Unit title	Cyber Security and Incident Management
Guided learning hours	120
Number of lessons	23 + three weeks (×1.5 hours) for planned assessment set task windows
Duration of lessons	5 hours (2 × 2.5 hours)
Links to other units	
● Unit 1: Information Technology Systems – Strategy, Management and Infrastructure ● Unit 2: Creating Systems to Manage Information ● Unit 3: Using Social Media in Business ● Unit 4: Programming ● Unit 9: IT Project Management ● Unit 13: Software Testing ● Unit 15: Cloud Storage and Collaboration Tools ● Unit 20: Business Process Modelling Tools	

Key to learning opportunities			
AW	Assignment writing	**PA**	Preparation for assessment
GS	Guest speaker	**V**	Visit
IS	Independent study	**GW**	Group work

Lesson	Topic	Lesson type	Suggested activities	Classroom resources
Learning aim A: Understand cyber security threats, system vulnerabilities and security protection methods				
1	**A1** Cyber security threats	IS GW	● **Lead in:** Introduce the unit and topic. Assess learners' prior knowledge of security issues and vulnerabilities. ● **Class discussion:** Differentiate internal and external threats.	● Tutor presentations ● Topical case studies ● Example security incidents

			● **Tutor presentation:** Use (topical) case studies to show how internal threats occur, e.g. sabotage, theft, natural disasters (flood, etc.), unauthorised access, system vulnerabilities, unsafe practices, etc. ● **Tutor presentation:** Use (topical) case studies to show how external threats occur, e.g. malicious software (different types), hacking (individual, commercial, government sponsored), sabotage and social engineering. ● **Individual activity:** Learner identify given incidents as either internal or external and suggest an appropriate category for the cause, e.g. unauthorised access, sabotage, etc. ● **Paired activity:** Learners investigate selected case studies which focus on the impact (operational, financial, reputational or intellectual loss) of a threat or vulnerability which has been exploited. ● **Tutor-led discussion:** Learners share their own experiences, e.g. leaked passwords, compromised accounts, Sony emails and account hack, Xbox Live DoS attacks, etc. ● **Small group activity:** Learners suggest how organisations can keep up with the changing landscape of cyber security threats and protect their operations and data. ● **Plenary:** Use directed Q&A to review the topic and prepare learners for the next session. ● **Homework:** Give each learner a scenario (with complexity tailored to support or challenge) based on an organisation network. Ask them to identify the risks to the specific network.	● Research materials (including internet access) ● Access to magazines and journals, e.g. *Cyber Defense Magazine*, *Digital Forensics Magazine*, *SC Magazine*
2	**A2** System vulnerabilities	IS	● **Lead in:** Recap content from the previous session. Assess learners' understanding of the sources of internal and external threats before introducing the topic. ● **Tutor-led practical demonstration:** Use practical demonstrations to illustrate different types of system vulnerability (e.g. a badly-	● Practical examples of system vulnerabilities ● Knowledge quiz

			configured firewall, poorly selected file permissions or user privileges, weak password policy, etc.). ● **Knowledge quiz:** Ask learners to consider given incidents and identify a system vulnerability which could have led to each incident (e.g. an attacker using a person's online account could be due to weak password policy). ● **Tutor-led practical demonstration:** Demonstrate the dangers posed by software applications, perhaps by: ○ downloading an infected application from an untrustworthy source onto a quarantined PC and observing the impact ○ performing an SQL injection attack on an insecure web application. ● **Tutor-led discussion:** Explore topical examples, e.g. botnets utilising weak security on IoT (Internet of Things) household devices to perform DDoS (Distributed Denial of Service) attacks. ● **Individual activity:** Learners research software and hardware vulnerabilities of specific products using appropriate sources, e.g. CVE database. If possible, allow learners to access YouTube, to find relevant videos (e.g. search for: ○ 'Network Threats: Port Scanning' ○ 'Hack All The Things: 20 Devices in 45 Minutes' ○ 'SQL Injection Basics Demonstration' ○ 'Vulnerability Assessment and Mitigating Attacks'. ● **Practical activity:** If possible, (allow learners to) duplicate well-chosen examples of vulnerabilities/threats in a controlled network environment, e.g. cross-site scripting (XSS), session hijacking, SQL injection, etc. ● **Individual activity:** Learners create informational posters about common attack vectors, including WiFi, Bluetooth, etc.	● Resources for practical demonstration of software dangers (e.g. port scanner, quarantined network and unsecured servers, infected application, quarantined host, anti-virus software, web application vulnerable to SQL injection, etc.) ● Research materials (including internet access) ● Access to YouTube ● CVE (Common Vulnerabilities and Exposures) database ● Acunetix Vulnerability Scanner Open Web Application Security Project (OWASP)

