**BTEC Level 3 National in Information Technology:**

**Unit 11**

Learner Workbook 1

**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](http://qualifications.pearson.com/en/qualifications/btec-nationals/information-technology-2016.html):   * Unit specification * Instructions for Conducting External Assessments (ICEA) * **Unit 11** Sample Assessment Materials (SAMs) * **Unit 11** Sample Marked Learner Work (SMLW) * **Unit 11** Scheme of work * **Unit 11** Delivery guide * **Unit 11** Scheme of work * **Unit 11** Administrative guide * **Unit 11** Templates * Any other new/updated documentation relevant to this unit   The information in this learner workbook is considered to be correct at the date of publication. |

**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)**

|  |
| --- |
| A cyber-attack is an assault launched by cybercriminals using one or more computers against a single or multiple computers or networks. A cyber-attack can maliciously disable computers, steal data, or use a breached computer as a launch point for other attacks. |

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

|  |
| --- |
| Data protection is crucial for every business. To assess the risks, companies need to know what data they are storing and using. If the data you hold includes personal data (and it almost certainly will), then the company must carry out regular data protection audits, to get an overview of the data they use, how well it is protected and how they are complying with data protection legislation, including GDPR. |

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

|  |  |
| --- | --- |
| **Type** | **Explanation** |
| Hacker | A hacker is an individual who uses computer, networking or other skills to overcome a technical problem. The term also may refer to anyone who uses their abilities to gain unauthorized access to systems or networks in order to commit crimes. |
| Insider | An insider threat is a security risk that originates from within the targeted organisation. It typically involves a current or former employee or business associate who has access to sensitive information or privileged accounts within the network of an organisation, and who misuses this access. |
| Script kiddie | A disparaging term often used to refer to less experienced malicious hackers who use existing software to launch hacking attacks. While security professionals tend to craft their own tools, script kiddies pick up off the shelf exploits, scripts, and tools to attack a target.  Considered less skilled than professional penetration testers, or white hat hackers, script kiddies usually don’t understand the inner workings of software and computer networking. |
| Scammer/Phisher | Scammers make unsolicited phone calls or place misleading pop-up Internet advertisements to try to convince unsuspecting computer users that something is seriously wrong with their computers that must be fixed immediately. Scammers often pose as representatives of reputable, well-known computer or software companies.  Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. |

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

|  |  |
| --- | --- |
| **Type** | **Explanation** |
| Espionage | Cyber espionage is a form of cyber-attack that steals classified, sensitive data or intellectual property to gain an advantage over a competitive company or government entity. Generally, we think of cyber espionage in terms of theft of intellectual property, but it could also be focused upon the theft of confidential information related to acquisitions, marketing plans and other types of data. |
| Public good | Cyber-attacks in the interests of the public good are carried out by so called ‘hacktivists’ who use computers and computer systems to promote their own views on particular issues, such as human rights, animal rights or ethics. |
| Score settling | Disgruntled ex-employees may pose a serious threat to organisations as sources of cyber-crimes targeting their former employers. They may use their knowledge of systems to attack the organisation for financial gain. |
| Thrill | There are some that are intrinsically motivated to simply attack an organisation or person for no other reason than to create chaos and destruction. |
| Fraud | Theft of personally identifiable information (PII), that is then monetised is a classic example of financial motivation of cyberattacks. Primarily perpetrated by organized criminal groups, this motivation represents a large percentage of cyberattacks against retailers and health care providers. |

1. In your own words **describe** what is meant by the term ‘cyber security.’ **(PASS)**

|  |
| --- |
| Cyber Security is how organisations and individuals protect their information, assets, data software and hardware. |

**Topic 1**

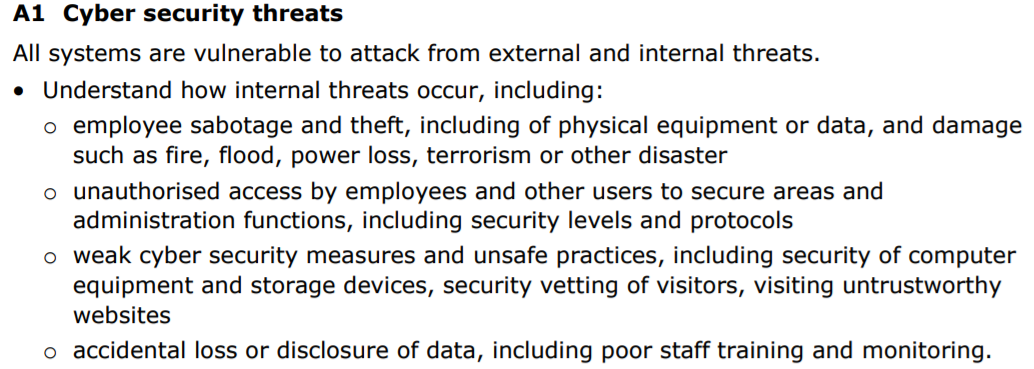
**Internal Threats**

**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:**

****

**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)**

|  |
| --- |
| Computer sabotage is the input, alteration, erasure or suppression of computer data or computer programmes, or interference with computer systems, with the intent to hinder the functioning of a computer or a telecommunication system.  https://itlaw.fandom.com/wiki/Computer\_sabotage#:~:text=Definition,computer%20or%20a%20telecommunication%20system. |

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

|  |
| --- |
| In general, theft refers to the illegal act of taking something that does not belong to you and has not been freely given to you.  In the context of a computer network, this could include data theft, Identify theft or software piracy. |



1. **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)**

|  |
| --- |
| [Tesla worker 'carried out extensive and damaging sabotage'](https://news.sky.com/story/tesla-worker-carried-out-extensive-and-damaging-sabotage-11410001) |



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

|  |
| --- |
| Tips to prevent employee sabotage, from HRDept.co.uk:  <https://www.hrdept.co.uk/blog/seven-tips-protect-business-employee-sabotage/>  1. Start at the beginning with your recruitment. A thorough recruitment process can help to make sure you are hiring employees that are a good fit for your business. Comprehensive reference checks, a reliable interview process and employee vetting can highlight causes of concern early on.  2. Accountability for actions. Each employee should be aware of their own accountability. Breaking down business goals and explaining how they relate on a team or employee level can help to get everyone on the same page and working towards the same purpose.  3. Need to know basis. With information sharing in mind, it’s wise to consider who needs to know what and how much. Updating managers and employees is beneficial but you’ll also need to protect yourself when it comes to sensitive data.  4. Policies for protection. Policies are a good way to inform employees of your expectations and can help you to manage a difficult employee. Policies on social media use, conduct and data protection can all help to provide a solution in the event of employee sabotage.  5. A time and place for feedback. Regular reviews offer an opportunity to pick up on potential problems. You can use this time for feedback and to look for a resolution. Correct documentation is essential should you need to refer back to previous meetings.  6. Don’t skimp on security. Change passcodes and revoke access when employees leave, or sooner if the situation is urgent. You’ll also want to protect your online brand reputation. Use social media listening to watch for brand mentions and address any online grievances.  7. Company culture. An inclusive and diverse culture that promotes employee voice can keep you in touch with the overall well-being of your workforce. If trouble is brewing, it could be time to collect feedback or consider a team-building away day.  Evaluation: will depend on student’s persepective. |

