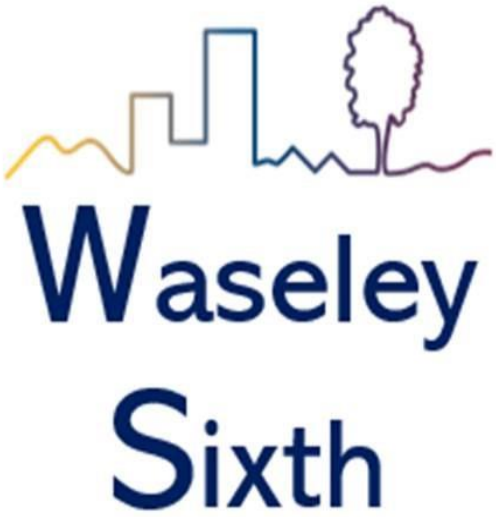

Level 3 IT
Bridging Course

BTEC Level 3 National in Information Technology:

Learner Workbook

Learning Aim A:

Cyber security threats, system vulnerabilities and security protection methods

Learner name	
Tutor name	

DISCLAIMER

This learner workbook is designed to give learners an introduction to the content listed under the essential content section within the specification for **BTEC NQF IT Level 3 Unit 11** (Cyber Security and Incident Management.) Learners must cover all specified content before the assessment.

Tutors need to ensure that this learner workbook is used in conjunction with the following

documents which can be found on the Pearson website:

Equivalent to 1 A Level

UNIT NUMBER	UNIT TITLE	GLH	ASSESSMENT
1	Information technology systems	120	External
2	Creating systems to manage information	90	External
3	Using social media in business	90	Internal
5	Data modelling	60	Internal

Start of Learning Aim A Review

Topic	Checklist Item	Confidence		
		Low	Medium	High
Topic 1 Internal Threats	I know the causes of sabotage and theft and the methods that can be used to reduce them.			
	I know the causes of unauthorised access and the methods that can be used to reduce them.			
	I know the causes of unsafe working practices and the methods that can be used to reduce them.			
	I know the causes of accidental loss, disclosure of data and methods that can be used to reduce them.			
Topic 2 External Threats	I know the meaning of malware, the different types and how they can threaten the security of a computer system.			
	I know the meaning of a virus, the different types and how they can threaten the security of a computer system.			
	I know the meaning of hacking, the different types and how they can threaten the security of a computer system.			
	I know the meaning of social-engineering, the different types and how they can threaten the security of a computer system.			
Topic 3 Impacts of Credible Threats	I know what operation loss means and how this impacts an organisation.			
	I know what financial loss means and how this impacts an organisation.			
	I know what reputation loss means and how this impacts an organisation.			
	I know what intellectual property loss means and how this impacts an organisation.			
Topic 4 System Vulnerabilities	I know why a network may become vulnerable and how to reduce these vulnerabilities.			
	I know why an organisation may become vulnerable and how to reduce these vulnerabilities.			
	I know why software may become vulnerable and how to reduce these vulnerabilities.			
	I know why operating systems may and how to reduce these vulnerabilities.			
	I know why mobile/portable devices may become vulnerable and how to reduce these vulnerabilities.			
	I know why cloud computing may become vulnerable and how to reduce these vulnerabilities.			
	I know what an attack vector is and how to reduce these vulnerabilities.			
	I know where to find information on the latest hardware and software threats.			

Continued on the next page…..

Start of Learning Aim A Review Continued…

Topic	Checklist Item	Confidence		
		Low	Medium	High
Topic 5 Legal Responsibilities	I know the requirements under the Data Protection Act 1998 to keep data safe.			
	I know the definitions of illegal practices under the Computer Misuse Act 1990.			
	I know the requirements to allow companies to monitor employees under the Telecommunications Regulations 2000.			
	I know the requirements under the Fraud Act 2006 to deal with fraud.			
	I know the duties of employers and employees under the Health & Safety at Work Act 1974.			
Topic 6 Physical Security	I know the different uses and effectiveness of locks/card entry systems.			
	I know the different uses and effectiveness of biometrics.			
	I know the different uses and effectiveness of CCTV/alarm systems.			
	I know the different uses and effectiveness of security staff/guards.			
	I know the different types of backups, why they are used.			
	I know the difference between on-site and off-site backups and why they are used.			
Topic 7 Antivirus and Firewalls	I know the use of and effectiveness of antivirus software.			
	I know why antivirus software makes use of signatures and heuristics.			
	I know the use of and effectiveness of firewalls.			
	I know different filtering techniques used by firewall software.			
Topic 8 Authentication & Access Controls	I know what is meant by the term user authentication.			
	I know the different types of user authentication and how effectively they secure data.			
	I know what is meant by the term access control.			
	I know different types of access control.			
	I know different access controls that can be used and how effectively they secure IT systems.			
Topic 9 Encryption	I know what is meant by the term encryption.			
	I know the different uses of encryption.			
	I know the different methods of encryption.			
	I know how effectively encryption methods keep data safe.			
Topic 10 Protecting Wireless Networks	I know why wireless networks are more vulnerable to attacks.			
	I know what is meant by the term MAC address filtering and SSID and how effectively they secure a wireless network.			
	I know different methods of wireless encryption and how effectively they secure a wireless network.			
	I know what should be considered when designing a network			

	to reduce the risks of attacks.			

Introduction

What is Cyber Security?

Introduction

What is cyber security?

1. In your own words **describe** what is meant by the term 'cyber-attack.' **(PASS)**

Type your answer here.

2. **Explain** the different reasons why organisations should keep data safe. **(PASS)**

Type your answer here.

3. **Describe** what is meant by the following types of attack. **(PASS)**

Type	Explanation
Hacker	Type your answer here.
Insider	Type your answer here.
Script kiddie	Type your answer here.
Scammer/Phisher	Type your answer here.