			● **Plenary:** Use directed Q&A to review the topic and prepare learners for the next session.	
3	**A3** Legal responsibilities	IS GW	● **Lead in:** Recap content from the previous session. Ask learners about their understanding of system vulnerabilities and give a range of examples of how these can occur. ● **Tutor presentation:** Give an overview of relevant legislation that applies to different systems in learners' home country. Use or share relevant websites and articles to illustrate the key points – for example, you could search for: ○ 'Cybersecurity regulations and their impacts' (UAE) ○ 'MPs pass 2019 Cyber Security Law' (Jordan) ○ 'Stricter enforcement of cybersecurity rules to be expected in the Netherlands' (Netherlands) ○ 'Getting the deal through – Cybersecurity Turkey' (Turkey) ○ 'Cyber Security: Where does Pakistan stand?' (Pakistan) ● **Individual activity:** Learners summarise relevant legislation and present their findings to their peers, perhaps via a blog, wiki or podcast. ● **Tutor-led discussion:** Consider relevant legislation and how organisations and individuals should respond. ● **Knowledge quiz:** Test learners' knowledge of key legislation, matching content, coverage and usage. ● **Tutor-led presentation:** Compare and contrast local and international legislation, e.g. 2001 USA Patriot Act, 1998 Digital Millennium Copyright Act (DMCA), etc. ● **Individual activity:** Learners explore news stories and case studies about prosecutions under local legislation. Encourage them to consider the impact of internet-based cybercrime on the sovereignty of legal authority.	● Tutor presentation ● Research materials (including internet access) ● Relevant legislation ● Case studies about legislative issues regarding IT security

			● **Paired activity:** Learners identify the biggest threats to internet security and discuss whether existing legislation is effective. ● **Plenary:** Use directed Q&A to review the topic and prepare learners for the next session.	
4	**A4** Physical security measures	IS GW	● **Lead in:** Recap content from the previous session (legal responsibilities and security-related legislation in learners' native country). Assess learners' understanding of different pieces of legislation and how organisations should respond in hypothetical situations. ● **Tutor presentation:** Introduce various physical security measures that can be used by an organisation. ● **Tutor-led practical demonstration:** Demonstrate the use of biometric devices to access systems, e.g. unlocking a desktop PC using a fingerprint scanner. ● **Paired activity:** Learners explore physical security measures including basic biometrics (e.g. voice recognition, fingerprint scanners, RFID-style devices, etc.). Provide examples for learners to examine. ● **Individual activity:** Learners consider a range of security scenarios and select and justify appropriate physical security measures. ● **Paired/small group activity:** Learners work in pairs or small groups to present their recommendations (from the individual activity) to their peers for feedback. ● **Tutor presentation:** Discuss physical security measures as applied to data storage, data protection and backup procedures. ● **Individual activity:** Learners practically explore physical security measures applied to data storage, e.g. use of backup tools and media, removable drives, etc. **Stretch and challenge:** If any learners finish early, ask them to	● Tutor presentation ● Biometric devices ● Physical security devices ● Security scenarios ● Research materials (including internet access) ● Removable hard drives, backup devices and software tools ● Guest speaker from, or visit to, a secure location, e.g. data centre or hosting company