**Unauthorised Access**

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

|  |
| --- |
| **Unauthorized access** is when someone gains access to a website, program, server, service, or other system using someone else's account or other methods. For example, if someone kept guessing a [password](https://www.computerhope.com/jargon/p/password.htm) or [username](https://www.computerhope.com/jargon/u/username.htm) for an account that was not theirs until they gained access, it is considered unauthorized access. |

1. **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)**

|  |
| --- |
| Once a person has gained access to a system, they may then steal, modify, disclose or destroy the data.  Data Theft can be very profitable – hackers steal information about individuals or organisations and either use the information to set up new identities for criminal transactions or sell the information on for a fee.  Data is entered stored and modified by those with authorisation. Sometimes individuals or groups seek to alter the data that manages the information system. When data is illegally modified it is to blackmail or cause harm to an organisation or individual.  Information disclosure is allowing information to pass to an organisation or person without permission. This could be financial data regarding the company assets or future plans, or it could be government information regarding how many soldiers are available for deployment, how many aircraft are stationed in certain airbases and of what type.  The destruction of data can be carried out by authorised individuals. However, it can also be destroyed remotely using software – which in the case of Trojan software can select and destroy specific data sets, such as falsified personnel records or payments made into money laundering schemes. |



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

|  |
| --- |
| Strategies that can be used to reduce the risk of unauthorised access:   1. **Strong Password Policy**   Enforce best practices for user passwords—force users to select long passwords including letters, numbers and special characters, and change passwords frequently.  Educate users to avoid using terms that can be guessed in a brute force attack, inform them about routine password updating, and to tell them to avoid sharing passwords across systems.   1. **Two Factor Authentication (2FA) and Multifactor Authentication**   Credentials based on user-names, passwords, answers to security questions, etc. are known more generally as knowledge-based security factors. Knowledge-based factors are an important authentication method, but they are inherently weak and easy to compromise.  One of the best ways to prevent unauthorized access is to supplement knowledge-based factors with additional authentication methods:  Possession factors — authentication via objects possessed by the user. For example, a mobile phone, a security token or a physical card.  Inherence factors — authentication via something the user is or has. This includes biometric authentication using fingerprints, iris scans or voice recognition.   1. **Physical Security Practices**   As important as cybersecurity is, don’t neglect physical security. Train users to always lock devices when walking away from their desks, and to avoid writing down passwords or leaving sensitive documents in the open. Have a clear policy about locking office doors and ensure only authorized parties can enter sensitive areas of your physical facility.   1. **Monitoring User Activity**   It is crucial to monitor what is happening with user accounts, to detect anomalous activity such as multiple login attempts, login at unusual hours, or login by users to systems or data they don’t usually access. There are several strategies for monitoring users and accounts:  Log analysis — security analysts can gain visibility into logs of sensitive enterprise systems and uncover suspicious activity  Rule-based alerts — security tools can alert security staff to suspicious activity patterns, such as multiple login attempts or incorrect login to sensitive systems  Behavioural analytics — User and Event Behavioural Analytics (UEBA) monitors users and systems, establishes a baseline of normal activity, and detects any behaviour that represents an anomaly and may be malicious.   1. **Endpoint Security**   Historically, most security breaches were a result of penetrating the network perimeter. Today, many attacks circumvent network defences by directly targeting endpoints, such as employee workstations, servers, cloud instances. Installing antivirus on every endpoint is the most basic security measure.  Beyond antivirus, many organizations are deploying comprehensive endpoint protection measures that include:  Next-generation antivirus (NGAV) – able to detect malware and other threats even if they don’t match known patterns or signatures  Endpoint Detection and Response (EDR) – provides visibility and defensive measures on the endpoint itself, when attacks occur on endpoint devices |

**Safe working practices**

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

|  |
| --- |
| Safe working practice in this context is not about the height of your monitor or how much time you spend at a screen. It is about educating your employees about cyber security and physical security, for instance: use VPNs at home to access the office remotely, have firewalls on all computers, encrypt and limit access to organisationally sensitive data. |

1. **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)**
2. Securely checking visitors are genuine

|  |
| --- |
| Visitors are anyone who does not have normal access to an area. They should only be given unescorted entry if they can show a suitable form of identification and have proper security clearance from someone inside the organisation for a genuine reason.  This can be supplemented using an electronic access control system, which allows organisations to issue visitors with access cards enabled for the specific areas that they can access, for a specific period.  These passes must be always worn, then collected and disabled at the end of the day. All visitors must be registered. |

1. Ensuring users visit trustworthy website

|  |
| --- |
| Use filtering software to manage access to websites.  Use website blocking software to block unsuitable sites  All employees to sign an agreement not to access any sites that may not be in line with the company policy. |

**Accidental loss and disclosure of data**

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

|  |
| --- |
| Data loss is the intentional or unintentional destruction of information, caused by people and or processes from within or outside of an organization. Data loss is like a data breach, in that data is compromised. However, in a data breach, data is usually unharmed but in the wrong hands. Data loss can occur in a data breach, but the data itself is destroyed. |

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

|  |
| --- |
| Accidental disclosure of data is where personal data is unknowingly or accidentally disclosed to someone who does not have the right to see that data. For instance, sending an email to an unintended recipient. |

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

|  |
| --- |
| If a company doesn’t have a good staff training programme for cyber security, staff amy not be aware of the steps that they need to take to protect the company’s data, and they may unknowingly exploit vulnerabilities in the company's systems, for instance by leaving their computer unlocked. If staff are not monitored and their access managed, they may allow accidental disclosure of data by allowing attackers access to company systems, or by leaving a USB on a train. This would be a huge risk to the reputation of the company. |

**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**

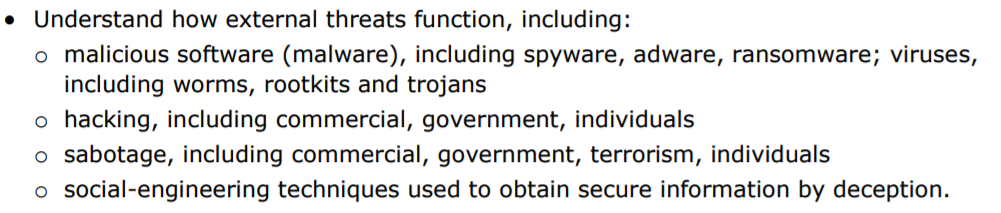
**External Threats**

**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** thedifferent 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:**