4. **Describe** what is meant by the following motivations for an attack. **(PASS)**

Type	Explanation
Espionage	Type your answer here.
Public good	Type your answer here.
Score settling	Type your answer here.
Public good	Type your answer here.
Thrill	Type your answer here.
Fraud	Type your answer here.

5. In your own words **describe** what is meant by the term 'cyber security.' **(PASS)**

Type your answer here.

Topic 1

Internal Threats

Topic 1: Internal Threats

Topic 1: Topic Objectives:

- **Pass - Describe** what is meant by different internal threats.
- **Merit - Describe** the different methods that organisations could use to reduce the risks caused by internal threats.
- **Distinction - Evaluate** how effectively these security methods reduce the risks caused by internal threats.

Topic 1: Specification Coverage:

A1 Cyber security threats

All systems are vulnerable to attack from external and internal threats.

- Understand how internal threats occur, including:
  - employee sabotage and theft, including of physical equipment or data, and damage such as fire, flood, power loss, terrorism or other disaster
  - unauthorised access by employees and other users to secure areas and administration functions, including security levels and protocols
  - weak cyber security measures and unsafe practices, including security of computer equipment and storage devices, security vetting of visitors, visiting untrustworthy websites
  - accidental loss or disclosure of data, including poor staff training and monitoring.

Topic 1: Introductory Task:

Lookup the word '**Disgruntled**.'

Think of an experience you have had with a company where you became disgruntled (e.g. having to wait 40 minutes in a restaurant for your food to be served).

Describe how this made you feel and how your attitude towards the company changed. **(PASS)**

Type your answer here.

Topic 1: Deeper Learning Activities:

Sabotage and theft

1. **Describe** what is meant by the term 'sabotage' in the context of a computer network. **(PASS)**

Type your answer here.

2. **Describe** what is meant by the term 'theft' in the context of a computer network. **(PASS)**

Type your answer here.

3. **Research an** organisation that has experienced employee sabotage or theft.

   Describe:

   - Which employee was responsible
   - Why the employee carried out the attack
   - The impacts the attack had on the organisation **(MERIT)**

Type your answer here.

4. **Research** strategies that organisations can use to reduce the risks caused by disgruntled employees **(MERIT)** and **evaluate** how effective these strategies are. **(DISTINCTION)**

Type your answer here.

Unauthorised Access

5. **Describe** what is meant by the term ‘unauthorised access’ in the context of a computer network. **(PASS)**

Type your answer here.

6. **State** example actions a user may carry out once they have gained unauthorised access to a network **(PASS)** and **explain** the impacts of these. **(MERIT)**

Type your answer here.

7. **Research** strategies that organisations can use to reduce the risk of unauthorised access **(MERIT)** and **evaluate** how effective these strategies are. **(DISTINCTION)**

Type your answer here.

Safe working practices

8. **Describe** what is meant by the term ‘safe working practice’ in the context of a computer network. **(PASS)**

Type your answer here.

9. **Research three** different safe working practices which can be used to solve the following statements **(MERIT)** and **evaluate** the effectiveness of each of them. **(DISTINCTION)**

i. Securely checking visitors are genuine

Type your answer here.

ii. Ensuring users visit trustworthy website

Type your answer here.

Accidental loss and disclosure of data

10. **Describe** what is meant by the term ‘accident loss of data’ in the context of a computer network. **(PASS)**

Type your answer here.

11. **Describe** what is meant by the term ‘accident disclosure of data.’ **(PASS)**

Type your answer here.

12. **Explain** why poor staff training and monitoring can contribute to accidental loss or disclosure of data. **(MERIT)**

Type your answer here.

Topic 1: Progress Check

Topic	Confident (Tick)	Need to revisit (Tick)
I know the causes of sabotage and theft and methods that can be used to reduce them.		
I know the causes of unauthorised access and methods that can be used to reduce them.		
I know the causes of unsafe working practices and methods that can be used to reduce them.		
I know the causes of accidental loss, disclosure of data and methods that can be used to reduce them.		

Topic 1: Grade Yourself

Grade Description	The statement that best describes my progress is…
Pass - Describe what is meant by different internal threats.	
Merit - Describe the different methods that organisations could use to reduce the risks caused by internal threats.	
Distinction- Evaluate how effectively these security methods reduce the risks caused by internal threats.	
My strengths….. Type your answer here.	
My areas for development… Type your answer here.	

Topic 2

External Threats

Topic 2: External Threats

Topic 2: Topic Objectives:

- **Pass - Describe** what is meant by the terms malicious software, hacking, sabotage and social engineering.
- **Merit – Explain** the different methods/types of malicious software, hacking, sabotage and social engineering.
- **Distinction- Assess** how malicious software, hacking, sabotage and social engineering could impact the security of a network using detailed relevant examples.

Topic2: Specification Coverage:

- Understand how external threats function, including:
  - malicious software (malware), including spyware, adware, ransomware; viruses, including worms, rootkits and trojans
  - hacking, including commercial, government, individuals
  - sabotage, including commercial, government, terrorism, individuals
  - social-engineering techniques used to obtain secure information by deception.

Topic 2: Introductory Task:

Describe what high profile cyber security incidents you have come across in the news. **(PASS)**

Type your answer here.

Topic 2: Deeper Learning Activities:

Malware

1. **Describe** what is meant by the term 'malware.' **(PASS)**

Type your answer here.

2. **Explain** the different types of malware **(PASS)** and **analyse** how they can impact the security of a system. **(MERIT)**

Type	Explanation	Impact on security
Spyware	Type your answer here.	Type your answer here.
Adware	Type your answer here.	Type your answer here.
Ransomware	Type your answer here.	Type your answer here.

Viruses

3. **Describe** what is meant by the term 'virus.' **(PASS)**

Type your answer here.