			report on a recent security breach and explain how these measures could have been implemented better to improve security. • **Guest speaker/visit:** If possible, invite a guest speaker from, or arrange a visit to, a secure location (e.g. a data centre or hosting company). This will help learners to consider security measures in a real-world context. • **Knowledge quiz:** Test learners' ability to identify strengths and weaknesses of each physical security measure. • **Plenary:** Use directed Q&A to review the topic and prepare learners for the next session.	
5	**A5** Software and hardware security measures	GW IS	• **Lead in:** Recap content from the previous session. Assess learners' understanding of different physical security options by asking them to select and justify the most appropriate protection for a given scenario. • **Tutor presentation:** Review the role of anti-virus software, how it works, signatures, heuristics, scanning and memory resident protection and integration with operating system functions (e.g. opening a file) and applications (e.g. web browser client). • **Tutor-led practical demonstration:** Show how to install, configure and update an anti-virus suite on a range of operating systems, e.g. Mac OS X, Linux and Microsoft Windows. • **Paired activity:** Learners to install, configure and update an anti-virus suite on a range of operating systems. Learners should also have an opportunity to remove or heal an infected file on a quarantined device. • **Tutor presentation:** Review the role of a firewall, showing how rules are created to block incoming and outgoing packets of data depending on source and destination IP, protocol, port number, etc. Differentiate between different types of firewall and how they are implemented on different operating systems.	• Tutor presentation • Anti-virus suites and operating systems • Compromised quarantined devices • Firewalls (various) • Administrative rights on various devices, including command shell/prompt access • Network infrastructure • Network applications to generate traffic, e.g. web browser, email, FTP, SSH clients, etc. • Network protocol analyser

			● **Individual activity:** Learners install and configure a firewall to accept, block, drop or log specific packets of data depending on aspects of the transmission (e.g. connection state, source or destination IP, UDP or TCP, port number, etc.). ● **Paired activity:** Learners test their partner's firewall security configuration, identifying good configuration (which prevents threats) and bad configuration (either not protecting the system or preventing legitimate programs or services from functioning correctly). ● **Knowledge quiz:** Test learners' knowledge of anti-virus software and firewall protection. ● **Plenary:** Use directed Q&A to review the topic and prepare learners for the next session.	● Wireshark ● Squid-cache (a caching proxy)
6	**A5** Software and hardware security measures	IS GW	● **Lead in:** Recap content from the previous session. Assess learners' understanding of anti-virus software and firewalls by asking them to select and justify the most appropriate protection for a given scenario. ● **Tutor presentation:** Introduce the concept of authentication and authorisation, explaining the differences between them. Explain multi-factor authentication techniques and the rationale behind them. ● **Individual activity:** Learners test various login procedures, particularly those with multi-factor authentication. They should experiment with creating strong passwords and different forms of authentication, including knowledge-based, Kerberos and certificate-based (e.g. SSH public/private key pairs and agent forwarding). ● **Tutor-led discussion:** Discuss authorisation and the concept of different user permissions, especially in a secure system.	● Tutor presentation ● SSH key generator ● SSH client, e.g. Putty ● Three-factor authentication website ● Administrative access to a network operating system, including management of user profiles