****

**Topic 2: Introductory Task:**

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

|  |
| --- |
| In December 2020, it emerged that [SolarWinds had been the victim of possibly the biggest state-orchestrated cyber attack in history](https://www.computerweekly.com/news/252507279/The-Security-Interviews-How-SolarWinds-came-through-its-darkest-hour), after a Russia-backed group compromised its Orion platform and used it to target government bodies. The fallout from this attack persisted throughout 2021, and through it all, SolarWinds’ new CEO, Sudhakar Ramakrishna, emerged as a bit of a security hero for his frank and honest response.  In August 2021, Microsoft came under fire after a series of miscommunications resulted in a situation where users [failed to patch their Microsoft Exchange servers properly](https://www.computerweekly.com/news/252505767/Half-of-MS-Exchange-servers-at-risk-in-ProxyShell-debacle), leaving them exposed to three distinct vulnerabilities. Redmond had patched two of the bugs – which together could be chained to achieve remote code execution on a target system – in April 2021, but did not disclose them or assign them a CVE number, meaning IT security teams missed their significance until much later.  In July 2021, questions were asked [over the work of Israel-based cyber surveillance specialist NSO Group](https://www.computerweekly.com/news/252504149/Pegasus-mobile-RAT-abused-to-monitor-journalists-and-activists) after the exposure of more than 50,000 phone numbers belonging to activists, journalists and other people deemed “of interest” to some of the world’s most repressive regimes that had allegedly been using its Pegasus remote access trojan (RAT). While NSO Group denies wrongdoing, it has haemorrhaged support and investment, and become the subject of US government sanctions.  At the end of May 2021, security and data privacy experts were quick to warn the public of proposed NHS Digital plans [to scrape medical data on 55 million patients in England into a new database](https://www.computerweekly.com/news/252501494/Privacy-experts-concerned-over-NHS-data-collection-plans). The GPDPR database would have contained swathes of sensitive information, such as data on diagnoses, symptoms, observations, test results, medications, allergies, immunisations, referrals, recalls and appointments. It was also supposed to have included information on physical, mental and sexual health, data on gender, ethnicity and sexual orientation, and data on staff who had treated patients. The plans were later put back pending changes, but for IT leaders the story highlighted the importance of appropriate data collection, consent, and transparency in service development. |

**Topic 2: Deeper Learning Activities:**

**Malware**

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

|  |
| --- |
| Malware is intrusive software that is designed to damage and destroy computers and computer systems. Malware is a contraction for “malicious software.” Examples of common malware includes viruses, worms, Trojan viruses, spyware, adware, and ransomware. |

1. **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 | Spyware is malicious software that runs secretly on a computer and reports back to a remote user. Rather than simply disrupting a device’s operations, spyware targets sensitive information and can grant remote access to predators. Spyware is often used to steal financial or personal information. A specific type of spyware is a keylogger, which records your keystrokes to reveal passwords and personal information. | Data compromised by spyware often includes collecting confidential info such as:  Login credentials — passwords and usernames  Account PINs  Credit card numbers  Monitored keyboard strokes  Tracked browsing habits  Harvested email addresses |
| Adware | Adware is malicious software used to collect data on your computer usage and provide appropriate advertisements to you. While adware is not always dangerous, in some cases adware can cause issues for your system. Adware can redirect your browser to unsafe sites, and it can even contain Trojan horses and spyware. Additionally, significant levels of adware can slow down your system noticeably. Because not all adware is malicious, it is important to have protection that constantly and intelligently scans these programs. | Effects of Adware:  It slows down the browsing speed  Brings down the processing speed of the PC  Interrupts with the system’s performance  Changes to browser homepage and search results  Customized ads are displayed on web pages and when clicked, malware gets downloaded at the back end.  It is just not about displaying advertisements on the users’ screen. The prime objective of the adware definition is to collect data from the user without showing its presence in the user’s system. It does not show any indication of its installation in the program menu. |
| Ransomware | Ransomware is malicious software that gains access to sensitive information within a system, encrypts that information so that the user cannot access it, and then demands a financial payout for the data to be released. Ransomware is commonly part of a phishing scam. By clicking a disguised link, the user downloads the ransomware. The attacker proceeds to encrypt specific information that can only be opened by a mathematical key they know. When the attacker receives payment, the data is unlocked. | The impacts of a ransomware attack to your company could include the following:  temporary, and possibly permanent, loss of data  possibly a complete shutdown of operations  financial loss as a result of revenue generating operations being shut down  financial loss associated with remediation efforts  damaged to company reputation |

**Viruses**

1. **Describe** what is meant by the term ‘virus.’ **(PASS)**

|  |
| --- |
| Viruses are a subgroup of malware. A virus is malicious software attached to a document or file that supports macros to execute its code and spread from host to host. Once downloaded, the virus will lay dormant until the file is opened and in use. Viruses are designed to disrupt a system’s ability to operate. As a result, viruses can cause significant operational issues and data loss. |

1. **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 | Worms are a malicious software that rapidly replicates and spreads to any device within the network. Unlike viruses, worms do not need host programs to disseminate. A worm infects a device via a downloaded file or a network connection before it multiplies and disperses at an exponential rate. Like viruses, worms can severely disrupt the operations of a device and cause data loss. | Worms can modify and delete files, and they can even inject additional malicious software onto a computer. Sometimes a computer worm’s purpose is only to make copies of itself over and over — depleting system resources, such as hard drive space or bandwidth, by overloading a shared network. In addition to wreaking havoc on a computer’s resources, worms can also steal data, install a backdoor, and allow a hacker to gain control over a computer and its system settings. |
| Rootkits | A rootkit allows someone to maintain command and control over a computer without the computer user/owner knowing about it. | Once a rootkit has been installed, the controller of the rootkit can remotely execute files and change system configurations on the host machine. A rootkit on an infected computer can also access log files and spy on the legitimate computer owner’s usage. |
| Trojans | Trojan viruses are disguised as helpful software programs. But once the user downloads it, the Trojan virus can gain access to sensitive data and then modify, block, or delete the data. | Unlike normal viruses and worms, Trojan viruses are not designed to self-replicate, but can have highly destructive effects: from deleting files to destroying all the contents of the hard disk. Trojans can also capture and resend confidential data to an external address or open communication ports, allowing an intruder to control the infected computer remotely |

**Hacking**

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

|  |
| --- |
| Hacking is an attempt to exploit a computer system or a private network inside a computer. Simply put, it is the unauthorised access to or control over computer network security systems for some illicit purpose.  Hacking can be described as gaining unauthorised access to a computer system by improper means.  Unauthorised access can be describes as gaining access to a computer system using usual means of access but without consent. |

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

|  |  |
| --- | --- |
| **Type** | **Description** |
| Individual | A hacker is an individual who uses computer, networking or other skills to gain unauthorized access to systems or networks in order to commit crimes. |
| Government | Government hacking permits the exploitation of vulnerabilities in electronic products, especially software, to gain remote access to information of interest. This information allows government investigators to monitor user activity and interfere with device operation. Government attacks on security may include malware and encryption backdoors. The National Security Agency's PRISM program and Ethiopia's use of FinSpy are notable examples. |



