefing exercise** ○ Divide the class into small groups, assigning each group the role of a network forensic team preparing for a briefing with supervisory authorities. Each group will: ○ Draft a presentation outlining their proposed network-testing methodology, emphasising permissions, risk management, and the distinction between passive and active scanning. ○ Create a checklist of requirements and contingencies they need to address before conducting the tests (e.g., obtaining permissions, testing protocols for live systems). ○ After the activity, groups will deliver their briefings, and the class will give feedback as if they were the supervisory authorities, focusing on gaps or potential risks.	How to use Wireshark https://www.youtube.com/watch?v=zWoHJ3oGRGY How to review network logs with event viewer https://www.youtube.com/watch?v=PO2g5oYDpJQ

	Individual activity – Malware response plan ○ Each learner will develop a quick-response plan for a hypothetical malware alert. Using a given malware scenario, they will: ○ Describe the immediate steps to isolate the malware (e.g., firewall adjustments, monitoring traffic). ○ Propose follow-up analysis steps, like examining logs or using specific forensic tools. ○ Submit their plans in the form of an action plan document.	
D1.1.4 Documenting the scene	**Whole class instruction teaching and learning – Introduction with case study** ○ Introduce the importance of documenting a digital incident scene by walking through a case study of a cyber incident. ○ Explain steps such as securing the scene, taking photographs, and collecting witness statements. ○ Show examples of scene plans, photos, and contemporaneous notes, discussing their value in reconstructing events. ○ Emphasise the role of prior planning for different scenarios, such as physical breaches vs. digital-only incidents. **Small group activity – Scene documentation simulation** ○ Divide the class into small groups and assign each group a simulated incident scene to document (e.g., a breached server room or workstation left unsecured). Each group will: ○ Develop a scene plan, identifying critical areas for documentation and mapping evidence points. ○ Take mock "photos" and create quick sketches/diagrams (they can sketch these or use basic digital tools).	Securing the Scene: Ensure the area is isolated to prevent unauthorized access or tampering. This may involve restricting physical access and disconnecting affected systems from networks. https://www.college.police.uk/app/investigation/forensics Photographing and Sketching: Capture detailed photographs of the scene, including device configurations, cable connections, and any visible anomalies. Create sketches to provide spatial context and highlight the location of key components. https://www.ojp.gov/pdffiles1/nij/219941.pdf Collecting Witness Statements: Interview individuals present during the incident to gather firsthand accounts.

	○ Write a set of contemporaneous notes detailing observations as they document the scene. ○ Each group will share their documentation with the class, explaining their decisions and how they ensured thorough coverage. **Individual activity – Incident documentation checklist** ○ Each learner will create an incident documentation checklist to use when responding to a cyber incident. The checklist should include: ○ Steps for securing the scene. ○ Items to document (photos, plans, notes). ○ Guidelines for taking contemporaneous notes and statements. ○ Learners submit their checklists and receive feedback on completeness and practicality.	Ensure statements are clear, unbiased, and accurately recorded. https://www.cps.gov.uk/legal-guidance/witnesses
D2 Systematic forensic analysis of a suspect system D2.1.1 Retaining snapshots of the system	**Whole class instruction teaching and learning - Introduction** ○ Explain the importance of maintaining accurate records during a forensic investigation. Introduce key requirements for effective documentation, including timely recording and comprehensive details. ○ Use real-world examples to illustrate why these records are crucial for legal validity and internal investigations. **Small group activity - Exploring data preservation methods** ○ Each group will examine different types of system data to preserve during forensic analysis, such as RAM, virtual machines, and deleted files. Tasks include: ○ Identifying potential uses for each data type in an investigation	System Imaging: Creating a bit-by-bit copy of a system's storage devices ensures all data, including deleted files and slack space, is captured. This process preserves the original state of the system for analysis. https://www.geeksforgeeks.org/digital-evidence-preservation-digital-forensics/

	○ Discussing specific preservation techniques, such as hash generation and imaging ○ Presenting their findings, focusing on best practices for each data type. **Paired activity - Hash function practice** ○ Learners will practice creating hash functions and checksums to ensure data integrity in forensic images. Each pair will: ○ Generate a hash for a set of sample files ○ Alter one file and recheck the hash to observe any changes ○ Reflect on how hash verification can detect tampering or corruption.	
D2.1.2 Requirements for the recording of all findings and considering how reliable the evidence is D2.1.3 Requirements for the recording of any alterations that have been intentionally and unintentionally imposed by the investigator	**Whole class instruction teaching and learning – Introduction** ○ Introduce the concept of chain of custody in digital forensics, emphasising its role in maintaining the integrity and reliability of evidence. ○ Explain essential practices, such as ensuring only competent individuals handle evidence, and discuss examples where improper handling compromised cases. ○ Explain the importance of documenting any changes made to evidence, whether accidental or intentional, and introduce the concept of evidence admissibility. **Small group activity - Building a chain of custody process** ○ Groups will design a basic chain of custody process for a forensic case scenario. Each group will: ○ Outline key steps in handling digital evidence from initial collection to final storage ○ Identify potential risks to evidence integrity at each step	Chain of Custody: The chain of custody refers to the chronological documentation of evidence handling, from its initial collection to its presentation in court. Maintaining an unbroken chain of custody is vital for demonstrating that the evidence has remained untampered and is in the same condition as when it was first collected. This process involves detailed records of who collected the evidence, the methods used, and any transfers or analyses conducted. https://www.infosecinstitute.com/resources/digital-forensics/computer-forensics-chain-custody

	○ Present their chain of custody process, highlighting measures to prevent data alteration. **Paired activity - Examining evidence reliability** ○ Pairs will review sample forensic reports and analyse the methods used to protect evidence reliability. Each pair will: ○ Identify actions taken to avoid altering data on the device ○ Assess how responsibilities are documented to ensure accountability ○ Share findings with the class, discussing how these practices contribute to evidence admissibility. **Individual activity - Reflective journal on preserving evidence integrity** ○ Learners will write a reflective journal entry on the importance of working with copies rather than originals. They will: ○ Summarise key reasons for preserving the original device/data untouched. ○ Reflect on how they would approach a case where working with a copy was not possible, documenting all potential changes. ○ Consider what they've learned about balancing evidence integrity with investigation requirements.	
D2.1.4 Requirements for the creation of visual evidence of findings	**Whole class instruction teaching and learning - Introduction** ○ Introduce the role of visual evidence in forensic investigations. Explain why photos, videos, screenshots, and metadata are crucial for documenting digital evidence in a way that can be easily verified and presented in legal or internal investigations. Use examples of visual documentation, such as timestamped screenshots, to illustrate key practices.	Metadata in forensics https://www.ironhack.com/gb/blog/metadata-forensics-when-files-can-speak-and-reveal-the-truth

	Small group activity - Capturing visual evidence ○ Each group will be provided with a mock "evidence" scenario on a computer system, such as an open document or file directory. Their tasks are to: ○ Capture screenshots of the evidence, including timestamps. ○ Take "photos" (using smartphones if allowed or as simulated steps) of any physical components relevant to the scenario. ○ Create a brief "report" explaining the context and method of each visual capture to ensure clarity in a court or review setting. **Paired activity - Metadata analysis** ○ Pairs will be given a sample file or image with metadata. They will: ○ Analyse the metadata to determine key details such as creation date, last modified date, and any geolocation data. ○ Document their findings, discussing how these details could support or refute claims in an investigation. ○ Present their metadata findings to the class, explaining the significance of each metadata element in the forensic process.	
D2.1.5 Ensuring the evidence is relevant and not a false positive	**Whole class instruction teaching and learning - Introduction** ○ Introduce learners to the concept of false positives in digital forensics, discussing how irrelevant data can complicate investigations. Explain how tools like file signatures and search criteria help narrow down relevant evidence and reduce errors. **Small group activity - Creating search criteria for relevance** ○ Give each group a list of files (simulated or written on paper) containing a mix of relevant and irrelevant items (e.g., a case	False positives ruining people's lives (case studies) https://solicitorsnortheast.co.uk/false-positives-in-digital-evidence-ruining-peoples-lives/ False positives and negatives

	involving image files where only specific formats or names are relevant). Their tasks are to: ○ Define search criteria, such as specific file types, names, or keywords, to identify relevant items. ○ Share their criteria with the class, explaining how it helps reduce false positives.	https://www.guardrails.io/blog/false-positives-and-false-negatives-in-information-security/ Problems of false positives https://censys.com/the-perils-of-false-positives/
D2.2.1 Provide evidence of a crime and/or an incident	**Whole class instruction teaching and learning - Introduction** ○ Explain how cyber forensic findings are assessed to determine whether they indicate evidence of criminal activities, regulatory breaches, or cyber incidents. ○ Introduce categories such as criminal offenses, regulatory breaches, civil liability, policy non-compliance, cyber-attacks, and instances of negligence or mismanagement. Use case examples to illustrate how incidents might fall into one or more categories. ○ Prompt discussion on the potential consequences of these findings for organisations, focusing on legal and operational impacts. **Small group activity – Case analysis for evidence classification** ○ Assign each group a real or hypothetical forensic case study. Have groups analyse the findings to: ○ Identify potential categories of incidents (e.g., criminal, cyber-attack, negligence). ○ Determine indicators within the evidence that might support each classification. ○ Predict potential impacts based on the classification. ○ After the analysis, groups will present their findings, discussing how each case fits into the given categories.	Categorising incidents https://ico.org.uk/action-weve-taken/data-security-incident-trends/glossary-of-terms/incident-categories/ https://www.ncsc.gov.uk/information/categorising-uk-cyber-incidents