			• **Tutor-led practical demonstration:** Show how administrative control of rights and permissions can affect users' rights to resources using a variety of operating systems. • **Individual activity:** Allow learners to change authorisation and user permissions to affect their (and others') access to resources, e.g. folders, files, processes and physical devices. • **Paired activity:** Learners test their partner's permissions, identifying good configuration (which prevents unauthorised access or alteration of data) and bad configuration (either not protecting the system or preventing legitimate programs or services from functioning correctly). • **Plenary:** Use directed Q&A to review the topic and prepare learners for the next session.	
7	**A5** Software and hardware security measures	IS	• **Lead in:** Recap content from the previous session. Assess learners' understanding of authentication measures by asking them to select and justify the most appropriate protection for a given scenario. • **Tutor-led discussion:** Discuss the concept of trusted computing and its key components, e.g. endorsement key, memory curtaining, sealed storage, etc. • **Tutor presentation:** Describe basic encryption concepts including how it works (an outline), its objectives and commercial applications. Use a real-world example to illustrate each commercial application – e.g. using an HTTPS connection on a website to obscure the transmission of sensitive data (such as usernames and passwords on a login). • **Tutor-led practical demonstration:** Show how to secure a wireless local area network (WLAN) from unauthorised access using techniques such as channel changing, MAC address filtering, limited guest networks, SSID broadcast suppression, wireless encryption (WEP, WPA, WPA2, WPS), etc. **Note:** There are many tutorials on video sharing sites that	• Tutor presentation • HTTPS website • Network protocol analyser • Switch, router, wireless access point, etc. • Knowledge quiz

			demonstrate the successful reveal of WEP encryption keys. This type of activity can be replicated cheaply (using older hardware and open source software) in a controlled classroom environment. • **Individual activity:** Learners practise encryption, wireless network protection tactics, etc. **Stretch and challenge:** If any learners finish early, ask them to write some questions to be used in the quiz activity. • **Knowledge quiz:** Test learners' understanding of hardware measures that can be used to improve security. • **Plenary:** Use directed Q&A to review the topic and prepare learners for the next session.	
8	Preparation for assessment of learning aim A	PA IS	• **Lead in:** Recap content of learning aim A. • **Individual activity:** Learners work through two case study questions based around the content of learning aim A. This task should test learners' ability to demonstrate knowledge and understanding of technical language, security threats, system vulnerabilities and security protection methods, and the implications of successful threats. • **Tutor-led discussion:** Discuss the case studies and model outcomes. • **Plenary:** Review the model outcomes, focusing on areas which learners found challenging.	• Practice case studies mirroring the external set task, Part A
Learning aim B: Explore the security implications of networked systems				
9	**B1** Network types	GW IS	• **Lead in:** Review prior learning about trusted computing, encryption and securing wireless networks. Assess learners' understanding of these measures by asking them to select and justify the most appropriate protection for a given scenario. • **Tutor presentation:** Present the applications and features of networks. Introduce networks in ascending order (e.g. PAN to WAN)	• Tutor presentation • Materials for posters • Access to networks (e.g. LAN, WLAN,

			and define and differentiate terms such as intranet, extranet, internet and cloud. ● **Tutor-led discussion:** Discuss physical and logical topologies and ask learners to explore different types. ● **Individual or small group activity:** Learners create network topology posters for display in the classroom. ● **Tutor-led practical demonstration:** Use appropriate media, connections and devices to demonstrate the various standards for wired and wireless connections. Differentiate between network architecture models including peer-to-peer, client/server and thin client. ● **Tutor-led discussion:** Using an example, discuss modern trends in networking including 'bring your own device' (BYOD), the 'Internet of Things' (IoT) and software-defined networking (SDN). ● **Individual activity:** Learners use network visualisation tools (e.g. Cisco Packet Tracer) to create networks and interpret schematic diagrams in an interactive fashion. **Stretch and challenge:** Any learners who finish early can prepare instructional posters on the various data visualisation tools available. ● **Knowledge quiz:** Use a game to test learners' knowledge of key terms (e.g. matching cards with network terms and definitions). Learners can work in pairs or small groups. ● **Plenary:** Use directed Q&A to review the topic and prepare learners for the next session.	WAN, PAN, Piconet, etc.) ● Research materials (including internet access) ● Wired and wireless media (e.g. RJ45 jacks, patch panels, CAT 5e UTP cables, coaxial cable, optical fibre, antennae, etc.) ● Network visualisation software ● Peer-to-peer and client/server LAN ● Cisco Packet Tracer ● Cards with network terms and definitions
10	**B2** Network components (hardware)	IS GW	● **Lead in:** Recap content from the previous session. Assess learners' understanding of the different types of network, including their names, features, properties, sizes, uses, etc. ● **Tutor presentation:** Show the different components of a typical network. (Note: Learners are likely to have encountered some	● Tutor presentation ● Resources for practical activity (e.g. network cable crimpers, cyclops sheath stripper,