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

|  |
| --- |
| In December 2021 Brazil’s Ministry of Health suffered a major ransomware attack that resulted in the unavailability of Covid-19 data for millions of citizens. Following that attack , all of the MoH's websites, including ConecteSUS, which tracks the trajectory of citizens in the public healthcare system, became unavailable. This includes the COVID-19 digital vaccination certificate, which is available via the ConecteSUS app.  According to a message left by the Lapsus$ Group, which has claimed responsibility for the attack, some 50TB worth of data has been extracted from the MoH's systems and subsequently deleted. "Contact us if you want the data returned", the message said, alongside contact details for the authors of the attack.    The incident followed a previous attack on the Brazilian Health Regulatory Agency (Anvisa). The attack was focused on the healthcare declaration for travellers, compulsory for individuals entering Brazil via airports.  The attack took place soon after the cancellation of the World Cup qualifier match between Brazil and Argentina, whereby Anvisa interrupted the game after four Argentinian players were accused of breaking COVID-19 travel protocols.  Similarly, the latest issue faced by the Ministry of Health occurs amid increasing pressure on the Brazilian government to demand COVID-19 vaccination certificates from international travellers coming to Brazil as a response to the rise of the omicron variant.  This is not the first major security issue faced by Brazil's Ministry of Health over the last few months. In November 2020, the personal and health information of more than 16 million Brazilian COVID-19 patients were leaked online after a hospital employee uploaded a spreadsheet with usernames, passwords, and access keys to sensitive government systems on GitHub.  Less than a week later, another major security incident emerged. The personal information of more than 243 million Brazilians, including alive and deceased, was exposed online after web developers left the password for a crucial government database inside the source code of an official MoH website for at least six months.  The impact of these repeated attacks will be to affect the public’s trust in the confidentiality of the data that is held in their medical records, some of which could potentially be very personal. It is the equivalent of the NHS main databases being breached.  Had the organisation not been able to access the backup data, this would also have meant that millions of Brazilians would have been unable to confirm their vaccination status, having a potential impact on their travel plans. |

**Sabotage**

1. **Describe** what is meant by the term ‘sabotage.’ **(PASS)**

|  |
| --- |
| Computer sabotage involves deliberate attacks intended to disable computers or networks for the purpose of disrupting commerce, education and recreation for personal gain, committing espionage, or facilitating criminal conspiracies, such as drug and human trafficking. According to the Federal Bureau of Investigation, computer sabotage costs billions of dollars in legal fees to recover damages such as identity theft and to repair vital infrastructure that serves hospitals, banks and 911 services. |

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

|  |  |
| --- | --- |
| **Type** | **Description** |
| Terrorism | Cyberterrorism is the use of cyber based tools by terrorists to inflict damage on a country’s military, financial or service sectors. |
| Individual | On an individual level, sabotage is a deliberate act (or series of acts) that are destructive or hindering to another individual in some way. |
| Commercial | With regard to computers, sabotage is the deliberate damage to equipment. Infecting a website with malware is an example of information sabotage. |
| Government | Sabotage against another government, e.g. causing the power grid in a nation to go down or defence systems to be stopped. |



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

|  |
| --- |
| Sabotage is also another way from where an attack can be launched. It defines the activities that are deliberately carried out to disrupt service.  The common attacks that can take place include DDoS attacks. DDoS stands for Distributed Denial of Service, and it's a method where cybercriminals flood a network with so much malicious traffic that it cannot operate or communicate as it normally would. This causes the site's normal traffic, also known as legitimate packets, to come to a halt.  The largest DDoS attack reported recently was by Amazon Web Services in 202. This attack measured 2.3 Tbps - terabits per second. It is a measure of the amount of data being sent every second to the servers of the victim company. This is not the biggest attack ever, but the biggest ever recorded. Lots of companies Many organizations do not publicly disclose the extent or volume of attacks they experience as they fear the reputational risk to their brand.  According to Corero.com (<https://www.corero.com/blog/the-damaging-impacts-of-ddos-attacks/>) there are a number of impacts:  **Loss of revenue**  Downtime can be extremely costly, depending on the type of business and the size of the organization. One hour of downtime for a financial institution versus an hour of downtime for a university network may incur very different costs, but the impact on customers or users is significant in either case. In the past year, Veeam software reported that an hour of downtime from a High Priority application is estimated to cost $67,651, while this number is only a little lower at $61,642 for a normal application. With such a balance between High Priority and Normal in impact costs, it’s clear that “all data matters” and that downtime is intolerable anywhere within today’s environments.” For further evidence of the increasingly costly impact of enterprise server downtime, see this Statistica report for 2019.  **Lost productivity**  When a business application or service is degraded, or worse, is taken offline completely, that usually means employees can’t work as efficiently, or in many cases, at all. This has become particularly apparent during the COVID-19 pandemic, as a much larger percentage of employees now work remotely and depend on reliable connectivity to collaborate with their colleagues. When factoring in the overall cost of a DDoS attack, CISOs should consider the cost per hour of employee downtime.  **Remediation costs**  Scrambling to recover IT systems during and after a DDoS attack incurs additional labor costs, such as overtime or the need to use outside consultants. And, the fallout can affect more than just the IT staff; a DDoS attack and the associated downtime can impact a company’s public relations, and strain existing customer support teams who may be scrambling to respond to customer complaints or requests.  **Damage to brand reputation**  Some industries — such as gaming, hosting, datacenters, and financial services — rely heavily on their reputation for service availability. If customers can’t trust that a vendor will be consistently online and available, they can easily spread the word online, via Google Reviews or other social media channels. To acquire new customers in a highly competitive market a company must maintain a positive reputation.  **Loss of market share**  DDoS attacks can create customer churn. When an end user is denied access to Internet-facing applications, or if latency issues obstruct the user experience, it can impact the bottom line, because customers who can’t rely on a company to provide consistent service may go elsewhere to conduct their business.  **Ransom costs**  Although ransomware is a distinctly different type of cyber-attack, in recent years DDoS attackers have increasingly paired DDoS attacks with ransom demands, i.e., attackers threaten an organization by holding their files hostage and threatening to launch a DDoS attack on top of that, unless the organization pays an exorbitant bitcoin ransom fee. It’s not wise to pay a ransom fee, but let’s face it, sometimes companies do. It’s usually not something that makes the news, because organizations don’t want to publicly admit that they have paid a ransom. One exception was the Colonial Pipeline incident earlier this year, in which the company paid $5 million USD in ransom to be freed from its hostage position. And as was the case recently with Ireland’s Health service agency, sometimes cybercriminals test a system by launching DDoS attacks before they install ransomware. |

**Social-engineering**

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

|  |
| --- |
| Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information. |

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

|  |  |
| --- | --- |
| **Type** | **Description** |
| Telephone | Phone hacking involves any method where someone forces access into your phone or its communications. This can range from advanced security breaches to simply listening in on unsecured internet connections. It can also involve physical theft of your phone and forcibly hacking into it via methods like brute force. |
| Phishing | Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. |
| Shoulder Surfing | Shoulder surfing is a criminal practice where thieves steal your personal data by spying over your shoulder as you use a laptop, ATM, public kiosk or other electronic device in public. Despite the funny name, it's a security risk that can cause a financial wipeout. |