	Pair activity – Consequences of evidence classification ○ Ask each pair to select one category (e.g., regulatory breach, internal policy non-compliance) and research real-life consequences organisations face when findings support such classifications. They will: ○ Summarise a case and its classification. ○ Describe legal, financial, and operational consequences for the organisation. ○ Suggest preventative strategies that could reduce recurrence. ○ Pairs will share their case study findings with the class. **Individual activity – Visual representation of incident categories** ○ Have learners individually create an infographic or concept map categorising types of cyber incidents, using examples and illustrating the consequences of each type (e.g., regulatory breaches, cyber-attacks). ○ They should visually connect how these types interrelate and how each can impact an organisation.	
D2.2.2 Show that the system has been externally and/or internally compromised	**Whole class instruction teaching and learning - Introduction** ○ Introduce indicators of potential system compromise, covering unusual traffic patterns (inbound, outbound, geographically unusual), signs of DoS/DDoS attacks, and other anomalies such as irregular login attempts and DNS requests. ○ Explain each indicator's role in forensic analysis, emphasising how these signs point to either internal or external system compromise. ○ Use visual examples, like heat maps or network flow diagrams, to illustrate different types of unusual network activity.	Indicators of compromise https://www.fortinet.com/resources/cyberglossary/indicators-of-compromise https://www.microsoft.com/en-gb/security/business/security-101/what-are-indicators-of-compromise-ioc

	Small group activity – Traffic and access anomaly identification ○ Provide each group with simulated network data logs that include various anomalies (e.g., high-volume inbound traffic from a specific region, multiple failed login attempts, or unusual DNS queries). Have groups: ○ Identify signs of compromise in the logs. ○ Classify each anomaly as indicative of an internal or external compromise. ○ Suggest a possible source or intent behind each anomaly (e.g., DoS attack, internal sabotage). **Individual activity – Suspicious activity infographic** ○ Learners will create an infographic that visually represents various indicators of system compromise. The infographic should include categories like unusual traffic, DNS requests, and suspicious data/file changes, with icons or diagrams illustrating each. Encourage learners to use brief descriptions to clarify how each indicator might appear in a system log or alert.	https://www.cloudflare.com/en-gb/learning/security/what-are-indicators-of-compromise/
D2.3.1 Actions to prevent security incidents from reoccurring in the future	**Whole class instruction teaching and learning - Introduction** ○ Discuss the importance of writing comprehensive security reports to prevent future incidents. ○ Explain key sections of a report, such as identifying procedural errors, unforeseen challenges, and specific areas for improvement in detection and response. ○ Use a sample security incident to guide learners through how structured reporting can highlight vulnerabilities and remediation.	Incident reports https://safetyculture.com/topics/incident-report/ https://www.dataguard.co.uk/blog/how-soon-after-an-incident-should-you-write-a-report/

	Pair activity - Remediation recommendation report ○ Each pair will draft a report outline for a chosen incident, focusing on suggested remedial actions to prevent recurrence. They will include: ○ Headings and sub-headings to structure sections like procedural errors and unforeseen problems. ○ Proposed actions for procedural, technical, and training improvements. ○ Pairs will exchange their outlines with another pair for feedback on clarity and completeness.	
D2.3.2 Improvements to the content of IT policies	**Whole class instruction teaching and learning - Introduction** ○ Introduce the concept of updating IT policies as a proactive approach to cyber security. ○ Explain how effective policies contribute to preventing incidents by setting clear guidelines on system use, data handling, and security measures. ○ Review examples of outdated policies and discuss how they could be improved to reflect current security needs. **Small group activity - Policy gap analysis** ○ Each group will review a sample IT policy and identify potential gaps or areas for improvement, such as outdated password protocols or insufficient data access controls. ○ Their task is to: ○ Highlight weaknesses in the policy. ○ Suggest specific updates or additions that would strengthen the policy (e.g., adding multi-factor authentication requirements). ○ Present their recommendations to the class, discussing how each improvement could prevent future security incidents.	BYOD policy creation https://www.ncsc.gov.uk/collection/device-security-guidance/bring-your-own-device/action-2-develop-the-policy Write a policy https://www.pdq.com/blog/how-to-write-a-company-it-policy/ https://clickup.com/blog/it-policies-and-procedures/

	Pair activity - policy update proposal ○ In pairs, learners will draft a proposal for updating a specific policy area, such as data protection or employee access controls. Their proposal should include: ○ A brief assessment of the current policy's limitations. ○ Recommended policy updates, such as enhanced data encryption requirements or employee security training. ○ Pairs will then present their proposals, explaining how these changes improve overall security.	
D2.3.3 Improvements to security protection measures	**Whole class instruction teaching and learning - Introduction** ○ Introduce the categories of security protection measures—physical, software, hardware, processes and procedures, and training. ○ Use real-world examples to illustrate how these measures work together to protect against cyber threats. ○ Explain how evaluating and enhancing these areas can close gaps in security and help prevent incidents. **Small group activity - Security enhancement analysis** ○ Assign each group one category of security protection measures (e.g., physical or software). Their task is to: ○ Identify common weaknesses in their assigned category. ○ Research and propose specific improvements (e.g., implementing biometric access for physical security or updating antivirus software for software security). ○ Present their suggestions to the class, detailing how these enhancements reduce vulnerabilities and improve security.	Training: Educates personnel on security best practices. Enhancements include regular cybersecurity awareness programs, phishing simulation exercises, and role-based security training to ensure staff are equipped to recognize and respond to threats. https://www.npsa.gov.uk/security-culture Processes and Procedures: Establishes standardised protocols for security operations. The NCSC's Cyber Security Design Principles offer a framework for developing secure systems and processes. https://www.ncsc.gov.uk/collection/cyber-security-design-principles

Delivering signposted transferable skills

Signposted transferable skills are not mandatory for the delivery of the unit, and it is therefore your decision to deliver these skills as a part of the qualification. Below we have provided some ideas of teaching and learning activities that you could use to deliver these skills if you chose to.

Transferable skills	Ideas for delivery
SP – CT Critical thinking	Case study analysis: • Summarise the key issues in their own words • Create mind maps identifying core problems and related factors • Write problem statements that demonstrate understanding of complex situations Research projects: • Create annotated bibliographies justifying their source selections • Compare contrasting viewpoints from different sources • Build evidence tables showing which information supports different arguments • Develop research portfolios documenting their information gathering process Evaluation exercises: • Fact-check news articles and identify potential bias • Create credibility scorecards for different sources • Design evaluation matrices comparing different solutions • Lead peer discussions analysing the strength of different arguments Real-world problem-solving: • Create decision trees showing their analytical process • Develop presentations explaining how they reached their conclusions • Participate in structured debates defending their reasoning

Resources

This section has been created to provide a range of links and resources that are publicly available that you might find helpful in supporting your teaching and delivery of this unit in the qualification. We leave it to you, as a professional educator, to decide if any of these resources are right for you and your students, and how best to use them.

Pearson is not responsible for the content of any external internet sites. It is essential that you preview each website before using it to ensure the URL is still accurate, relevant, and appropriate. We'd also suggest that you bookmark useful websites and consider enabling students to access them through the school/college intranet.