			components in the previous topic; however, they can be explored fully, in context, here.) - **Individual activity:** Learners examine and combine different types of network component with the aim of creating a simple LAN. This could include making (and testing) Cat 5 cables, punching patch panels, using WAPs, a LAN switch and NICs, etc. As such, you could split this into two separate activities: component preparation and network build and test. - **Tutor-led practical demonstration:** Introduce applications and features of external media and storage, including flash drives and optical media. - **Paired activity:** Learners explore and compare functionality and features of different external media, in terms of capacity, transfer rates, access time, robustness, reliability, etc. - **Plenary:** Use directed Q&A to review the topic and prepare learners for the next session.	punch down tool, cable tester, wiring diagrams (e.g. EIA/TIA T-568A/B), NICs, switch, hub, WAP, straight-through and crossover cables, etc.) - Administrative rights on target devices - External media
11	**B2** Network components (software)	GW	- **Lead in:** Recap content from the previous session. Assess learners' understanding of hardware-oriented network components, including their names, features, properties, sizes, uses, etc. - **Tutor-led practical activity:** Demonstrate different applications and features of a range of software components. - **Paired activity:** Lead and monitor a series of suitably differentiated activities for learners, such as: ○ installing and configuring a network operating system ○ using network tools to confirm connectivity or troubleshoot issues, e.g. ping, ifconfig/ipconfig, traceroute, DNS, arp, etc. ○ using monitoring tools to view network throughput ○ viewing network events and system/device logs ○ sniffing transmitted packets in network traffic using a protocol analyser	- NICs, Switch, Hub, WAP, straight-through and crossover cables, etc. - Administrative rights on target devices - Network visualisation software - Peer-to-peer and client/server LAN

			○ scanning a network's open ports for vulnerabilities ○ installing and testing network-aware applications such as relational databases by remotely connecting and querying a simple data source. ● **Tutor-led discussion:** Review outcomes of practical activities, including new skills learned, problems encountered and solutions discovered. ● **Plenary:** Use directed Q&A to review the topic and prepare learners for the next session.	● Administrative access to reporting, system logs and functionality on a network operating system ● Port scanning software
12	**B3** Networking infrastructure services and resources	IS	● **Lead in:** Recap content from the previous session. Assess learners' understanding of different network components and their purposes and uses within a network installation. ● **Tutor presentation:** Explain the application and function of TCP/IP, ports, packets and network address translation (NAT), including the structure of IPv4 and IPv6 addressing and RFC 1918 private addresses. If possible, demonstrate the use of a protocol analyser to capture incoming and outgoing data packets; explain that this can be very informative when tracking a simple network operation such as a ping. ● **Individual activity:** Learners use a simple protocol analyser to track packets 'in' and 'out' of their computer, inspecting the data being sent and the source and destination IP addresses. ● **Individual activity:** Learners investigate network configuration, including the use of domains and sub-domains. ● **Tutor-led practical demonstration:** Demonstrate different configurations that change the way network devices work, e.g. a router issuing IP addresses via DHCP, or use of a switch to segment a network using its VLAN functionality. ● **Tutor-led individual activity:** Help learners to explore a variety of network infrastructure services, such as:	● Tutor presentation ● Network protocol analyser ● Access to networks (e.g. LAN, WLAN, WAN, PAN, piconet, etc.) ● Router with administrative access ● Server with network operating system and administrative access ● OpenLDAP ● SSH client ● Devices with DHCP clients ● Remote desktop client