4. **Explain** the different types of virus **(PASS)** and **analyse** how they can impact the security of a system. **(MERIT)**

Type	Explanation	Impact on security
Worms	Type your answer here.	Type your answer here.
Rootkits	Type your answer here.	Type your answer here.
Trojans	Type your answer here.	Type your answer here.

Hacking

5. **Describe** what is meant by the term 'hacking' and how this is different to 'unauthorised access.' **(PASS)**

Type your answer here.

6. **Explain** the different types of hacking. **(MERIT)**

Type	Description
Individual	Type your answer here.
Commercial	Type your answer here.
Government	Type your answer here.

7. **Research** an organisation that was attacked by a hacker and **assess** the impacts caused to the organisation. **(DISTINCTION)**

Type your answer here.

Sabotage

8. **Describe** what is meant by the term 'sabotage.' **(PASS)**

Type your answer here.

9. **Explain** the different types of sabotage. **(MERIT)**

Type	Description
Commercial	Type your answer here.
Government	Type your answer here.
Terrorism	Type your answer here.
Individual	Type your answer here.

10. **Research** an organisation that was attacked by sabotage **externally** and **assess** the impacts caused to the organisation. **(DISTINCTION)**

Type your answer here.

Social-engineering

11. **Describe** what is meant by the term ‘social-engineering.’ **(PASS)**

Type your answer here.

12. **Explain** the different types of hacking. **(MERIT)**

Type	Description
Telephone	Type your answer here.
Phishing	Type your answer here.
Shoulder Surfing	Type your answer here.

13. **Research** an individual that was the target of social engineering and **assess** the impacts caused to the individual. **(DISTINCTION)**

Type your answer here.

Topic 2: Progress Check

Topic	Confident (Tick)	Need to revisit (Tick)
I know the meaning of malware, the different types and how they can threaten the security of a computer system.		
I know the meaning of a virus, the different types and how they can threaten the security of a computer system.		
I know the meaning of hacking, the different types and how they can threaten the security of a computer system.		
I know the meaning of social-engineering, the different types and how they can threaten the security of a computer system.		

Topic 2: Grade Yourself

Grade Description	The statement that best describes my progress is…
Pass - Describe what is meant by the terms malicious software, hacking, sabotage and social engineering.	
Merit – Explain the different methods/types of malicious software, hacking, sabotage and social engineering.	
Distinction- Assess how malicious software, hacking, sabotage and social engineering could impact the security of a network using detailed relevant examples.	
My strengths….. Type your answer here.	
My areas for development… Type your answer here.	

Topic 3

Impacts of Credible Threats

Topic 3: Impacts of credible threats

Topic 3: Topic Objectives:

- **Pass – Describe** what is meant by the following impacts: operation loss, financial loss, reputation loss and intellectual property loss.
- **Merit – Explain** why these can impact an organisation using detailed examples.
- **Distinction- Discuss** how the level of impact is determined by the value of loss and why this value is not always a monetary one.

Topic 3: Specification Coverage:

- Understand that the impact of a credible threat is likely to result in some form of loss, such as:
  - operational loss, including manufacturing output, service availability and service data
  - financial loss, including organisational, compensation and legal liability
  - reputation loss, including lack of service and employee or customer information
  - intellectual property loss, including new product design or trade secret.
- Understand that the impact level of a successful attack on an organisation is determined by the value of the loss, and that the value may not always be a monetary one.
- Know that cyber security threats vary over time and cyber security organisations provide regular updates on the current and changing threat landscape.

Topic 3: Introductory Task:

In May 2017, the NHS suffered a cyber attack where a group of hackers spread ransomware called 'WannaCry.'

Research the short-term and long-term impacts this attack had.

Apart from impacting on patient care, what other impacts did this attack have? **(PASS)**

Type your answer here.

Topic 3: Deeper Learning Activities:

Operation Loss

1. **Describe** what is meant by the term 'operation loss.' **(PASS)**

Type your answer here.

2. **Explain** what is meant by the following types of operation loss **(MERIT)** and **analyse** how these can impact an organisation. **(DISTINCTION)**

Type	Explanation	Impact on Organisation
Manufacturing output	Type your answer here.	Type your answer here.
Service availability	Type your answer here.	Type your answer here.
Service data	Type your answer here.	Type your answer here.

Financial Loss

3. **Describe** what is meant by the term 'financial loss.' **(PASS)**

Type your answer here.

4. **Explain** what is meant by the following types of financial loss **(MERIT)** and **analyse** how these can impact an organisation. **(DISTINCTION)**

Type	Explanation	Impact on Organisation
Organisational	Type your answer here.	Type your answer here.
Compensation	Type your answer here.	Type your answer here.
Legal liability	Type your answer here.	Type your answer here.

Reputational Loss

5. **Describe** what is meant by the term 'reputational loss.' **(PASS)**

Type your answer here.

6. **Explain** what is meant by the following types of reputational loss **(MERIT)** and **analyse** how these can impact an organisation. **(DISTINCTION)**

Type	Explanation	Impact on Organisation
Lack of service	Type your answer here.	Type your answer here.
Loss of employee / customer information	Type your answer here.	Type your answer here.

Intellectual Property Loss

7. **Describe** what is meant by the term 'intellectual property loss.' **(PASS)**

Type your answer here.

8. **Explain** what is meant by the following types of intellectual property loss **(MERIT)** and **analyse** how these can impact an organisation. **(DISTINCTION)**

Type	Explanation	Impact on Organisation
Loss of new product designs	Type your answer here.	Type your answer here.
Loss of trade secrets	Type your answer here.	Type your answer here.

Topic 3: Progress Check

Topic	Confident (Tick)	Need to revisit (Tick)
I know what operation loss means and how this impacts an organisation.		
I know what financial loss means and how this impacts an organisation.		
I know what reputation loss means and how this impacts an organisation.		
I know what intellectual property loss means and how this impacts an organisation.		