Websites

Action Fraud - UK's national fraud and cybercrime reporting center
www.actionfraud.police.uk

BCS Security Group - Professional body for IT practitioners with a focus on security
www.bcs.org/security

Centre for the Protection of National Infrastructure (CPNI) - UK government authority for protective security advice
www.cpni.gov.uk

CREST UK - Certification body for the technical security industry
www.crest-approved.org

Cyber Aware - UK government's advice on how to stay secure online
www.cyberaware.gov.uk

Cyber Essentials - UK government-backed certification scheme
www.cyberessentials.ncsc.gov.uk

Cyber Security Challenge UK - Organization running cybersecurity competitions and learning programs
www.cybersecuritychallenge.org.uk

Department for Digital, Culture, Media & Sport - UK government department overseeing cyber policy
www.dcms.gov.uk/cyber-security

GCHQ - UK's intelligence and security organization
www.gchq.gov.uk

Information Commissioner's Office (ICO) - UK's independent authority for data protection and information rights
www.ico.org.uk

Institute of Information Security Professionals (IISP) - UK's professional body for cybersecurity practitioners
www.iisp.org

ISO 27001:2013 - International Organization for Standardization's information security standard
www.iso.org/isoiec-27001-information-security.html

Kaspersky Live Cyber Attack Map
https://cybermap.kaspersky.com/

National Cyber Security Centre (NCSC) - UK's technical authority for cyber security incidents and guidance
www.ncsc.gov.uk

National Institute of Standards and Technology (NIST) - US authority for cybersecurity standards and guidelines
www.nist.gov

Open Web Application Security Project (OWASP) - International web security community and standards
www.owasp.org

Radware Live Threat Map
https://livethreatmap.radware.com/

Textbooks

Bhardwaj, D.A., Kaushik, K., Practical Digital Forensics: Forensic Lab Setup, Evidence Analysis, and Structured Investigation Across Windows, Mobile, Browser, HDD, and Memory, BPB Publications, 2023, (978-93-5551-145-4).

Kiser, Q., Computer Networking and Cybersecurity: A Guide to Understanding Communications Systems, Internet Connections, and Network Security Along with Protection from Hacking and Cyber Security Threats, 2020, (9798682990887).

Lammle, T., Buhagiar, J., CompTIA Network+ Study Guide: Exam N10-009, Sybex, 2024, (978-1-394-23560-5).

Neil, I., CompTIA Security+ SY0-701 Certification Guide: Master cybersecurity fundamentals and pass the SY0-701 exam on your first attempt;, Packt Publishing, 2024, (978-1-83546-153-2).

Oettinger, W., Learn Computer Forensics: Your one-stop guide to searching, analyzing, acquiring, and securing digital evidence, 2nd Edition, Packt Publishing, 2022, (978-1-80323-830-2).

Sammons, J., The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics, Syngress, 2014, (978-0-12-801635-0).

Sheward, M., Digital Forensic Diaries, 2017, (978-1-5215-1446-7).

Spafford, E., Metcalf, L., Dykstra, J., Cybersecurity Myths and Misconceptions: Avoiding the Hazards and Pitfalls that Derail Us, Addison-Wesley Professional, 2023, (978-0-13-792923-8).

Walker, S., Cybersecurity Bible: The Complete Guide to Detect, Prevent and Manage Cyber Threats Includes Practical Tests & Hacking Tips for IT Security Specialists, 2024, (9798336422184).

Pearson paid resources also available

- Pearson Student book
- ActiveBook (a digital version of the Student Book, via ActiveLearn Digital Service)
- Digital Teacher Pack (via ActiveLearn Digital Service)

Unit 3: Website Development

Unit overview

Unit 3: Website Development	
Assessment type: Internal	
Learning Aim	**Topics**
A Understand how the principles of website development are used to create effective websites	A1 Purpose and principles of websites A2 Planning a website in response to a client brief
B Explore website design skills and techniques to meet client requirements	B1 Website design B2 Asset management techniques
C Develop a website to meet client requirements	C1 Common tools and techniques to produce a website C2 Website development processes C3 Testing
Assessment overview This unit is Internal assessed through a Pearson-Set Assignment Brief (PASB). Pearson sets the assignment for the assessment of this unit. The PSAB will take approximately 15 hours to complete. The PSAB will be marked by centres and verified by Pearson. The PSAB will be valid for the lifetime of this qualification.	

Common misconceptions

Below are some common misconceptions related to the content of this unit by students and ideas for how you can help your learners to avoid and overcome these.

What is the misconception?	How to help learners overcome it
Inline CSS styles should be used instead of external spreadsheets.	Learners can explore inline CSS Styles by following tutorials on w3school's to support the development of understanding of CSS. https://www.w3schools.com/html/html_css.asp
Closing HTML Tags is optional	It's best practice for programmers to ensure each opening HTML tag has a closing tag. The only exception to this are the following HTML tags. • <area>: Used for the area inside of an image map • <base>: The base URL for all relative URLs in a document • : A line break • <img>: The image tag • <link>: Sets linkage between a document and an external resource

Learning Activities and Resources

This section offers a starting point for delivering the unit by outlining a logical sequence through the unit topics and suggesting practical activities and teacher guidance for covering the main areas of content during guided learning time. Transferable skills are integrated into various activities, with those embedded in a unit indicated by an acronym in square brackets. The acronym combines the letters from the broad skill area and the specific transferable skill, e.g., [IS-WC].

Please note the activities provided below are suggestions and not mandatory. Pearson is not responsible for the content of any external internet sites. It is essential that you preview each website before using it to ensure the URL is still accurate, relevant, and appropriate.

Learning Topic	Activities and guidance for unit content delivery	Resources
A1 Purpose and principles of websites	**Whole class teaching and learning – Introduction** • Using visual aids and examples of different websites with the following purpose (e-commerce, provide information, promote products or services and to provide entertainment.) • Have a class discussion looking at how different websites achieve the purpose of each category. For example, how Amazon falls into the e-commerce and promoting products category. **[EL-SRS]** • Have interactive discussions about student's own experiences of websites that they actively use. For example, they may discuss they come have YouTube promoting. **[EL-PRS]** **Whole class teaching and learning – Target Audience** • Present the user demographics to the class. These will typically include age, gender, location, income, education and types of technology usage. **Independent task – Demographics of websites**	**Amazon** – e-commerce website: Amazon.co.uk **Wikipedia** – Information Website: Wikipedia.com **BBC I-Player** - Entertainment based website: bbc.co.uk/iplayer **Netflix** – Entertainment based website: netflix.com/ **Apple** – Promotion of products: apple.com

	• Ask learners to research the typical demographics of a range of websites and user personas of typical users. **[IS-WC]** **Whole class teaching and learning – Principles of website development** • Introduce students to principles of website development. This includes page layout, navigation, content and design, user experience, consistency, user friendliness, dynamic websites, cross browser compatibility and search engine optimisation. • Ask learners to carry out a review of current websites and describe the key principles of website development that have been implemented. This can cover a range of websites from the identified purposes stated in the specification but also be structured by the teacher to direct learner engagement. **[IS-WC]**	
A2 Planning a website in response to a client brief	**Whole class teaching and learning – Planning a website in response to a client brief** • Using visual aids and examples of client briefs, demonstrate to the learners what a typical client brief may look like when a client requires a new website to be developed for a set purpose. • Examples of client briefs: • **Example 1** ○ **Client Name**: GreenLeaf Organic Foods **Business Background**: GreenLeaf Organic Foods is a family-run business specialising in selling organic produce online. The company wants to expand its customer base and enhance its digital presence to compete with larger competitors. Currently they don't have a logo. ○ **Project Overview**: We need a complete redesign of our current website. The current site feels outdated and doesn't reflect our eco-friendly and	

	modern brand identity. We want to improve the user experience and increase online sales whilst having a new logo design. ○ **Key Goals**: ○ Increase online sales by 25% in the next six months. ○ Improve website navigation and user experience for both mobile and desktop users. ○ Reflect our brand's eco-friendly values visually and functionally. ○ **Specific Requirements**: ○ Integrate a modern, mobile-friendly design. ○ Add a blog section for organic lifestyle tips. ○ Include a "farm-to-table" story page showcasing where our produce comes from. ○ Improve the checkout process to reduce cart abandonment rates. ○ Ensure integration with our existing stock management system. ○ **Deadline**: Three months from project start. **Budget**: £16,000. • **Example 2: Marketing Campaign Brief** ○ **Client Name**: GlowFit Gym **Business Background**: GlowFit Gym is a chain of boutique fitness centres catering to young professionals. The company plans to launch a new premium fitness programme called "GlowFit Elite" to attract high-income clients. ○ **Project Overview**: We need a marketing campaign to introduce GlowFit Elite to our target audience. The campaign should position the programme as exclusive, results-driven, and worth the premium cost. ○ **Key Goals**:	

	○ Attract 500 new GlowFit Elite members within three months of the campaign launch. ○ Increase GlowFit Elite awareness on social media by 40%. ○ Generate leads for personalised consultations with sales representatives. ○ **Specific Requirements**: ○ Design a series of Instagram and LinkedIn adverts targeting young professionals. ○ Create a video showcasing the programme's unique benefits and real client success stories. ○ Set up a landing page to capture leads and schedule consultations. ○ Use metrics such as click-through rates and sign-up conversions to track campaign success. ○ **Deadline**: Campaign to launch within six weeks and run for three months. **Budget**: £8,000 for creative and paid adverts. ○ Discuss how to draw out the key information from the information, establishing the purpose, the problems to be solved, key messages and overall goals of the client. • The intended audience and technical requirements should be identified where possible. **Small group activity - Client consultations activity** • Assign learners groups where each learner will take on the role of the client.	