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

|  |
| --- |
| Shark Tank (like ‘The Apprentice’) television judge Barbara Corcoran was tricked in a nearly USD 400,000 phishing and social engineering scam in 2020. A cybercriminal impersonated her assistant and sent an email to the bookkeeper requesting a renewal payment related to real estate investments. He used an email address similar to the legitimate one. The fraud was only discovered after the bookkeeper sent an email to the assistant’s correct address asking about the transaction.  Democratic Party, 2016  One of the most iconic cases of social engineering is the United States presidential election in 2016. Spear phishing attacks led to the leak of emails and information from the Democratic Party that may have influenced the result of the election, with Donald Trump’s victory over Hillary Clinton. Hackers created a fake email from Gmail, inviting users, through a link, to change their passwords due to unusual activity. Fraudsters then had access to hundreds of emails containing sensitive information about the Clinton campaign.  Sony Pictures, 2014  After an investigation, the FBI pointed out that the cyberattack on Sony Pictures, in 2014, was the responsibility of the North Korea government. Thousands of files, including business agreements, financial documents and employees’ information, were stolen. Sony Pictures was targeted by spear phishing attacks. It appears employees were lured by fake Apple emails. |

**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** thedifferent 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**

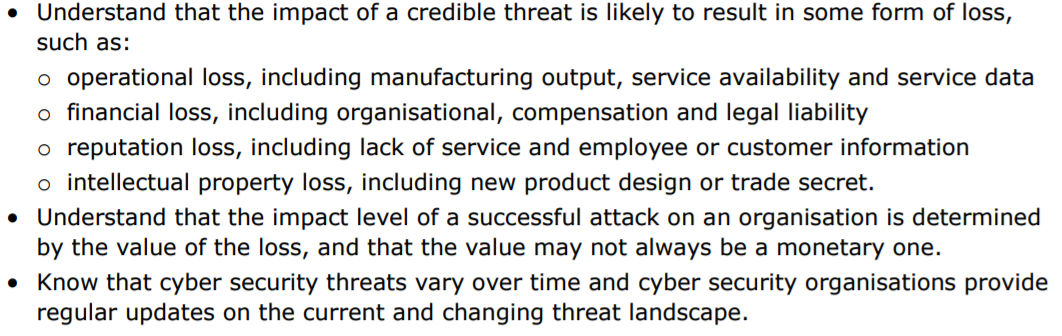
**Impacts of Credible Threats**

**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:**

****

**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)**

|  |
| --- |
| In 2017 the WannaCry ransomware hack hit companies worldwide including the NHS in the UK.  https://www.acronis.com/en-gb/articles/nhs-cyber-attack/  On Friday 12th May 2017, the NHS, was brought to a standstill for several days due to the WannaCry outbreak, affecting hospitals and GP surgeries across England and Scotland. Although the NHS was not specifically targeted, the global cyber-attack highlighted security vulnerabilities and resulted in the cancellation of thousands of appointments and operations, together with the frantic relocation of emergency patients from stricken emergency centres. Staff were also forced to revert to pen and paper and use their own mobiles after the attack affected key systems, including telephones.  The WannaCry ransomware exposed a **specific Microsoft Windows vulnerability**, not an attack on unsupported software. Most of the NHS devices infected with the ransomware, were found to have been running the supported, but unpatched, Microsoft Windows 7 operating system, hence the extremities of the cyber-attack. The ransomware also spread via the internet, including through the N3 network (the broadband network connecting all NHS sites in England), but fortunately, there were no instances of the ransomware spreading via NHSmail (the NHS email system).  NHS England reported at least 80 out of the 236 trusts were affected in addition to 603 primary care and other NHS organisations, including 595 GP practices. The Department, NHS England and the National Crime Agency reported that no NHS organisation paid the ransom, but the Department does not know how much disruption to services cost the NHS although estimates total £92m.  On Tuesday, March 14, 2017, Microsoft issued a security bulletin, which detailed the flaw and announced that patches had been released for all Windows versions that were currently supported at that time. The Department of Health was warned about the risks of cyber-attacks on the NHS a year before WannaCry and although it had work under way it did not formally respond with a written report until July 2017.  At the time of the attacks, the NHS was criticized for using outdated IT systems, including Windows XP, a 17-year-old operating system that could be vulnerable to cyber-attacks. In an unusual move, Microsoft released a WannaCry patch for unsupported systems such as Windows XP which Microsoft stopped supporting in 2014.  The NHS had not rehearsed for a national cyber-attack it was not immediately clear who should lead the response. There were problems with communications because emails were either infected or shut down to prevent the ransomware spreading. It’s clear that the disaster recovery plan at the time had not accounted for a cyber-attack of this scale nor were there communication contingencies if the main network was inaccessible. There was no clear relationship between trusts infected by WannaCry and the quality of their leadership, as rated by the Care Quality Commission.  The cyber-attack was stopped by an accidental kill switch discovered by Marcus Hutchins, a computer security researcher, by registering a domain that the ransomware was programmed to check. In the week after, the kill switch became the target of powerful botnets hoping to knock the domain offline and spark another outbreak.  Insufficient funding was highlighted as the main reason why the NHS was still supporting systems that did not reach cyber security standards. In December 2015, the NAO concluded that the continued deterioration in financial performance was not sustainable and that financial problems in the NHS were endemic. The WannaCry attack triggered a boost in investment from the government for cyber security in the NHS. This is a classic example of how a lack of understanding about the risks associated with cyber security vulnerabilities did not warrant a sufficient level of funding to meet the growing needs of large public institutions such as the NHS. According to a study by nature.com (<https://www.nature.com/articles/s41746-019-0161-6>) , the financial impact of the lower activity at the infected trusts during the WannaCry week was £5.9 m (95% confidence interval £3.6 m to £8.2 m), including £4m (£1.5 m to £6.6 m) in lost inpatient admissions, £0.6 m (£0.4 m to £0.8 m) from lost A&E activity, and £1.3 m (£0.9 m to £1.7 m) from cancelled outpatient appointments (Table [3](https://www.nature.com/articles/s41746-019-0161-6#Tab3)). Assuming that all trusts had been infected by WannaCry and affected to the same extend as the actually infected trusts, the total value of lost activity could have amounted to £35 m (£21.2 m to £48.8 m) in activity alone.Published examples of the effects resulting from IT failures, often seen in cyberattacks, include the loss of access to electronic health records and radiology and pathology results, drug dosing and drug administration errors, lack of contingency planning when traditional work patterns are affected, and, in the worst-case scenario, patient deaths due to incorrect data. |

**Topic 3: Deeper Learning Activities:**

**Operational Loss**

1. **Describe** what is meant by the term ‘operational loss.’ **(PASS)**

|  |
| --- |
| Operational Loss is loss due to errors, breaches, interruptions or damages—either intentional or accidental—caused by people, internal processes, systems or external events. |

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

|  |  |  |
| --- | --- | --- |
| **Type** | **Explanation** | **Impact on Organisation** |
| Manufacturing output | Operational losses in manufacturing can impact small and large companies, and they usually result from unexpected problems that arise during what should be a routine manufacturing process. | Time is added to the process, or the number of items produced falls short of goals, because of issues tied to machinery malfunctions, supply shortages, human error, weather and other issues that companies have varying abilities to control. |
| Service availability | Whether an organisation uses services from a third party company or from a unit within their own company, operating losses could be caused by service unavailability due to a catastrophic cyber event such as a ransomware attack. | An operating loss indicates that a company's core operations are not profitable and that changes need to be made to increase revenues, decrease costs, or both. This could mean that the company must make redundancies and reduce production levels. |
| Service data | Service Data includes product information included in feeds and transaction detail information such as unit prices and average basket values for websites. If this data is not available for a period of time or is unreliable due to data being obfuscated, operational losses could occur as the company will not know what stock lines to order, for example. | If the company is unable to access their service data they are unable to forecast what products or stock they will need to fulfil future orders. This will lead to a lack of stock (or over stock at a loss) and reputational risk to the company, leading to falling sales. |