			○ domain name system (DNS) ○ directory services (DS) including Microsoft Windows Active Directory and open source implements such as OpenLDAP ○ Dynamic Host Configuration Protocol (DHCP) ○ routing ○ remote access services such as Remote Desktop Protocol (RDP) or Secure Shell (SSH). ● **Tutor-led practical demonstration:** Demonstrate the installation, configuration and use of network services and resources including file and print services, web hosting, mail and communication services. One way of doing this is to enable a web server on a quarantined LAN and access its resources via a client using HTTP requests. You can track the whole HTTP request and response process by viewing the requests using a protocol analyser, inspecting the web server's access log, and finally rendering the transmitted resource on a web browser. Demonstrate real-time modifications to the served content by requesting the resource again. ● **Plenary:** Use directed Q&A to review the topic and prepare learners for the next session.	● Hosted services, e.g. HTTP (Apache, Microsoft IIS, etc), file and printer sharing, etc.
13	Preparation for assessment of learning aim B	PA IS	● **Lead in:** Recap content of learning aim B. ● **Individual activity:** Learners work through two case study questions based around the content of learning aim B. This task should test learners' ability to plan a secure computer network and manage security incidents, with justification. ● **Stretch and challenge:** Any learners who finish early can develop new case studies to show a range of issues and solutions. They can develop these case studies in further sessions or as homework. ● **Tutor-led discussion:** Discuss the case studies and model outcomes.	● Practice case studies mirroring the external set task, Part A

			● **Plenary:** Review the model outcomes, focusing on areas which learners found challenging.	
Learning aim C: Develop a cyber security protection plan for a specified organisation				
14	**C1** Assessment of computer system vulnerabilities	IS	● **Lead in:** Recap content from previous sections about the infrastructure of a network and the different services it provides. Assess learners' understanding of the services (e.g. DNS, DS, DHCP, etc.) and how they operate. ● **Tutor-led practical demonstration:** Introduce the tools and methods used to discover and assess vulnerabilities in computer systems. For example: o perform an automated port scan on a server (all ports or a given range), identifying the available services for each one reported o check a Microsoft Windows registry for embedded malware scripts or weak security settings o use automated website 'crawler' tools to look for vulnerabilities, e.g. Acunetix Vulnerability Scanner. ● **Individual activity:** Learners practise using a variety of these tools and methods to find known (i.e. engineered) vulnerabilities. ● **Tutor-led discussion:** Review with learners the purpose of independent third-party review of a system. ● **Tutor-led practical demonstration:** Review the Open Web Application Security Project (OWASP) Top 10 and its use in penetration testing. Where possible, give a practical illustration of each entry. ● **Knowledge quiz:** Test learners' knowledge of tools and techniques to discover and assess vulnerabilities in computer systems (perhaps using a matching exercise). ● **Plenary:** Use directed Q&A to review the topic and prepare learners for the next session.	● Port scanning software (or website) ● Microsoft Registry Editor (e.g. regedit.exe) ● Automated website 'crawler' tools (e.g. Acunetix Vulnerability Scanner) ● OWASP Top 10 ● Knoweldge quiz