	• The purpose of this activity is to help learners to ask the right questions to gather information about the purpose, key messages, and problems the website aims to solve. • A checklist could be provided to the learners about website goals, audience, and challenges the website should address. **[IS-V&NC]** **Whole class teaching and learning – Legal and ethical constraints** • Learners to be taught direct content on copyright, data protection, digital accessibility and the structure of a website. • This can be done as a presentation and supported by visual aids and links to current and relevant copyright/data protection articles / video news reports. **Small Group Activity - Case study analysis** • Present case studies involving real or hypothetical copyright infringement cases related to web content, images, or videos to the learners. This activity will help learners understand what constitutes copyright infringement, the importance of using licensed or original content, and potential legal implications. • Questions can be provided for analysis (e.g., "What could have been done to avoid this issue?") and encourage discussion on ethical content use. • The overall outcome of this activity is that learners will learn to recognise copyright risks and understand the value of respecting intellectual property rights in digital work. **[IS-T]**	
B1 Website design	**Whole class teaching and learning – Wireframes and designs**	Wireframe.cc – Free wireframing design software https://wireframe.cc/

	• Using visual aids and modelled examples introduce wireframe tools such as sketching on paper, graphic design software, UX design software and wire framing apps. • Show students how they can be used to design the visual elements of a website. • Model scenarios can be given to the learners to enable key client objectives to be achieved in the design phase of website design. **Small Group Activity – Wire framing techniques and design ideas** • Ask students to use wire framing techniques including hierarchy of page elements, balance of content, grouping, aligning of elements and accurate dimensions. • Visual styles will also allow learners to look at visual styles including colour palette, branding and typography. **Paired Activity – Reviewing fitness for purpose** • Give students tasks to review different types of websites to review the fitness for purpose, the clarity and details, user requirements and how each website meets the client requirements. • The tasks above will allow learners to be able to approach the design stage of web development to support progression onto a PSAB.	
B2 Asset management techniques	**Whole class teaching and learning – Asset management techniques** • Introduce learners to the idea of creating their own assets including writing headlines and copy. • This includes short sentences and paragraphs, avoiding jargon and appropriate modes of address. This will allow learners to be creative in their approach to designing assets to meet client needs. **[SP-C&I]**	Unsplash – Royalty free image website https://unsplash.com/ Pexels – Royalty free images and video website https://www.pexels.com/

	Paired activity – Image editing / manipulation techniques
	• Pair learners and ask them to undertake image editing and manipulation techniques.
	• Learners can learn different editing / manipulation techniques, along with ensuring that images are optimised for a website accordingly. Typically, this will result in the image quality not being affected, but the overall size of the image will be reduced.
	Small group activity – Sourcing assets scavenger hunt
	• Ask learners to look to identify and gather appropriate written copy, stock images, icons and videos. This will require learners to find royalty free content and gathering sources directly themselves. **[EL-PRS]**
	• Learners can be provided with a mock project brief (e.g. such as creating a website for a coffee shop).
	• Each group can be assigned the task of sourcing assets for the project.
	• This activity can include:
	  ○ **Writing copy**: Write a tagline or description using online copywriting guides.
	  ○ **Collecting images**: Find suitable royalty-free images from platforms like Unsplash or Pexels.
	  ○ **Collecting icons**: Locate free icons from sources like Font Awesome or Flaticon.
	  ○ **Collecting videos**: Search for relevant stock video clips from platforms like Pexels Videos or Pixabay.
		Flaticon – Royalty free icons https://www.flaticon.com/
		
		Font Awesome – Royalty free icons https://fontawesome.com/
		Pixabay – stock video clips https://pixabay.com/
		
		TinyJPG – Image compression software https://tinyjpg.com/
		
		Adobe Express – Image compression software https://www.adobe.com/express/
		
		Handbrake - Open Source Video Transcoder https://handbrake.fr/

	• Each group can present their chosen assets, explaining their relevance and licensing considerations.
	
	Individual activity – Preparing assets activities
	
	• Provide learners with the following asset activities to develop skills in the following set fields:
	
	  ○ Activity 1 – Video trimming challenge – Trim a video for a specific purpose. For example ask students to trim a video for a 30 second highlight reel.
	
	  ○ Activity 2 – Compression lab – Provide learners with large media files (e.g. 5MB image and a high-resolution video file). Ask learners to compress image files to under 1MB using tools like TinyJPG/Adobe Express and video files to under 50MB. The files should not lose quality after the compression has taken place.
	
	Individual activity – Managing assets
	
	• In this activity, the assets that have been created/modified from the previous task will be sourced accordingly. This will include the suitable naming of folders and files within a logical folder structure. For example, img_home.jpg or vid_welcome.avi.
	
	• This activity will prepare learners to be ready for the PSAB aspect of the unit.	

C1 Common tools and techniques to produce a website	**Whole class teaching and learning – HTML** • Using suitable software (notepad++, Dreamweaver etc.) introduce the new topic of HTML web design. Within this, learners will be taught how to use HTML and to use navigation such as menus, internal and external links and anchors. (w3 Schools)	**W3Schools – HTML Website Tutorials** https://www.w3schools.com/html/default.asp

	• Ask learners to carry out a series of activities to develop their skills in learning HTML to create webpages. Once these skills are embedded, learners will create hyperlinks between the webpages. • Ask leaners to create a webpage using the new skillsets gained from the first activity. They can create a webpage to include text, images, videos, tables of information and forms. **Individual activity – CSS** • Webpages will be enhanced by the use of Cascading Style Sheets (CSS) which will include colour, web typography, text formatting, links and buttons, tables and forms; page layout will also include CSS media queries and layout aesthetics. • Learners could be supported at this stage by a series of step-by-step instructions of how to apply CSS to the websites they have developed. **Whole class teaching and learning - Introduction to JavaScript** • Teacher to lead a series of JavaScript tutorials. This includes displaying images (e.g. sliders and gallery's), displaying information (e.g. accordion, tabs, modal box and filtering of information), animation (e.g. hover effects, transitions, animated logo and motion) and also the use of controlling video and video backgrounds. • Where applicable a search function, shopping cart or interactive maps can be added to the website. **Visit a local web design company**	**W3Schools** – CSS Tutorials https://www.w3schools.com/html/html_css.asp **W3 Schools** – HTML adding tables https://www.w3schools.com/html/html_tables.asp **W3Schools** – Javascript tutorials - https://www.w3schools.com/html/html_scripts.asp **W3Schools** – Adding video in HTML - https://www.w3schools.com/html/html5_video.asp **W3Schools** – Adding audio in HTML -

	• Enhance the learning of the course with a visit a local web design company to investigate their approach for SEO (Search Engine Optimisation) and how this is implemented.	https://www.w3schools.com/html/html5_audio.asp
C2 Website development processes	**Whole class teaching and learning – Accessibility** • Teacher led activity of the importance of accessibility being built into website design. This includes alternative tags, zoom features and text–to-speech. • Learners will research different websites to look at how well/not well they have been applied. They should consider the Web Content Accessibility guidance, World Wide Web Consortium (W3C) standards and HTML5 Standards. **Individual Activity – Website Self Review** • Can learners to individually evaluate a given website or their own website project against the following criteria: o Comparing the website's quality to similar websites in terms of design, functionality, and features. o Assess its suitability for the target audience and purpose, identifying strengths and areas for improvement. o Evaluate how well the website meets client requirements, considering specific goals and deliverables. o Identify any potential legal and ethical issues (e.g., copyright, data protection) and suggest ways to address them.	**W3Schools** – Alt Tags https://www.w3schools.com/tags/att_img_alt.asp **W3Schools** – Zoom functionality - https://www.w3schools.com/accessibility/accessibility_page_zoom.php **World Wide Web Consortium** – Markup validation service https://validator.w3.org **University of Reading** – Evaluating websites: https://libguides.reading.ac.uk/evaluating-websites