**Financial Loss**

1. **Describe** what is meant by the term ‘financial loss.’ **(PASS)**

|  |
| --- |
| Financial loss means loss of money or decrease in financial value. |

1. **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 | Financial loss to an organisation includes credit loss (borrowers not paying back their loans), market loss (based on the likelihood that a security will fluctuate in value) and liquidity loss (the ability of a bank to meet its obligations to its depositors and counterparties). | Losses resulting from business operations have the opposite effect of profits. Companies facing a reduced market share from lower consumer demand or a downturn in the business cycle may be forced to reduce operational output. Consistent business losses may force the company into bankruptcy. |

**Reputational Loss**

1. **Describe** what is meant by the term ‘reputational loss.’ **(PASS)**

|  |
| --- |
| Reputational damage is the loss to financial capital, social capital and/or market share resulting from damage to a firm's reputation. This is often measured in lost revenue, increased operating, capital or regulatory costs, or destruction of shareholder value. |

1. **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 | Consistent inability to meet customer needs or falling short of customer expectations. | If the organisation consistently fails to meet customer expectations, then those customers will find an alternative provider. The consequence of this is a reduction in income and potential failure. |
| Loss of employee / customer information | A cyberattack could mean the exposure/loss of employee or customer information. | Customers leave  New customers look for alternatives  Shareholders sell their shares, causing a drop in share price and the value of the company. |

**Intellectual Property Loss**

1. **Describe** what is meant by the term ‘intellectual property loss.’ **(PASS)**

|  |
| --- |
| Intellectual Property results from any person's creativity and ideas. Such rights can exist in a book, a brand, an invention, a design or a song. ... These are often referred to as piracy, for a copyright infringement, intentional copying for registered designs, and counterfeiting, for a trademark infringement. |

1. **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 | The loss or theft of products developed by a business, through a process of imagining, creating and iterating, that solve users’ problems or address specific needs in a given market. These products will be the intellectual property of the business | Customers lose the reason for buying from the business and not from their competitors. The company will probably suffer financial and reputational loss which can be devastating and threaten its viability as a going concern. |
| Loss of trade secrets | The loss or theft of a type of intellectual property that includes formulas, practices, processes, designs, instruments, patterns, or compilations of information that have inherent economic value because they are not generally known (secret). | Loss of revenue and reward for those who made the inventions or who have purchased licenses to provide goods and services based on them, as well as of the jobs associated with those losses. Undermines the incentive for businesses to innovate, which will slow the development of new inventions to the detrimental of all. |

**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**

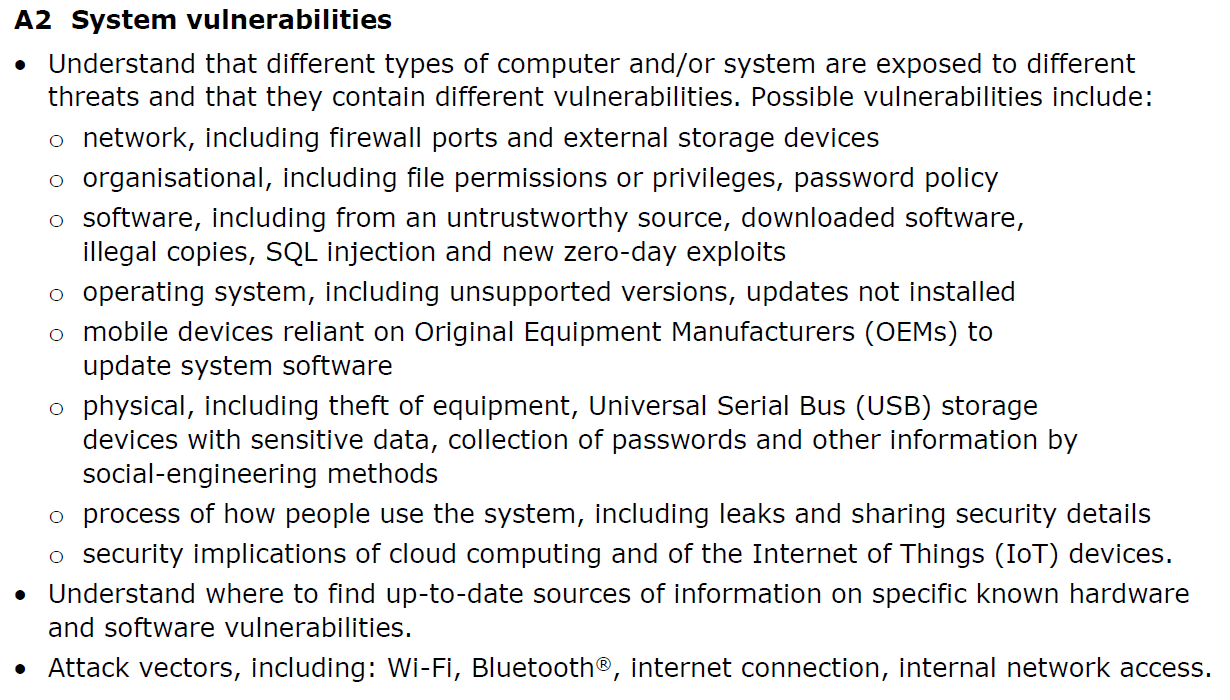
**System Vulnerabilities**

**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:**

****

**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)**

|  |
| --- |
| A network vulnerability is a weakness or flaw in software, hardware, or organizational processes, which when compromised by a threat, can result in a security breach. |