15	**C2** Assessment of the risk severity for each threat	IS	• **Lead in:** Recap content from the previous session. Assess learners' understanding of the tools and methods used to discover and assess a computer system's vulnerabilities. • **Tutor-led practical demonstration:** Show how to calculate the risk severity for given threats. For each threat, show learners how to: ○ define the risk severity as the probability of the threat occurring multiplied by the expected impact level/value of the loss ○ differentiate risks as low, medium, high or extreme ○ differentiate probability of the threat occurring as unlikely, likely or very likely ○ differentiate impact level/value of the loss as minor, moderate or major. • **Individual activity:** Learners create a risk severity matrix in a format of their choice (e.g. manual diagram, word-processed table, spreadsheet, website form or programmed solution). • **Individual activity:** Give learners a set of real-world scenarios and ask them to assess the probability and impact levels and thus calculate the risk severity. **Stretch and challenge:** Any learners who finish early can start to consider the steps that could be built into a plan to help prevent threats. (This leads into the next session.) • **Tutor-led discussion:** Learners share and discuss their risk calculations. Review the approaches and methods used and correct any misconceptions. • **Plenary:** Use directed Q&A to review the topic and prepare learners for the next session.	• Risk assessment grid • Real-world risk scenarios
16	**C3** A cyber security plan for a system	GW	• **Lead in:** Recap content from the previous session. • **Tutor-led discussion:** Discuss when to plan cyber security measures (based on medium, high and extreme risk severity for identified threats).	• Tutor presentation • Sample/model cyber security plan

			● **Tutor presentation:** Present a model cyber security plan for a given scenario and walk learners through the various sections, e.g. software and hardware protection measures, risk assessment, constraints, legal responsibilities, etc. ● **Small group activity:** In groups of 3 or 4, learners construct a document for a selected case study (after they have investigated the scenario, identified the vulnerabilities and assessed their risks). This document should mirror the model security plan, including similar content in an appropriate format. ● **Tutor-led activity:** Groups swap their plans with their peers and evaluate whether the protection measures would work as intended, identifying good practice and possible areas for improvement. Lead and moderate as appropriate. ● **Tutor-led practical demonstration:** Present a case study scenario (based on a particular organisation and its IT and cyber security set-up), including a range of possible threats to the system and a range of possible security measures to mitigate those threats. ● **Knowledge quiz:** Ask learners to classify threats as low, medium, high and extreme and say whether given cyber security measures would be effective against each threat. ● **Plenary:** Use directed Q&A to review the topic and prepare learners for the next session.	● Case studies
17	Preparation for assessment of learning aims C1–C3	PA IS	● **Lead in:** Recap content of learning aims C1–C3. ● **Individual activity:** Learners work through two case study questions based around the content of learning aims C1–C3. This task should test learners' ability to apply knowledge and understanding of security threats, system vulnerabilities and security protection methods and implications, to risk assess systems and select appropriate tools to secure them.	● Practice case studies mirroring the external set task, Part A

			• **Tutor-led discussion:** Discuss the case studies and model outcomes. • **Plenary:** Review the model outcomes, focusing on areas which learners found challenging.	
18	**C4** Internal policies	GW	• **Lead in:** Recap the steps involved in creating a cyber security plan for a given system. • **Tutor presentation:** Detail cyber security documentation which needs to be observed, established and maintained by an organisation. • **Tutor presentation:** Present general IT policies, their content and rationale. • **Tutor-led discussion:** Discuss and explore incident response policies. • **Group activity:** Learners role play a given IT incident response policy for a selected scenario and judge whether it is effective. • **Tutor-led discussion:** Discuss and explore disaster response policies. • **Plenary:** Use directed Q&A to review the topic and prepare learners for the next session.	• Tutor presentation • Sample/model cyber security documentation • Sample/model IT policies, e.g. acceptable use, internet use, email, etc. • IT incident response policy
19	**C5** External service providers	IS	• **Lead in:** Recap the types and uses of internal policies in an organisation. • **Tutor presentation:** Explore the role of an External Service Provider (ESP), using a case study to illustrate key points. • **Tutor-led discussion:** Discuss ESP agreements for cloud services, applications and storage. • **Knowledge quiz:** Ask learners to determine which types of agreement may be covered by data protection laws. • **Tutor-led discussion:** Discuss ESP agreements for hardware and software.	• Tutor presentation • ESP case study • ESP sample agreements