	○ Assess the consistency of design elements (e.g., colour scheme, navigation) across the website. ○ Review the website's readability, considering font choices, text layout, and accessibility for diverse users. **Paired Activity – Peer Review** • Ask learners work in pairs to provide feedback on each other's review. • Ask learners to discuss areas of agreement or disagreement. • They should offer constructive criticism to enable each learner to refine each other's evaluations. **Whole Class Teaching and Individual Activity - Website Publishing** • Provide students with an overview of the website publishing process. This includes the technical steps for deploying a website (e.g. hosting, domain setup) where applicable. Discuss the importance of ensuring compliance with legal and ethical guidelines during publication and the final pre-publishing checks for quality and user experience. • Learners then create a checklist for publishing their own or a hypothetical website, incorporating the insights gained.	**BITLAW** – Legal, Ethical and Copyright issues - https://www.bitlaw.com/internet/webpage.html **WebFX** – Website readability tool - https://www.webfx.com/tools/read-able/ **Webflow** – Website design process overview - https://webflow.com/blog/how-to-publish-a-website
C3 Testing	**Whole class teaching and learning - Introduction to testing** • Model an example of a test plan and discuss areas which should be tested on all websites. This includes links, user interactivity expected and the responsiveness to different screen sizes.	**BrowserStack** – How to perform website testing QA https://www.browserstack.com/guide/how-to-perform-website-qa-testing

	• Ask learners to create a test plan to ensure these areas have a suitable plan. They should then carry out their plan and produce test evidence such as screen shots or screen recordings. **Paired activity - Usability testing** • Ask learners to play the role of a user and complete a user testing audit. That can include how the website has taken into account the following criteria: accessibility, logical navigation, clarity of information and user experience.	

Delivering signposted transferable skills

Signposted transferable skills are not mandatory for the delivery of the unit, and it is therefore your decision to deliver these skills as a part of the qualification. Below we have provided some ideas of teaching and learning activities that you could use to deliver these skills if you chose to.

Transferable skills	Ideas for delivery
[EL-SRS] Secondary Research Skills	Within A1, Purpose and Principles of Websites, there is an opportunity for learners to develop secondary research skills. The teacher can provide a model answer, which is then evaluated for the quality and reliability of the secondary data, including checking the source, the date, the purpose, and the method of collection.
[EL-PRS] Primary Research skills	Within A1, Purpose and Principles of Websites, learners can conduct primary research on different types of websites as outlined in the specification. They can analyse the websites to understand how each website has been designed and the features incorporated into its design. Within B2, Asset Management, learners will have the opportunity to carry out primary research activities to collect assets for a set project. This may involve gathering images, sound, and video directly or researching online for royalty-free images.
[IS-WC] – Written Communication	Within A1, Purpose and Principles, an independent task will enable learners to produce a structured document in the style of a report to the teacher, focusing on the demographics of users for different types of websites as identified. This task can then be further developed, either in a group or independent context, by reviewing the identified websites and evaluating whether the implementation of their features is positive or negative based on client needs.
[SP-C&I] – Creativity	Within B2, Asset Management, learners will have the opportunity to demonstrate creativity by creating assets for a website based on a specific theme or purpose.
[IS-T] – Teamwork	The delivery guide includes several opportunities for group and whole-class participation. These activities provide an excellent opportunity for learners to work as part of a team with shared goals while also taking on individual roles and responsibilities.

Resources

This section has been created to provide a range of links and resources that are publicly available that you might find helpful in supporting your teaching and delivery of this unit in the qualification. We leave it to you, as a professional educator, to decide if any of these resources are right for you and your students, and how best to use them.

Pearson is not responsible for the content of any external internet sites. It is essential that you preview each website before using it to ensure the URL is still accurate, relevant, and appropriate. We'd also suggest that you bookmark useful websites and consider enabling students to access them through the school/college intranet.

Websites

Code Academy – Anyone can register on the Codecademy website. It includes free videos and training tutorials on how to develop websites. www.codecademy.com

CSS Zen Garden – This website allows anyone to explore different CSS templates which can be applied to a website design. It includes styles of website layouts and how those layouts can be achieved using CSS. www.csszengarden.com

Markup Validation Service (W3C) – This website allows you to validate website content for free. This enables you to check for errors and ensure that your website is W3C compliant. https://validator.w3.org

w3schools.com – A website is a useful starting point for anyone who wishes to learn how to use HTML, CSS, and JavaScript to produce websites. www.w3schools.comCode Academy – Anyone can register on the

Textbooks

Flanagan D – JavaScript: The Definitive Guide (Definitive Guides), Sixth Edition (O'Reilly Media, 2011) ISBN 9780596805524.

McFarland D – CSS: The Missing Manual, Fourth Edition (O'Reilly Media, 2015) ISBN 9781491918050

McGrath M – HTML5 in Easy Steps, Seventh Edition (In Easy Steps Limited, 2011) ISBN 9781840784251.

Pearson paid resources also available

- Pearson Student book
- ActiveBook (a digital version of the Student Book, via ActiveLearn Digital Service)
- Digital Teacher Pack (via ActiveLearn Digital Service)

Unit 4: Relational Database Development

Unit overview

Unit 4: Relational Database Development	
Assessment type: Internal	
Learning Aim	**Topics**
A Understand how the principles of relational database models, data storage and normalisation are used to create effective relational database solutions	A1 Relational database management systems A2 Manipulating data structures and data in relational databases A3 Normalisation A4 Planning a relational database solution in response to a client brief
B Design a relational database solution to meet client requirements	B1 Relational database design techniques and processes B2 Design documentation B3 Reviewing and refining designs
C Develop a relational database solution to meet client requirements	C1 Producing a database solution C2 Testing the database solution C3 Reviewing the database solution C4 Optimising the database solution
Assessment overview This unit is Internal assessed through a Pearson-Set Assignment Brief (PASB). Pearson sets the assignment for the assessment of this unit. The PSAB will take approximately 15 hours to complete. The PSAB will be marked by centres and verified by Pearson. The PSAB will be valid for the lifetime of this qualification	

Common misconceptions

Below are some common misconceptions related to the content of this unit by students and ideas for how you can help your learners to avoid and overcome these.

What is the misconception?	How to help learners overcome it
Students might confuse the different database keys such as the primary keys, foreign keys, special key and candidate key, thinking they serve the same purpose. They may believe that both are just "special fields" in a table, without fully understanding their distinct roles.	Clarify the difference such as that the primary key uniquely identifies each tuple in a table, while the foreign key is used to link tuples between two tables by referencing the primary key of another table. Use visual aids, like Entity Relationship Diagrams (ERDs), and hands-on examples where students create both keys in connected tables to reinforce the difference.
Students may assume that data and information are interchangeable terms, not realising that data is raw and unprocessed, while information is processed and meaningful.	Use simple, real-life examples. For instance, explain that a list of numbers (data) becomes information only when it's given context (e.g., "monthly sales figures"). Have students work with raw data, perform queries, and observe how it is transformed into useful information.
Students might think that a table and a relation are fundamentally different concepts, when in fact, in relational databases, they are the same thing. They may assume a relation is more abstract or technical.	Reinforce that a relation is just the formal term for a table in a relational database. Use the terms interchangeably during lessons to reduce confusion. Encourage students to practice writing queries where they work with multiple relations (tables).
Some students assume that once a table is in Second Normal Form (2NF), it is automatically in Third Normal Form (3NF), not realising that 3NF addresses a different type of dependency (transitive dependency).	Use examples where a table is in 2NF but still has transitive dependencies (i.e., a non-key attribute depends on another non-key attribute). For instance, in a table containing student information, if "city" depends on "postcode," which depends on the primary key, it's not in 3NF. Demonstrate how to remove these transitive dependencies to achieve 3NF.
Students might confuse the different database keys such as the primary keys, foreign keys, special key and candidate key, thinking they serve the same purpose. They may believe that both are just "special fields" in a table, without fully understanding their distinct roles.	Clarify the difference such as that the primary key uniquely identifies each tuple in a table, while the foreign key is used to link tuples between two tables by referencing the primary key of another table. Use visual aids, like Entity Relationship Diagrams (ERDs), and hands-on examples where students create both keys in connected tables to reinforce the difference.
Students may assume that data and information are interchangeable terms, not realising that data is raw and unprocessed, while information is processed and meaningful.	Use simple, real-life examples. For instance, explain that a list of numbers (data) becomes information only when it's given context (e.g., "monthly sales figures"). Have students work with raw data, perform queries, and observe how it is transformed into useful information.