Topic 3: Grade Yourself

Grade Description	The statement that best describes my progress is…
Pass – Describe what is meant by the following impacts: operation loss, financial loss, reputation loss and intellectual property loss.	
Merit – Explain why these can impact an organisation using detailed examples.	
Distinction- Discuss how the level of impact is determined by the value of loss and why this value is not always a monetary one.	
My strengths….. Type your answer here.	
My areas for development… Type your answer here.	

Topic 4

System Vulnerabilities

Topic 4: System Vulnerabilities

Topic 4: Topic Objectives:

- **Pass – Describe** a range of systems that can become vulnerable to attacks including: networks, software, operating systems, mobile devices, physical devices and cloud computing.
- **Merit – Describe** the vulnerabilities and threats that these systems may be exposed too.
- **Distinction- Discuss** why different types of computer systems are exposed to different threats and vulnerabilities.

Topic 4: Specification Coverage:

A2 System vulnerabilities

- Understand that different types of computer and/or system are exposed to different threats and that they contain different vulnerabilities. Possible vulnerabilities include:
  - network, including firewall ports and external storage devices
  - organisational, including file permissions or privileges, password policy
  - software, including from an untrustworthy source, downloaded software, illegal copies, SQL injection and new zero-day exploits
  - operating system, including unsupported versions, updates not installed
  - mobile devices reliant on Original Equipment Manufacturers (OEMs) to update system software
  - physical, including theft of equipment, Universal Serial Bus (USB) storage devices with sensitive data, collection of passwords and other information by social-engineering methods
  - process of how people use the system, including leaks and sharing security details
  - security implications of cloud computing and of the Internet of Things (IoT) devices.
- Understand where to find up-to-date sources of information on specific known hardware and software vulnerabilities.
- Attack vectors, including: Wi-Fi, Bluetooth®, internet connection, internal network access.

Topic 4: Introductory Task:

Think about all of the technological devices you have in your home. For each device state:

1. The name of the device
2. How old the device is
3. If never versions of that same device are available
4. How often the software gets updated

Do you know the answers to all of these questions? What do you think the risks may be of not knowing these answers? **(PASS)**

Type your answer here.

Topic 4: Deeper Learning Activities:

Network Vulnerabilities

1. **Describe** what is meant by the term 'network vulnerability.' **(PASS)**

Type your answer here.

2. **Explain** the different network vulnerabilities **(MERIT)** and **discuss** why these vulnerabilities are specific to computer networks. **(DISTINCTION)**

Type your answer here.

Organisational Vulnerabilities

3. **Describe** what is meant by the term 'organisational vulnerability.' **(PASS)**

Type your answer here.

4. **Explain** the different vulnerabilities **(MERIT)** and **discuss** why these vulnerabilities are specific to organisations. **(DISTINCTION)**

Type your answer here.

Software Vulnerabilities

5. **Describe** what is meant by the term 'software vulnerability.' **(PASS)**

Type your answer here.

6. **Explain** the different vulnerabilities **(MERIT)** and **discuss** why these vulnerabilities are specific to software. **(DISTINCTION)**

Type your answer here.

Operating System Vulnerabilities

7. **Describe** what is meant by the term 'operating system vulnerability.' **(PASS)**

Type your answer here.

8. **Explain** the different vulnerabilities **(MERIT)** and **discuss** why these vulnerabilities are specific to operating systems. **(DISTINCTION)**

Type your answer here.

Mobile Device Vulnerabilities

9. **Describe** what is meant by the term 'mobile device vulnerability.' **(PASS)**

Type your answer here.

10. **Explain** the different vulnerabilities **(MERIT)** and **discuss** why these vulnerabilities are specific to mobile devices. **(DISTINCTION)**

Type your answer here.

Physical Device Vulnerabilities

11. **Describe** what is meant by the term 'physical device vulnerability.' **(PASS)**

Type your answer here.

12. **Explain** the different vulnerabilities **(MERIT)** and **discuss** why these vulnerabilities are specific to physical devices. **(DISTINCTION)**

Type your answer here.

Cloud Computing Vulnerabilities

13. **Describe** what is meant by the term 'cloud computing vulnerability.' **(PASS)**

Type your answer here.

14. **Explain** the different vulnerabilities **(MERIT)** and **discuss** why these vulnerabilities are specific to cloud computing. **(DISTINCTION)**

Type your answer here.

Attack Vector

15. **Describe** what is meant by the term 'Attack Vector.' **(PASS)**

Type your answer here.

16. **Explain** the different attack vectors **(MERIT)** and **discuss** methods that can be used to reduce their risks. **(DISTINCTION)**

Type your answer here.

Keeping up-to-date

17. **Research** different sources that you can use to keep up-to-date on specific known hardware and software vulnerabilities. **(PASS)**

Type your answer here.

Topic 4: Progress Check

Topic	Confident (Tick)	Need to revisit (Tick)
I know why a **network** may become vulnerable and how to reduce these vulnerabilities.		
I know why an **organisation** may become vulnerable and how to reduce these vulnerabilities.		
I know why **software** may become vulnerable and how to reduce these vulnerabilities.		
I know why **operating systems** may and how to reduce these vulnerabilities.		
I know why **mobile/portable devices** may become vulnerable and how to reduce these vulnerabilities.		
I know why **cloud computing** may become vulnerable and how to reduce these vulnerabilities.		
I know what an **attack vector** is and how to reduce these vulnerabilities.		
I know where to **find information** on the latest hardware and software threats.		

Topic 4: Grade Yourself

Grade Description	The statement that best describes my progress is…
Pass – Describe a range of systems that can become vulnerable to attacks including: networks, software, operating systems, mobile devices, physical devices and cloud computing.	
Merit – Describe the vulnerabilities and threats that these systems may be exposed too.	
Distinction- Discuss why different types of computer systems are exposed to different threats and vulnerabilities.	
My strengths….. Type your answer here.	
My areas for development… Type your answer here.	