			• **Tutor presentation:** Outline the implications of ESP agreements. • **Individual activity:** Learners create a suitable ESP agreement between two parties for a given scenario. • **Tutor-led discussion:** Review common features of learners' ESP agreements and give feedback. • **Plenary:** Use directed Q&A to review the topic and prepare learners for the next session.	
20	Preparation for assessment of learning aims C4 and C5	PA IS	• **Lead in:** Recap content of learning aims C4 and C5. • **Individual activity:** Learners work through two case study questions based around the content of learning aims C4 and C5. This task should test learners' ability to evaluate protection methods and security documentation, make reasoned judgements and draw conclusions about their efficacy. • **Tutor-led discussion:** Discuss the case study and model outcomes. • **Plenary:** Review the model outcomes, focusing on areas which learners found challenging.	• Practice case studies mirroring the external set task, Part A
Learning aim D: Examine procedures to collect forensic evidence following a security incident				
21	**D1** Forensic collection of evidence	GS IS GW	• **Lead in:** Recap content about external service providers. Assess learners' understanding of the role of an ESP and the types of agreement made with them (and their implications). • **Tutor presentation:** Detail the process of collecting evidence after a security incident, using a forensically-sound methodology. Present desktop forensic activities. **Note:** Learners should understand the processes in their native country, although UK/USA methodologies also have value. • **Guest speaker:** If possible, arrange for a digital forensic scientist to talk about local forensic investigation rules. • **Individual activity:** Lead and support practical sessions to impart new practical skills, e.g.	• Tutor presentation • Guest speaker • Operating system, administrative access, file system activities and tools

			○ cloning a file system ○ checking recently mounted devices ○ showing recent firewall activity ○ viewing configuration files ○ scanning a system for operating security holes and network or application vulnerabilities. ● **Guest speaker:** Invite a guest speaker, perhaps from your own institution's network infrastructure and services team, to provide additional insight and hold a learner Q&A session. ● **Tutor-led discussion:** Discuss the challenges of live forensics. ● **Tutor-led practical demonstration:** Examine and demonstrate the procedures involved in network forensics. ● **Paired activity:** Learners perform a series of network forensics tasks. Review their work and give feedback, particularly where their actions have contaminated the evidence base and could adversely affect the investigation or potential prosecution. ● **Knowledge quiz:** Test learners' understanding of how evidence can be collected and documented safely, without potential contamination or data loss. ● **Plenary:** Use directed Q&A to review the topic and prepare learners for the next session.	
22	**D2** Systematic forensic analysis of a suspect system	GW	● **Lead in:** Recap correct procedures to follow when collecting forensic evidence of a system incursion or security incident. Assess learners' understanding of the typical activities and practical skills involved. ● **Tutor-led discussion:** Discuss the requirements for maintaining accurate records. ● **Tutor presentation:** Present a checklist of different evidence sources and show how to attain them.	● Tutor presentation ● Forensic evidence checklist ● Model forensic report

			• **Tutor-led practical demonstration:** Work through a model forensic report of an incident and guide learners to: ○ evaluate the findings and determine whether or not they prove a crime has been committed ○ show the source of the compromise (internal or external) ○ ascertain whether a single cause can be clearly proven. • **Paired activity:** Learners make recommendations on how to prevent similar security incidents in future. They should draw on security measures they have already been taught and they must justify their selections appropriately. • **Tutor-led discussion:** Give feedback on learners’ recommendations. • **Knowledge quiz:** Use a Q&A session to assess learners’ ability to identify different evidence sources and how they are attained. • **Plenary:** Use directed Q&A to review the topic and prepare learners for the next session.	
23	Preparation for assessment of learning aim D	PA	• **Lead in:** Recap content of learning aim D. • **Individual activity:** Work through case study questions based around the content of learning aim D. This task should test learners’ ability to analyse forensic evidence data and information to identify security breaches and manage security incidents. • **Tutor-led discussion:** Discuss the case study and model outcomes. • **Plenary:** Review the model outcomes, focusing on areas which learners found challenging.	• Practice case studies mirroring the external set task, Part B
24–26	Planned assessment	AW	• **Set task**	

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