Learning Activities and Resources

This section offers a starting point for delivering the unit by outlining a logical sequence through the unit topics and suggesting practical activities and teacher guidance for covering the main areas of content during guided learning time. Transferable skills are integrated into various activities, with those embedded in a unit indicated by an acronym in square brackets. The acronym combines the letters from the broad skill area and the specific transferable skill, e.g., [IS-WC].

Please note the activities provided below are suggestions and not mandatory. Pearson is not responsible for the content of any external internet sites. It is essential that you preview each website before using it to ensure the URL is still accurate, relevant, and appropriate.

Learning Topic	Activities and guidance for unit content delivery	Resources
A1 Relational database management systems	**Whole class discussion – Introduction to databases** • Start the unit by showing students some data sets and discussing what is meant by the term *data*, what data could be stored about them, and where it is stored. • Show students some data in a database and discuss the meaning of the term *database* and the benefits of keeping data structured in this way (e.g., data can be searched quickly, it can be backed up more easily). **Paired activity – Desktop and server databases** • Ask students to research the difference between desktop databases and server databases, including the benefits and drawbacks of each approach. Students can then share their findings with the class. **Whole class teaching and learning – Database demonstration** • Show students example databases and ask them to identify and discuss different database structures (e.g., relation, attribute, domain, tuple, degree, cardinality) and what they mean.	Notes on desktop and server databases, e.g. Database management – databasemanagement.fandom.com Computer Science GURU Notes on key database terms – computerscience.gcse.guru Tech Target – technology – related content and resources for IT professionals and business techtarget.com Data.gov.uk – Government open data portal – Example datasets for a range of different databases data.gov.uk

	• Demonstrate how to draw entity-relationship diagrams for a range of different databases using one-to-one, one-to-many, and many-to-many relationships. • Demonstrate how to set up a database using suitable software. While doing this, reinforce different concepts, including various relational keys (e.g., super key, candidate key, primary key, foreign key) and why these must be defined. • Explain the two main types of integrity constraints (entity integrity and referential integrity) and discuss how these rules help improve the correctness of data. • Demonstrate how to use relational algebra sets and symbols (e.g., union, intersect, join, and select) to query a database to find data that meets set criteria. **Paired activity – Reinforcement activity** • Give students descriptions of different database tables and ask them to identify the various database concepts and relational keys. • Give students descriptions of different databases and ask them to create entity-relationship diagrams. This can be extended by asking students to identify the different relational keys that would be used.	Teach-ICT – Notes Entity Relationship Diagrams (ERDs), e.g. – teach-ict.com Database software (e.g. Microsoft Access, MySQL, Oracle)
A2 Manipulating data structures and data in relational databases	**Whole class discussion – Why do databases need to be manipulated?** • Start this topic by asking students to think of examples of when data about them needs to be updated, modified, deleted, or when new information about them needs to be stored. • Discuss what would happen if data within databases was static and never updated. **Paired activity – Purposes of queries and reports** • Ask students to research the purpose of a database query and specific examples for different contexts. Students can then share their findings with the class.	**Computer Science GURU** – Notes on database queries, e.g computerscience.gcse.guru **Data.gov.uk** – Government open data portal – Example datasets for a range of different databases, e.g. Find open data – data.gov.uk

	• Ask students to research the purpose of a database report and good practices that could be followed when designing a report. Students can then share their findings with the class. **Whole class teaching and learning – Queries and reports demonstration** • Demonstrate how to set up a query using a graphical user interface. At first, this can be kept simple using a single table with basic search criteria. For example, you might query a particular customer in the database to update, modify, or delete the data. Next, use multiple tables and more complex search criteria. This could be extended further by demonstrating the use of SQL. **Paired activity – Reinforcement activity** • Give students a database and ask them to run specific queries to update, modify, and delete data from the database.	
A3 Normalisation	**Whole class activity – Problems of un-normalised databases** • Show students an un-normalised database and ask them to identify the problem with it (e.g., it contains duplicate data) and discuss the issues this can create (e.g., creates inconsistencies, makes maintenance more difficult). • Ask students to predict what issues the next stage might address before demonstrating. • Model how anomalies can be created when updating, inserting, and deleting data. Explain that this can be reduced by normalising the database. **Whole class activity – Stages of normalisation** • Next, tell students the characteristics of each normal form and demonstrate how to apply these characteristics by taking un-normalised data and showing students how to put it into first, second, and then third normal form. **Paired activity – Normalisation exercises** • Give students different un-normalised datasets and ask them to normalise these into third normal form. Once students have done this, ask them to	**LearnLearn** – Notes on database normalisation learnlearn.uk **ADA Computer Science** – Free computer science resources adacomputerscience.org **Data.gov.uk** – Government open data portal – Example datasets for a range of different databases, e.g. Find open data – data.gov.uk **Kaggle datasets** – AI and ML community https://www.kaggle.com/datasets

	draw an entity-relationship diagram to show how the entities link together. Students could then share their answers with the rest of the class. **Paired activity – Referential integrity** • Ask students to research the purpose of referential integrity. • Students can then share their findings with the class. • After the research, demonstrate a practical example of referential integrity using the datasets normalised earlier. • Challenge students to think of scenarios where referential integrity might be violated (e.g., orphan records) and how to avoid these. **Paired activity – Data dictionary** • Ask students to create a data dictionary for each dataset they normalised earlier. • Provide a template for the data dictionary to help students structure their work. Within this, they should clearly indicate where referential integrity can be used and the different keys that will be used (e.g., primary, foreign, and composite). Students could then share their answers with the rest of the class.	
A4 Planning a relational database solution in response to a client brief	**Whole class discussion – Scoping a database** • Tell students to imagine that they have been asked to create a database from scratch. • Ask students to discuss the different stages that could be involved when creating a new database. • Provide a visual aid, such as a flowchart or timeline, to show the stages of database development and their order. • Use guiding questions to encourage deeper thinking, such as: "What could go wrong if you skipped the research stage?" "Why is defining the purpose the first step?"	**Zibtek** – Notes on database development processes, e.g. – zibtek.com

	• Encourage students to connect the stages to real-world examples, such as apps or systems they use • Narrow the stages down to defining the purpose, research, defining the technical vocabulary, and defining the logical structure. • Ask students to discuss why these steps need to be carried out in this order and the possible consequences of not following this order. **Small group activity – Researching the stages of database development** • Split the group into three and then ask each group to research the activities that would be carried out in one stage of database development. This includes: – Group 1 – Defining the purpose. This should include the problem to be solved and any technical requirements that may be specified. – Group 2 – Research. This should include why it's important to research existing databases, the resources available, and key information that should be included to indicate the structure of the database. – Group 3 – Defining the technical vocabulary and defining the logical structure stages of database development. Students can then share their findings with the rest of the group or the class.	
B1 Relational database design techniques and processes	The vast majority of the techniques and processes in this topic have already been covered in A1, A2, A3, and A4. In this topic, students will learn when these different techniques and processes are applied during database development. **Revision – Key database terms** • Start this topic by recapping key database terms such as: relation, attribute, domain, tuple, degree, cardinality, super key, candidate key, primary key, foreign key, composite key, referential integrity, and the stages of normalisation. **Guest speaker** • If possible, invite guest speakers who have either developed or used databases and can tell students about real-world applications, challenges, and best practices in database design and management.	**Tutor Chase** – Notes on database schema, tutorchase.com **Data.gov.uk** – Government open data portal – Example datasets for a range of different databases, e.g. Find open data – data.gov.uk **Database management** – Notes on desktop and server database – databasemanagement.fandom.com

	Whole class discussion – Entity relationship modelling • Tell students that designing a database involves creating a conceptual model that focuses on the high-level structure and purpose of a database, and a logical model that adds more detail to the conceptual model and breaks it down further. Ask students to discuss the techniques and processes they have learned so far to help define the conceptual (e.g., entity names, relationships) and logical models (e.g., entity names, relationships). • Next, discuss the relational algebra that can be used to define the relationships (e.g., one-to-many) and the relational algebra that can be used to perform operations on data (e.g., AND, OR, NOT). **Paired mini group project – Creating a model** • Give students a specific scenario (e.g., a vet appointment system, library management system). • Ask students to create a conceptual model and logical model. • Offer scaffolding, such as a template or checklist for creating the conceptual and logical models • Next, ask students to use relational algebra to define the relationships between the entities. • For relational algebra, provide examples of operations (e.g., selecting records where specific conditions are met) before asking students to apply these techniques independently. • Finally, ask students to use relational algebra to define criteria that can be used to perform operations on the data within the scenario. **Individual activity – DBMS selection and database implementation tools** • Ask students to research the different factors that should be considered when choosing between a server solution or a cloud/server-based solution. Students can then share their findings with the class. • Next, ask students to research the meaning of prototyping and testing and how these can be applied to the design of a database.	