Topic 5

Legal Responsibilities

Topic 5: Legal Responsibilities

Topic 5: Topic Objectives:

- **Pass - Describe** different legislation that organisations must follow when using digital systems.
- **Merit - Explain** the legal requirements organisations must follow under each legislation.
- **Distinction- Evaluate** the impact that each legislation has on data security, illegal practices, monitoring staff, fraudulent purposes and working practices.

Topic 5: Specification Coverage:

A3 Legal responsibilities

Understand how the current and relevant European Union (EU) General Data Protection Regulation (GDPR) and United Kingdom legislation or other international equivalents apply to different systems, including:

- Data Protection Act 1998 and amendments, requirements for organisations to keep data secure
- Computer Misuse Act 1990 and amendments, its definitions of illegal practices and applications
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 and amendments, requirements to allow companies to monitor an employee's communication and internet use while at work
- Fraud Act 2006 and amendments, requirements to deal with services using IT-based methods to steal information for fraudulent purposes
- Health and Safety at Work etc. Act 1974 – duties of employers, employees, the Health and Safety Executive (HSE) and others, general prohibitions.

Topic 5: Introductory Task:

Consider the following questions: **(PASS)**

1. What personal data does your centre store about you?
2. How would you expect your centre to use your personal data?
3. Is your centre allowed to monitor what you do on the computer network?

Type your answer here.

Topic 5: Deeper Learning Activities:

Data Protection Act 1998

1. **Describe** the purpose of this law. **(PASS)**

Type your answer here.

2. **Explain** the legal requirements for organisations to keep data safe. **(PASS)**

Type your answer here.

3. **Research** and **describe** different methods that organisations can use in order to meet the requirements of this law. **(MERIT)**

Type your answer here.

4. **Research** and **evaluate** the impact this law has had on improving data security. **(DISTINCTION)**

Type your answer here.

Computer Misuse Act 1990

5. **Describe** the purpose of this law. **(PASS)**

Type your answer here.

6. **Explain** the legal definitions of 'illegal practices' under this law. **(PASS)**

Type your answer here.

7. **Research** and **describe** different methods that organisations can use in order to meet the requirements of this law. **(MERIT)**

Type your answer here.

8. **Research** and **evaluate** the impact this law has had on reducing illegal practices. **(DISTINCTION)**

Type your answer here.

Telecommunications Regulations 2000

9. **Describe** the purpose of this law. **(PASS)**

Type your answer here.

10. **Research** and **discuss** why this law was setup and the impacts on users. **(DISTINCTION)**

Type your answer here.

Fraud Act 2006

11. **Describe** the purpose of this law. **(PASS)**

Type your answer here.

12. **Describe** the legal definitions of 'fraud'. **(PASS)**

Type your answer here.

13. **Research and describe** different ways that IT systems can be used to carryout fraud. **(MERIT)**

Type your answer here.

14. **Research** and **evaluate** the impact this law has had on reducing fraud. **(DISTINCTION)**

Type your answer here.

Health & Safety at Work Act 1974

15. **Describe** the purpose of this law. **(PASS)**

Type your answer here.

16. **Research and describe** different methods that the following groups can use in order to meet the requirements of this law. **(MERIT)**

Employers
Type your answer here.

Employees
Type your answer here.

Health & Safety Executive
Type your answer here.

Topic 5: Progress Check

Topic	Confident (Tick)	Need to revisit (Tick)
I know the requirements under the Data Protection Act 1998 to keep data safe.		
I know the definitions of illegal practices under the Computer Misuse Act 1990.		
I know the requirements to allow companies to monitor employees under the Telecommunications Regulations 2000.		
I know the requirements under the Fraud Act 2006 to deal with fraud.		
I know the duties of employers, employees and the Health and Safety Executives under the Health & Safety at Work Act 1974.		

Topic 5: Grade Yourself

Grade Description	The statement that best describes my progress is…
Pass - Describe different legislation that organisations must follow when using digital systems.	
Merit - Explain the legal requirements organisations must follow under each legislation.	
Distinction- Evaluate the impact that each legislation has on data security, illegal practices, monitoring staff, fraudulent purposes and working practices.	
My strengths….. Type your answer here.	
My areas for development… Type your answer here.	

Topic 6

Physical Security

Topic 6: Physical Security

Topic 6: Topic Objectives:

- **Pass – Describe** different physical security measures that can be used to secure IT systems.
- **Merit – Explain** why different physical security measures would be used.
- **Distinction- Evaluate** how effectively physical security methods keep data safe.

Topic 6: Specification Coverage:

A4 Physical security measures

Understand the use and effectiveness of physical security measures, including:

- site security locks, card entry, biometrics, closed-circuit television (CCTV), security staff, alarms, protected cabling and cabinets
- data storage, data protection and backup procedures, including planned automated backup, on- and off-site data storage and cloud storage.

Topic 6: Introductory Task:

Look around the classroom that you are currently in.

Imagine there is an attacker outside the door with intent to steal the IT hardware.

1. What can you physically setup to stop the attacker from entering the room?
2. What could you setup that might deter the attacker from entering the room? **(PASS)**

Type your answer here.

Topic 6: Deeper Learning Activities:

Physical Security:

1. **Describe** what is meant by the term 'physical security. ' **(PASS)**

Type your answer here.

2. **Describe** what is meant by the following types of physical security. **(PASS)**

Type	Description
Locks	Type your answer here.
Card entry systems	Type your answer here.
Biometrics	Type your answer here.
CCTV	Type your answer here.
Security guards/staff	Type your answer here.
Alarms	Type your answer here.
Protected cabling	Type your answer here.
Protected cabinets	Type your answer here.

3. **Research** and **explain** the different methods of each type of physical security **(MERIT)** and **evaluate** how effectively locks improve the security of a network.