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

|  |
| --- |
| At the broadest level, network vulnerabilities fall into three categories: hardware-based, software-based, and human-based. **Hardware Issues** Any device on a network could be a security risk if it's not properly managed. Routers and security appliances are the front lines of defense, but they require proper use to work well. They need periodic firmware upgrades, and they should be replaced if patches are no longer available. Devices which IT management doesn't know about pose a risk. **Physical Device Security** One of the surest ways to break into a network is to gain unsupervised physical access to its devices. It doesn't take long to install malware on it. The intruder can download code from a prearranged location or copy it off a USB device.  The intruder can use the installed application as a backdoor or spyware. It can log keystrokes, attach itself to a logged-in account, or monitor internal traffic.  Personal physical access isn't strictly necessary. Criminals have mailed [**malicious USB drives**](https://www.redteamsecure.com/blog/usb-drop-attacks-the-danger-of-lost-and-found-thumb-drives) as "gifts" to potential victims. Once they're plugged in, they go to work installing malware.  Laptops, smartphones, and tablets are subject to theft. If it automatically connects to a VPN, a stolen device gets the thief inside the network. Any devices which regularly leave the office should be encrypted and have strong [**password**](https://www.redteamsecure.com/blog/if-your-password-looks-like-this-youre-in-big-trouble) protection. **Firewall Issues** The network firewall is its first line of defense. It can be a separate box, part of the router, or a virtual device. It should open ports for incoming access only when they're supposed to be. Default configurations sometimes install unnecessary services. Unknown, unmanaged services are security risks. Most machines on a network have no need to run a server, and they shouldn't be able to.  A good firewall protects against blacklisted IP addresses and mitigates DDoS attacks. Many network managers have moved beyond traditional firewalls to web application firewalls (WAFs), which recognize attack patterns and block such requests. They can keep out SQL injection attempts, cross-site scripting, and other attacks. They're also known as next-generation firewalls.  One firewall isn't always enough. Networks with internal servers benefit from segmentation, keeping the machines that hold sensitive information away from the network's edge. A secondary firewall for the protected segment further reduces the chance of exploitable vulnerabilities. **Wireless Access** Wi-Fi lets you connect devices easily without any wiring. This convenience is also its vulnerability. A poorly secured Wi-Fi network lets nearby devices connect, getting past the firewall. Some networks set up access points without a password, creating two kinds of risks. First, anyone nearby can gain access. Second, Wi-Fi without a password is unencrypted, and devices are readily available to read incoming and outgoing traffic.  Wi-Fi access points with the default configuration, with a widely used SSID and a password everyone knows, aren't any better. Passwords that are posted on walls for any visitor to read are in the same category. Default settings make it easier to spoof the network's Wi-Fi and lure users to rogue access points. Wi-Fi routers should have unique SSIDs and strong passwords.  "Shadow IT" access points are another security risk. If some areas have poor coverage, employees may connect their own hotspots and not protect them adequately. **IoT Devices** Too many devices for the [**Internet of Things (IoT)**](https://www.redteamsecure.com/blog/interview-with-cso-online-the-mirai-botnet-dyn-dns-and-iot-security) are cheaply made and have inadequate security. Such devices are vulnerable points in a network. It's often impossible to configure them or update their firmware. The best solution is to avoid insecure devices and buy from reputable vendors. If there's any doubt, the devices should be segregated into a subnet that has restricted access to the rest of the network and no access to the Internet. **Unauthorized Devices** That last category leads into the general problem of unauthorized devices on the network. Employees, just trying to do their job better, sometimes put their own computers on the network or attach devices to them. The IT department doesn't know about them, making it harder to manage the network. They're rarely up to company security standards.  BYOD policies are on the edge. The IT department should set standards for acceptable devices, including software to protect both the device and the network. Allowing just any mobile device to connect, including ones with antiquated operating systems, opens up serious risks.  Other user-owned devices may likewise be acceptable if they serve a work-related purpose, but the IT department should vet them, and their access to the network should be limited. If the network has strong security requirements, even allowing that may be too much.  Regardless of the policy, the IT department should keep an inventory of all devices and their IP addresses. It can't address the security issues in a device it doesn't know is there. **Software Security Vulnerabilities** Now we come to the software side of [**network security**](https://www.redteamsecure.com/penetration-testing/network-penetration-testing). Even a simple network has machines with multiple operating systems and many applications. If any of them have significant flaws, intruders will exploit them and gain access to the entire network. As with hardware, it's impossible to secure what you don't know is there. Leaving applications wide open for anyone to use without limitation makes it easy to exploit flaws. **Outdated And Buggy Software** A common [**application security**](https://www.redteamsecure.com/penetration-testing/web-application-penetration-testing) problem is outdated software with known vulnerabilities. If it isn't up to date, it's a target waiting for someone to aim at it. Regular network vulnerability scanning can discover these problems so that the IT managers can install the latest security patches.  It's easy to forget about software that falls into disuse but not fully remove it. Plug-ins and add-ons on content management systems are especially prone to this. IT managers should be aware of all software that can be affected over the Internet and either maintain it or get rid of it.  Some software, especially code written in-house, may have problems that aren't easily fixed. They're open to zero-day exploits. Sometimes there is no escape from this risk, but tight access control will limit the danger. **Unmanaged Software** Shadow IT is a problem with software as well as hardware. When employees put software on their machines without going through IT approval, they're likely to create a security risk. The software may be risky by its nature, and most likely no one is applying security patches. Users can even be fooled into installing a Trojan horse that will infiltrate the network.  Ironically, this sometimes happens because IT policies are too strict. If employees can't do what they need by going through channels, they'll find other ways to get their jobs done. IT people should work with employees to find secure solutions to their problems. **Security Vulnerabilities From Configuration** Carelessness when configuring software opens the way for security breaches. An application's defaults generally optimize usability ahead of security. Default names for directories, files, and accounts give attackers a head start. Protecting administrative accounts is especially important. Changing the name of each admin account and restricting access to it will keep the chances of unauthorized access low.  Having a virtual private network is valuable. Because employees can access it from anywhere, there's no need to expose internal-use software to the Internet. At the same time, a VPN has its own security risks. Configuring it securely is crucial. **User Issues** Engineers can manage hardware and software issues, but human ones often seem intractable. People make mistakes. They use weak passwords or don't guard them carefully. They open phishing messages. They click on links to malicious websites. Getting them to understand and follow a security policy is a challenge. **Authentication And Authorization** People aren't good at devising strong passwords. They create ones that are easy to guess, and they reuse ones they've previously created. They write them down where others can see them. Software can impose minimum password complexity requirements, but that helps only up to a point.  Multi-factor authentication greatly improves account security. Whether the second factor uses text messaging, a mobile application, or a specialized device, it keeps anyone from breaking in using just password theft.  Password managers encourage users to create hard-to-guess passwords since they don't have to remember them. A password generator and a password manager used together, provide good account protection. **Deception Of Users** Trickery is a favorite way of breaking network security. Phishing messages, scam phone calls, and lookalike sites are a few of the tricks for making people give up confidential information without knowing it. [**Security awareness**](https://www.redteamsecure.com/blog/6-low-cost-security-solutions) training and testing make employees more alert to such schemes and less likely to fall for them.  Still, anyone can be fooled some of the time. The principle of least privilege reduces the damage when they are. Accounts should have only the permissions necessary to do the job. Only a few accounts should have unlimited access. That way, someone who breaks into an account can't get as far.  (https://www.redteamsecure.com/blog/the-most-common-types-of-network-vulnerabilities) |