	• Encourage students to summarise their findings in a visual format (e.g., a comparison chart). • Students can then share their findings with the class. **Whole class discussion – Quality, effectiveness and appropriateness** • Ask students to discuss the key factors that should be considered when determining the quality, effectiveness, and appropriateness of a database design. Such factors can include correctness of data, relationships between data, data integrity, and effective normalisation.	
B2 Design documentation	This is a practical topic that allows students to draw on everything they have learned in learning aim A and B and apply this to design a solution to meet client requirements. **Whole class discussion – Design specification key terms** • Tell students what is meant by the term design specification and discuss what this may include. Then focus on the requirements of the brief, audience, purpose, and client requirements. • Discuss what these are and why they must be considered during the design stage of a database, as well as the difference between brief requirements and client requirements. • Encourage students to brainstorm additional factors that could influence a design specification, such as budget or scalability. **Individual activity – DBMS selection and database implementation tools** • Ask students to research the legal and ethical considerations of database design. They should focus their research on data protection legislation and application regulations. Students can then share their findings with the class. **Paired activity – Data structure designs** • Give students a detailed scenario for a new database that needs to be developed (e.g., client appointment scheduler, student enrolment system) and ask students to create a design specification by stating the requirements of the brief, audience, purpose, client requirements, and legal and ethical considerations.	**Microsoft** – Notes of database effective database design, e.g support.microsoft.com **UXPin** – Notes of creating effective user interfaces, e.g. uxpin.com

	• Provide templates or partially completed examples to guide students in creating their design specifications and data structures. • Include peer review: students could exchange their designs and provide constructive feedback based on given criteria. • Students can then draw upon their knowledge of learning aim A and create data structure designs by normalising the data, drawing an ERD, and creating a data dictionary. **Whole class discussion – User interfaces** • Tell students what is meant by the term user interface and why this is used. Show students examples of both good and bad user interface designs and discuss the good and bad features of each. • Ask students to critique the examples, discussing accessibility, usability, and design aesthetics. • Encourage them to think about how user needs should inform design choices. **Individual activity – Form design** • Include a practical demonstration of different form design controls in action before students begin their research • Ask students to research the meaning of practical uses of different form design controls (e.g., input fields, calculated fields, disabled fields). Students can then share their findings with the class. • Students can then embed their knowledge from their research and create a set of user interface designs for the menus, queries, and reports. **Whole class discussion – Testing** • Discuss what is meant by the term testing and the different areas of a database that should be tested. This should focus on data integrity, functionality, accessibility, and usability of the different areas of the database, such as the menus, queries, and reports. • Structure the discussion around real-world examples of failed systems due to poor testing, emphasising the importance of thorough and iterative testing.	

	• Discuss when testing should be carried out during the database development and why. **Paired activity – Implementation plan** • Ask students to research implementation plans. They can start by researching the common reasons why IT projects fail in the real world and how to avoid this. Encourage students to consider factors like stakeholder communication and risk management in their implementation plans. • They could then research the different things that should be included in an implementation plan (e.g., timescales, resources, team members, etc.). Students can then share their findings with the class.	
B3 Reviewing and refining designs	**Whole class discussion – Testing** • Discuss possible ways of involving the client during the development of a database and both the benefits and drawbacks of involving the client. • Next, discuss the different factors that should be considered during a self-review. This can include suitability for the user, meeting client requirements, legal and ethical constraints, and consistency. **Peer review – Design specification** • In the last topic, students created a design specification including details of the brief requirements, audience, purpose, client requirements, data structure designs, and user interface designs. Ask students to peer-review each other's design specifications and provide feedback. This should focus on the factors discussed at the start of the topic (e.g., suitability for the user, meeting client requirements, legal and ethical constraints, and consistency). **Individual activity – Refining and updating documentation** • Ask students to look at the feedback that they received during the peer review and consider which aspects they will implement and which aspects they will disregard, and why. Then, ask students to refine their ideas and solutions by updating the design specification documentation.	**Test Sigma** – Notes on effective database testing – testsigma.com/
C1 Producing a database solution	**Whole class activity – Developing database development skills**	**Tutorial Point** – Database development tutorials – tutorialspoint.com

	• Demonstrate how to use a specific Database Management System (DBMS) such as Microsoft Access to allow students to build up a set of skills. This includes how to create a database, tables, links/relationships between the tables, and validation rules. Alternatively, another approach would be for students to be provided with tutorials for them to work through at their own pace. **Individual activity – Developing a database** • Ask students to use the skills that they have developed so far to implement the tables from their design specification. They should create the database, tables, links/relationships, and the data validation. • Encourage students to document their implementation process, noting any challenges they face and how they overcome them. • Students can either use the design specification that they have created in an earlier topic or they can be given one that has already been made. **Whole class activity and individual activity – Structured Query Language (SQL)** • Provide examples of both simple and complex SQL commands, breaking them into manageable steps. • Once students have a good understanding of these tools, demonstrate how to apply these skills using Structured Query Language (SQL). • This can be done through tutor demonstrations or by providing students with tutorials for them to work through at their own pace. • Next, ask students to write SQL to implement the same tables from their design specification again. However, this time, they should create the tables, links/relationships, and the data validation using an SQL approach. • Discuss the differences between the two approaches and the benefits and drawbacks of each approach. **Whole class activity – Generating outputs and creating a user interface** • Demonstrate how to generate outputs such as queries and reports. This can be built up by demonstrating how to write simple query search criteria on a single field/table.	**W3Schools** SQL tutorials – w3schools.com

	• This can then be expanded to include more advanced queries involving complex criteria on multiple tables. • Then, demonstrate how to create reports and model good practice with presentation features. • Finally, demonstrate how to create user interfaces to navigate around the user interface, including data entry forms and child forms. • Provide a checklist of good practices for creating reports, such as consistent formatting, clear titles, and summarised data. **Individual activity – Developing outputs and a user interface** • Ask students to use the skills that they have developed so far to implement the queries, reports, and user interface from their design specification. • Students can either use the design specification that they have created in an earlier topic or they can be given one that has already been made. • Encourage students to test their outputs and interfaces by simulating user scenarios. **Whole class activity and individual activity – Populating a database** • Finally, demonstrate how to populate a database with data by importing/adding data from an external dataset. • Emphasise the importance of cleaning and validating external datasets before importing them into the database • Then, give students the opportunity to practice this technique in their own database. **Project-based learning – Database development** • Now that students have developed some database skills, they can be given a different design specification and asked to implement the database on their own. This includes setting up the tables, queries, reports, user interface, and importing data. • Provide a design specification that reflects a real-world scenario and incorporates both basic and advanced requirements. • Encourage students to present their final database, explaining their design choices and reflecting on challenges faced.	