Type	Types	Explanation	Effectiveness
Locks	Type your answer here.	Type your answer here.	Type your answer here.
Card entry systems	Type your answer here.	Type your answer here.	Type your answer here.
Biometrics	Type your answer here.	Type your answer here.	Type your answer here.
CCTV	Type your answer here.	Type your answer here.	Type your answer here.
Security guards/staff	Type your answer here.	Type your answer here.	Type your answer here.
Alarms	Type your answer here.	Type your answer here.	Type your answer here.
Protected cabling	Type your answer here.	Type your answer here.	Type your answer here.
Protected cabinets	Type your answer here.	Type your answer here.	Type your answer here.

Data Storage:

1. **Describe** what is meant by the term 'backup.' **(PASS)**

Type your answer here.

2. **Describe** what is meant by each type of backup **(PASS)** and **explain** why each type of backup would be used. **(MERIT)**

Type	Description	Why would this be used
Full	Type your answer here.	Type your answer here.
Differential	Type your answer here.	Type your answer here.
Incremental	Type your answer here.	Type your answer here.

3. **Explain** the difference between 'on-site' backups and 'off-site' backups and why they would be used. **(PASS)**

Type your answer here.

4. **Research** and **evaluate** how effectively backups improve the security of a network. **(DISTINCTION)**

Type your answer here.

Topic 6: Progress Check

Topic	Confident (Tick)	Need to revisit (Tick)
I know the different uses and effectiveness of locks/card entry systems.		
I know the different uses and effectiveness of biometrics.		
I know the different uses and effectiveness of CCTV/alarm systems.		
I know the different uses and effectiveness of security staff/guards.		
I know the different uses and effectiveness of protected cabling/cabinets.		
I know the different types of backups, why they are used.		
I know the difference between on-site and off-site backups and why they are used.		

Topic 6: Grade Yourself

Grade Description	The statement that best describes my progress is…
Pass – Describe different physical security measures that can be used to secure IT systems.	
Merit – Explain why different physical security measures would be used.	
Distinction- Evaluate how effectively physical security methods keep data safe.	
My strengths….. Type your answer here.	
My areas for development… Type your answer here.	

Topic 7

Antivirus and Firewalls

Topic 7: Antivirus and Firewalls

Topic 7: Topic Objectives:

- **Pass - Describe** how antivirus software and firewalls can be used to secure IT systems.
- **Merit - Explain** the techniques used by antivirus software and firewalls to identify threats.
- **Distinction- Evaluate** how effectively antivirus software and firewalls keep data safe.

Topic 7: Specification Coverage:

A5 Software and hardware security measures

- Understand the use and effectiveness of software and hardware security measures, including:
  - antivirus software and detection techniques, including virus signatures, heuristics techniques used to identify potentially suspicious file content, techniques for dealing with identified threats
  - software and hardware firewalls and the filtering techniques they use, including:
    - packet filtering and inspection
    - application layer awareness
    - inbound and outbound rules
    - network address

Topic 7: Introductory Task:

Have you ever heard of antivirus and firewall software?

Do they have different roles or do they do the same thing? **(PASS)**

Type your answer here.

Topic 7: Deeper Learning Activities:

Antivirus Software

1. **Describe** what is meant by the term 'antivirus' software. **(PASS)**

Type your answer here.

2. **Describe** what is meant by the term 'virus signature' **(PASS)** and **explain** why antivirus software makes use of it. **(MERIT)**

Type your answer here.

3. **Describe** what is meant by the term 'heuristics' **(PASS)** and **explain** why antivirus software makes use of it. **(MERIT)**

Type your answer here.

4. **Research** and **evaluate** how effectively antivirus software improves the security of a network. **(DISTINCTION)**

Type your answer here.

Firewalls

5. **Describe** what is meant by the term 'firewall' software. **(PASS)**

Type your answer here.

6. **Describe** what is meant by the term 'packet filtering' **(PASS)** and **explain** why firewall software makes use of it. **(MERIT)**

Type your answer here.

7. **Describe** what is meant by the term 'inbound' and 'outbound' traffic' **(PASS)** and **explain** different rules that can be setup for each. **(MERIT)**

Type your answer here.

8. **Research** and **evaluate** how effectively firewall software improves the security of a network. **(DISTINCTION)**

Type your answer here.

Topic 7: Progress Check

Topic	Confident (Tick)	Need to revisit (Tick)
I know the use of and effectiveness of antivirus software.		
I know why antivirus software makes use of signatures and heuristics.		
I know the use of and effectiveness of firewalls.		
I know different filtering techniques used by firewall software.		

Topic 7: Grade Yourself

Grade Description	The statement that best describes my progress is…
Pass - Describe how antivirus software and firewalls can be used to secure IT systems.	
Merit - Explain the techniques used by antivirus software and firewalls to identify threats.	
Distinction- Evaluate how effectively antivirus software and firewalls keep data safe.	
My strengths….. Type your answer here.	
My areas for development… Type your answer here.	

Topic 8

User Authentication & Access Controls

Topic 8: User Authentication & Access Controls

Topic 8: Topic Objectives:

- **Pass - Describe** how user authentication and access controls can be used to secure IT systems.
- **Merit - Explain** why the different methods of authentication and access controls would be used.
- **Distinction- Evaluate** how effectively different user authentication methods and access controls secure IT systems.

Topic 8: Specification Coverage:

- user authentication:
  - user login procedures
  - strong password
  - text and graphical password
  - biometric authentication
  - two-step verification
  - security tokens, including USB-based and near field keys
  - knowledge-based authentication, including question and response pairs
  - Kerberos network authentication for Windows® and Linux®-based operating systems
  - certificate-based authentication
- access controls and the methods to restrict users' access to resources, including applications, folders, files and physical resources
- trusted computing.

Topic 8: Introductory Task:

Have you ever heard of the term user authentication?

How do you authenticate yourself in order to gain access to:

- The network at your centre
- Your phone

What other devices do you have where you have to authenticate yourself? **(PASS)**

Type your answer here.