	• Facilitate peer review sessions where students provide constructive feedback on each other's work.	
C2 Testing the database solution	**Whole class and individual activity – Types of testing and test data** • By this point, it is likely that students will have developed a database, imported/added data into the database tables, and created a set of queries, reports, and a user interface. Discuss the importance of testing and the consequences of not thoroughly testing a database before handing it over to the client. Use real-world examples of database failures to illustrate the consequences of inadequate testing • Next, discuss the different types of test data (erroneous, extreme, and normal). Explain what they mean and why it's important to use as many types of data as possible when testing a database. • Additionally, discuss all of the different areas/objects of a database that should be tested (e.g., tables, queries, reports, forms, menus). **Paired activity – Object Testing** • Ask students to use the database that they have developed and write down tests that could be performed to test the different objects. Encourage students to create as many different types of tests as possible, including the use of erroneous, extreme, and normal data. • Encourage students to categorise their tests (e.g., functionality, data integrity, performance) to ensure comprehensive coverage. • Next, ask students to swap their test ideas with their partner and have their partner think of further tests that could be performed. **Whole class and individual activity – Usability testing** • Discuss what is meant by the term usability testing and why this should be carried out in addition to object testing. Discuss how this can be managed and the possible consequences of not carrying out usability testing. Then, discuss how to select suitable test users and why it's important to include more than one type.	**Test Sigma** – Notes on effective database testing – testsigma.com/

	Individual activity – Gather feedback • Ask students to prepare a questionnaire to gather feedback from users. Students should carefully think of the questions they want to ask and how these can lead to improving the database solution. • Suggest categories for questions, such as functionality, user interface design, and user satisfaction. • Teach students to phrase questions neutrally to avoid leading answers and ensure valid feedback. • They should also consider how the questions are relevant for the specific test users.	
C3 Reviewing the database solution	**Whole class and individual activity – Reviewing a database** • Discuss the different factors that should be considered when reviewing a database and why these factors are important. This includes the quality of the database, fitness for purpose, suitability against the original requirements, legal and ethical constraints, and strengths/improvements. • For each factor, discuss different ways/methods of reviewing them. For example, explore the various activities that could be completed to assess the quality of the database or its fitness for purpose. **Individual activity – Gather feedback** • Ask students to use the factors from the discussion to review their database and identify areas for development. Students should ensure that they base their reviews on evidence. For example, this could come from the results of object testing, usability testing, or a review with the client.	Example database files to review
C4 Optimising the database solution	**Whole class and individual activity – Performance of a database** • Discuss all the different factors that can impact the performance of a database. For example, consider the chosen data types, the volume of data, and the accuracy of data normalisation, etc. • For each factor discussed, explore possible solutions. For example, to improve the performance of queries, the solution may be to select only specific columns or use efficient joins/sub-queries. **Individual activity – Optimising a database**	Example database files to optimise

	• Ask students to optimise a database. This can either be a database that they have created themselves or one that has been provided to them for optimisation. • Students can be given a checklist to help them to identify potential performance issues. • Students can practise core optimisation techniques such as indexing, normalisation, and query refinement. • This exercise allows students to understand the impact of these adjustments and helps them recognise best practices in database design and performance tuning.	

Delivering signposted transferable skills

Signposted transferable skills are not mandatory for the delivery of the unit, and it is therefore your decision to deliver these skills as a part of the qualification. Below we have provided some ideas of teaching and learning activities that you could use to deliver these skills if you chose to.

Transferable skills	Ideas for delivery
MY – TPR Taking personal responsibility	There are lots of opportunities for students to demonstrate that they have taken personal responsibility. For example: Students can show that they have chosen techniques and processes that are suitable for the database they are designing. Students can show that they have produced a design specification ensuring it covers the requirements of the brief, audience, purpose, client and legal and ethical considerations. Students can show that they have self-reviewed their worked and refined their database designs before moving the database onto the production stage. Students can show that they have been able to follow their designs and develop a relational database on their own. Students can show that they have tested their developed database using different types of testing. Students can show that they have used criteria to review their database and optimise it to improve its performance.

Resources

This section has been created to provide a range of links and resources that are publicly available that you might find helpful in supporting your teaching and delivery of this unit in the qualification. We leave it to you, as a professional educator, to decide if any of these resources are right for you and your students, and how best to use them.

Pearson is not responsible for the content of any external internet sites. It is essential that you preview each website before using it to ensure the URL is still accurate, relevant, and appropriate. We'd also suggest that you bookmark useful websites and consider enabling students to access them through the school/college intranet.

Websites

Giraffe Academy

A collection of SQL database programming tutorials.
https://www.youtube.com/playlist?list=PLLAZ4kZ9dFpMGXTKXsBM_ZNpJwowfsP49

Neso Academy

A collection of database management systems tutorials regarding database design.
https://www.youtube.com/playlist?list=PLBlnK6fEyqRi_CUQ-FXxgzKQ1dwr_ZJWZ

TutorialsPoint

A collection of webpages covering the theory behind databases and how they are structured. https://www.tutorialspoint.com/dbms/index.htm

W3Schools

A collection of SQL tutorials including an interactive online editor to allow students to experiment with SQL code. https://www.w3schools.com/sql/

Textbooks

Forta, B., SQL in 10 Minutes a Day, 2020 (ISBN 0135182794)

Taylor, A. Database Development for Dummies, 2020 (ISBN 0764507524)

Pearson paid resources also available

- Pearson Student book
- ActiveBook (a digital version of the Student Book, via ActiveLearn Digital Service)
- Digital Teacher Pack (via ActiveLearn Digital Service)

5. Pearson Qualification Support and Resources

This section provides information on support and resources that are available on the Pearson website for this qualification.

Exam Wizard

A free online resource containing a huge bank of past paper questions and support materials to help you create your own mock exams and tests

Pearson Set Assignments (PSABs)

These assignments are set by Pearson and marked internally by the centre. They should be used for all internal assessments on the course. There are specific PSABs for each internally assessed unit on the course.

Purpose Statement

The Pearson Level 3 Alternative Academic Qualification BTEC National in Information Technology (Extended Certificate) is an Alternative Academic Qualification (AAQ) designed for post-16 students with an interest in the Digital sector and aiming to progress to higher education as a route to graduate level employment. Equivalent to one A Level in size, it is suitable for students looking to develop their applied knowledge and skills in Information Technology as part of a study programme alongside A Levels.

Results plus

A free online results analysis tool for teachers giving a detailed breakdown of students' performance in BTEC external assessments.

Specification

This document contains an overview of the qualification, qualification purpose and structure, units including content and assessment, planning and implementing the qualification, qualification grade, glossary of terms used for internally assessed units, Transferable skills framework, digital skills framework, sustainability framework.

Sample Assessment Material (SAMs)

These resources illustrate the format and style of questions for the external assessment for this qualification. A mark scheme is also provided which shows how credit is awarded for these questions. The resources can be used to help prepare learners for their external assessment.

Subject Adviser

A dedicated subject adviser available throughout the year so please do get in touch if you would like any support or guidance with:

- Planning your courses
- Overview of BTEC quality assurance processes
- Suggested resources
- Teaching and Assessment of internal units and components
- Teaching external units and components
- The training and support materials we have available.
- The training and support materials we have available.

Training

Available training sessions can be booked here. On the left-hand side of the screen, select the qualification 'BTEC National' and subject. Where current training is available a list of titles, an overview of the training and dates will be provided giving teachers the option to select and book onto relevant sessions.

Transferable Skills Guide for Teachers

This guide provides and overview of the BTEC Transferable Skills Framework and how it has been used to integrate the delivery of these skills in the new suite of BTEC Level 3 and Level 2 qualifications starting in 2025.

Transition Guide

This guide provides an overview of what's new in the qualification, a comparison of the previous qualification to this new qualification, an overview of the assessment approach, a mapping guide to show where content is the same, updated or new

Annexe

Curriculum Planning

The models in this section are intended to support your delivery planning and provide suggestions for the types and subjects of qualifications that might be delivered with this qualification.

Suggested combinations with other qualifications

This qualification can be combined in the following ways depending on the destination of students.

For students intending to progress to higher education to study Biotechnology

Option 1	Option 2	Option 3
Biology	Mathematics	Statistics

For students intending to progress to higher education to study Marketing.

Option 1	Option 2	Option 3
Business	Media Studies	Mathematics

BTEC Key Terms

GLH – Guided Learning Hours, time the students have supervised teaching and learning

IV – Internal Verification, for internal quality assurance

Lead IV – the person responsible for the internal quality assurance across a qualification or programme subject area.

PSAB – Pearson Set Assignment Brief, used for summative internal assessments

SV – Standards Verification, for external quality assurance

Transferable Skills

Managing Yourself

Acronym	
MY-TPR	Taking Personal Responsibility
MY-PS&R	Personal Strengths and Resilience
MY-COP	Career Orientation Planning
MY-PGS	Personal Goal Setting

Effective Learning

Acronym	
EL-MOL	Managing Own Learning
EL-CL	Continuous Learning
EL-SRS	Secondary Research Skills
EL-PRS	Primary Research Skills

Interpersonal Skills

Acronym	
IS-WC	Written Communications
IS-V&NC	Verbal and Non-verbal Communications
IS-T	Teamwork
IS-C&SI	Cultural and Social Intelligence

Solving Problems

Acronym	
SP-CT	Critical Thinking
SP-PS	Problem Solving
SP-C&I	Creativity and Innovation

March 2025

For information about Pearson Qualifications, including Pearson Edexcel and BTEC qualifications visit qualifications.pearson.com

Pearson Education Limited. Registered in England and Wales No. 872828
Registered Office: 80 Strand, London WC2R 0RL.

VAT Reg No GB 278 537121

Pearson
BTEC