Topic 8: Deeper Learning Activities:

User Authentication

1. **Describe** what is meant by the term 'user authentication.' **(PASS)**

Type your answer here.

2. **Describe** what is meant by the following types of user authentication. **(PASS)**

Type	Description
User login procedures	Type your answer here.
Strong password	Type your answer here.
Text and graphical password	Type your answer here.
Biometric authentication	Type your answer here.
Two-step verification	Type your answer here.
Security tokens	Type your answer here.
Knowledge-based authentication	Type your answer here.
Kerberos network authentication	Type your answer here.
Certificate-based authentication	Type your answer here.

3. **Research** and **explain** why each type of user authentication would be used **(MERIT)** and **evaluate** how effectively they secure an IT system. **(DISTINCTION)**

Type	Why is this used?	Effectiveness
User login procedures	Type your answer here.	Type your answer here.
Strong password	Type your answer here.	Type your answer here.
Text and graphical password	Type your answer here.	Type your answer here.
Biometric authentication	Type your answer here.	Type your answer here.
Two-step verification	Type your answer here.	Type your answer here.
Security tokens	Type your answer here.	Type your answer here.
Knowledge-based authentication	Type your answer here.	Type your answer here.
Kerberos network authentication	Type your answer here.	Type your answer here.
Certificate-based authentication	Type your answer here.	Type your answer here.

Access Controls

4. **Describe** what is meant by the term 'access control.' **(PASS)**

Type your answer here.

5. **Explain** why an organisation may want to restrict access to the following areas. **(MERIT)**

Type	Description
Applications	Type your answer here.
Folders	Type your answer here.
Files	Type your answer here.
Physical resources	Type your answer here.

6. **Describe** what is meant by the following access controls. **(PASS)** and **evaluate** how effectively they keep data secure. **(DISTINCTION)**

Type	Description	Effectiveness

Read	Type your answer here.	Type your answer here.
Write	Type your answer here.	Type your answer here.
Create	Type your answer here.	Type your answer here.
Edit	Type your answer here.	Type your answer here.
Delete	Type your answer here.	Type your answer here.

Trusted Computing

7. **Describe** what is meant by the term 'Trusted Computing.' **(PASS)**

Type your answer here.

Topic 8: Progress Check

Topic	Confident (Tick)	Need to revisit (Tick)
I know what is meant by the term user authentication.		
I know the different types of user authentication and how effectively they secure data.		
I know what is meant by the term access control.		
I know different types of access control.		
I know different access controls that can be used and how effectively they secure IT systems.		

Topic 8: Grade Yourself

Grade Description	The statement that best describes my progress is…
Pass - Describe how user authentication and access controls can be used to secure IT systems.	
Merit - Explain why the different methods of authentication and access controls would be used.	
Distinction- Evaluate how effectively different user authentication methods and access controls secure IT systems.	
My strengths….. Type your answer here.	
My areas for development… Type your answer here.	

Topic 9

Encryption

Topic 9: Encryption

Topic 9: Topic Objectives:

- **Pass - Describe** different types of encryption and how they secure IT systems.
- **Merit - Explain** why the different methods of encryption would be used.
- **Distinction- Evaluate** how effectively different encryption methods keep data safe.

Topic 9: Specification Coverage:

- Understand the purpose and uses of encryption, including:
  - safe password storage
  - digital rights management (DRM)
  - file, folder, disc encryption
  - communications encryption:
    - built into devices, including smartphones and tablets
    - The Onion Router (Tor)
    - virtual private networks (VPNs)
    - digital certificates and certificate authorities
    - Hypertext Transfer Protocol Secure (HTTPS)
    - public/private keys.

Topic 9: Introductory Task:

Have you ever heard of the term 'encryption?'

What transactions have you carried out online that used encryption? How do you know when encryption is being used? Would you still carryout online transactions without encryption? ' **(PASS)**

Type your answer here.

Topic 9: Deeper Learning Activities:

Encryption

1. **Describe** what is meant by the term 'encryption.' **(PASS)**

Type your answer here.

2. **Research** and **describe** what is meant by the following types of communications encryption **(PASS)** and **evaluate** how effectively they keep secure data. **(DISTINCTION)**

Type	Description	Effectiveness
Built into devices	Type your answer here.	Type your answer here.
The Onion Router (Tor)	Type your answer here.	Type your answer here.
Virtual private networks (VPNs)	Type your answer here.	Type your answer here.
Digital certificates and certificate authorities	Type your answer here.	Type your answer here.
Hypertext Transfer Protocol Secure (HTTPS)	Type your answer here.	Type your answer here.
Public/private keys	Type your answer here.	Type your answer here.

3. **Research** and **explain** why the following uses of encryption would be used by organisations. **(MERIT)**

Type	Explanation
Safe password storage	Type your answer here.
Digital Rights Managements (DRM)	Type your answer here.
File, folder, disc encryption	Type your answer here.

Topic 9: Progress Check

Topic	Confident (Tick)	Need to revisit (Tick)
I know what is meant by the term encryption.		
I know the different uses of encryption.		
I know the different methods of encryption.		
I know how effectively each encryption method keeps data safe.		

Topic 9: Grade Yourself

Grade Description	The statement that best describes my progress is…
Pass - Describe different types of encryption and how they secure IT systems.	
Merit - Explain why the different methods of encryption would be used.	
Distinction- Evaluate how effectively different encryption methods keep data safe.	
My strengths….. Type your answer here.	
My areas for development… Type your answer here.	

Topic 10

Protecting Wireless Networks

Topic 10: Protecting wireless networks

Topic 10: Topic Objectives:

- **Pass – Describe** the different precautions that can be taken to secure a wireless network from authorised access.
- **Merit – Explain** the benefits and drawbacks of these precautions.
- **Distinction - Discuss** why security should be considered when designing a network.

Topic 10: Specification Coverage:

- Precautions that can be taken to protect a wireless local area network (WLAN) from unauthorised access, including:
  - MAC address filtering and hiding the service set identifier (SSID)
  - wireless encryption – Wired Equivalent Privacy (WEP), Wi-Fi Protected Access 2 (WPA2) and Wi-Fi Protected Setup (WPS), mitigating known wireless vulnerabilities
  - consideration of security issues during network and system design to ensure security is built-in from the development stage.

Topic 10: Introductory Task:

Do you allow your phone to automatically connect to different wireless networks, including open wireless networks?

If so, which ones? Have you ever wondered if the wireless networks are secure? **(PASS)**

Type your answer here.

Topic 10 Deeper Learning Activities:

Securing Wireless Networks

1. **Describe** why wireless networks are vulnerable to unauthorised access. **(PASS)**

Type your answer here.

2. **Research** and d**escribe** the different precautions that can be used to secure a wireless network **(PASS)** and **explain** the benefits and drawbacks of each. **(MERIT)**

Type	Description	Benefits	Drawbacks
MAC address filtering	Type your answer here.	Type your answer here.	Type your answer here.
Wired Equivalent Privacy (WEP)	Type your answer here.	Type your answer here.	Type your answer here.
Wi-Fi Protected Access 2 (WPA2)	Type your answer here.	Type your answer here.	Type your answer here.
Wi-Fi Protected Setup (WPS)	Type your answer here.	Type your answer here.	Type your answer here.

3. **Discuss** why the security of a network should be considered when a network is being designed rather than waiting until the network is actually setup. **(DISTINCTION)**

Type your answer here.

Topic 10: Progress Check

Topic	Confident (Tick)	Need to revisit (Tick)
I know why wireless networks are more vulnerable to attack.		
I know what is meant by the term MAC address filtering and SSID and how effectively they secure a wireless network.		
I know different methods of wireless encryption and how effectively they secure a wireless network.		
I know what should be considered when designing a network to reduce the risks of attacks.		

Topic 10: Grade Yourself

Grade Description	The statement that best describes my progress is…
Pass – Describe the different precautions that can be taken to secure a wireless network from authorised access.	
Merit – Explain the benefits and drawbacks of these precautions.	
Distinction - Discuss why security should be considered when designing a network.	
My strengths….. Type your answer here.	
My areas for development… Type your answer here.	

End of Learning Aim A Review

Topic	Checklist Item	Confidence		
		Low	Medium	High
Topic 1 Internal Threats	I know the causes of sabotage and theft and methods that can be used to reduce them.			
	I know the causes of unauthorised access and methods that can be used to reduce them.			
	I know the causes of unsafe working practices and methods that can be used to reduce them.			
	I know the causes of accidental loss, disclosure of data and methods that can be used to reduce them.			
Topic 2 External Threats	I know the meaning of malware, the different types and how they can threaten the security of a computer system.			
	I know the meaning of a virus, the different types and how they can threaten the security of a computer system.			
	I know the meaning of hacking, the different types and how they can threaten the security of a computer system.			
	I know the meaning of social-engineering, the different types and how they can threaten the security of a computer system.			
Topic 3 Impacts of Credible Threats	I know what operation loss means and how this impacts an organisation.			
	I know what financial loss means and how this impacts an organisation.			
	I know what reputation loss means and how this impacts an organisation.			
	I know what intellectual property loss means and how this impacts an organisation.			
Topic 4 System Vulnerabilities	I know why a network may become vulnerable and how to reduce these vulnerabilities.			
	I know why an organisation may become vulnerable and how to reduce these vulnerabilities.			
	I know why software may become vulnerable and how to reduce these vulnerabilities.			
	I know why operating systems may and how to reduce these vulnerabilities.			
	I know why mobile/portable devices may become vulnerable and how to reduce these vulnerabilities.			
	I know why cloud computing may become vulnerable and how to reduce these vulnerabilities.			
	I know what an attack vector is and how to reduce these vulnerabilities.			
	I know where to find information on the latest hardware			

	and software threats.			

Continued on the next page…..

End of Learning Aim A Review Continued…

Topic	Checklist Item	Confidence		
		Low	Medium	High
Topic 5 Legal Responsibilities	I know the requirements under the Data Protection Act 1998 to keep data safe.			
	I know the definitions of illegal practices under the Computer Misuse Act 1990.			
	I know the requirements to allow companies to monitor employees under the Telecommunications Regulations 2000.			
	I know the requirements under the Fraud Act 2006 to deal with fraud.			
	I know the duties of employers and employees under the Health & Safety at Work Act 1974.			
Topic 6 Physical Security	I know the different uses and effectiveness of locks/card entry systems.			
	I know the different uses and effectiveness of biometrics.			
	I know the different uses and effectiveness of CCTV/alarm systems.			
	I know the different uses and effectiveness of security staff/guards.			
	I know the different types of backups, why they are used.			
	I know the difference between on-site and off-site backups and why they are used.			
Topic 7 Antivirus and Firewalls	I know the use of and effectiveness of antivirus software.			
	I know why antivirus software makes use of signatures and heuristics.			
	I know the use of and effectiveness of firewalls.			
	I know different filtering techniques used by firewall software.			
Topic 8 Authentication & Access Controls	I know what is meant by the term user authentication.			
	I know the different types of user authentication and how effectively they secure data.			
	I know what is meant by the term access control.			
	I know different types of access control.			
	I know different access controls that can be used and how effectively they secure IT systems.			
Topic 9 Encryption	I know what is meant by the term encryption.			
	I know the different uses of encryption.			
	I know the different methods of encryption.			
	I know how effectively encryption methods keep data safe.			
Topic 10	I know why wireless networks are more vulnerable to			

Protecting Wireless Networks	attacks.			
	I know what is meant by the term MAC address filtering and SSID and how effectively they secure a wireless network.			
	I know different methods of wireless encryption and how effectively they secure a wireless network.			
	I know what should be considered when designing a network to reduce the risks of attacks.			