**Organisational Vulnerabilities**

1. **Describe** what is meant by the term ‘organisational vulnerability.’ **(PASS)**

|  |
| --- |
| Type your answer here. |

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

|  |
| --- |
| Type your answer here. |

**Software Vulnerabilities**

1. **Describe** what is meant by the term ‘software vulnerability.’ **(PASS)**

|  |
| --- |
| Type your answer here. |

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

|  |
| --- |
| Type your answer here. |

**Operating System Vulnerabilities**

1. **Describe** what is meant by the term ‘operating system vulnerability.’ **(PASS)**

|  |
| --- |
| Type your answer here. |

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

|  |
| --- |
| Type your answer here. |

**Mobile Device Vulnerabilities**

1. **Describe** what is meant by the term ‘mobile device vulnerability.’ **(PASS)**

|  |
| --- |
| Type your answer here. |

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

|  |
| --- |
| Type your answer here. |

**Physical Device Vulnerabilities**

1. **Describe** what is meant by the term ‘physical device vulnerability.’ **(PASS)**

|  |
| --- |
| Type your answer here. |

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

|  |
| --- |
| Type your answer here. |

**Cloud Computing Vulnerabilities**

1. **Describe** what is meant by the term ‘cloud computing vulnerability.’ **(PASS)**

|  |
| --- |
| Type your answer here. |

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

|  |
| --- |
| Type your answer here. |

**Attack Vector**

1. **Describe** what is meant by the term ‘Attack Vector.’ **(PASS)**

|  |
| --- |
| Type your answer here. |

1. **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**



1. **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**

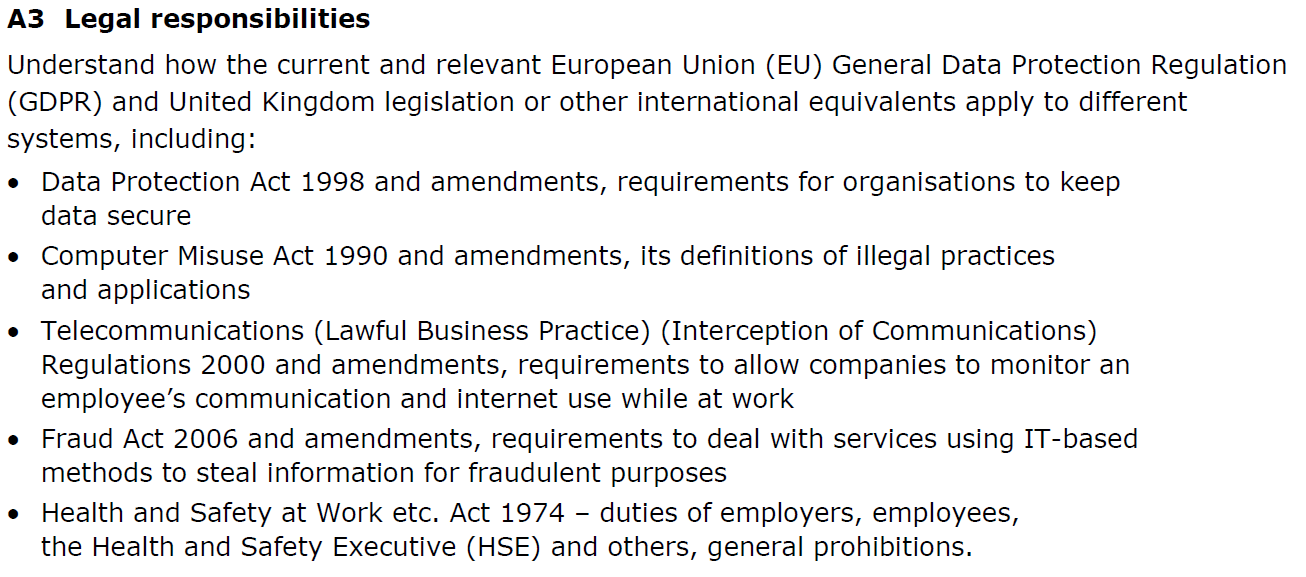
**Legal Responsibilities**

**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:**

****

**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. |

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

|  |
| --- |
| Type your answer here. |



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

|  |
| --- |
| Type your answer here. |



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

|  |
| --- |
| Type your answer here. |

**Computer Misuse Act 1990**

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

|  |
| --- |
| Type your answer here. |

1. **Explain** the legal definitions of ‘illegal practices’ under this law. **(PASS)**

|  |
| --- |
| Type your answer here. |



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

|  |
| --- |
| Type your answer here. |



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

|  |
| --- |
| Type your answer here. |

**Telecommunications Regulations 2000**

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

|  |
| --- |
| Type your answer here. |



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

|  |
| --- |
| Type your answer here. |

**Fraud Act 2006**

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

|  |
| --- |
| Type your answer here. |

1. **Describe** the legal definitions of ‘fraud’. **(PASS)**

|  |
| --- |
| Type your answer here. |



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

|  |
| --- |
| Type your answer here. |



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

|  |
| --- |
| Type your answer here. |

**Health & Safety at Work Act 1974**

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

|  |
| --- |
| Type your answer here. |



1. **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**

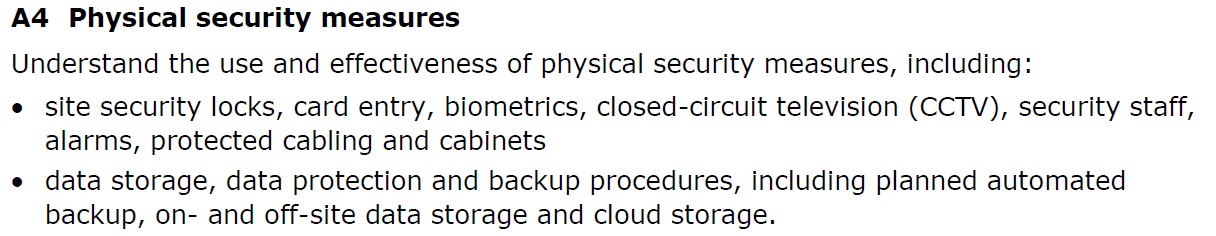
**Physical Security**

**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:**

****

**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. |

1. **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. |



1. **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. |

1. **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. |

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

|  |
| --- |
| Type your answer here. |

1. **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**

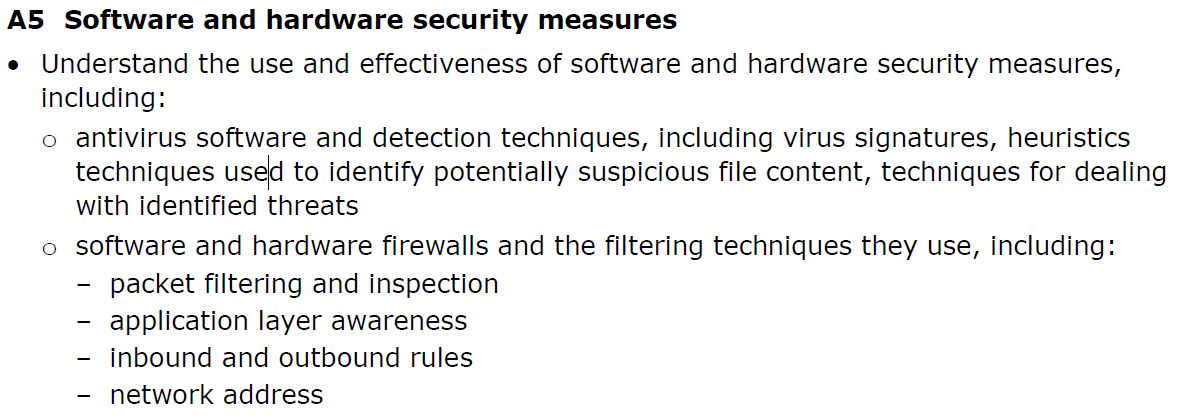
**Antivirus and Firewalls**

**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:**

****

**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. |

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

|  |
| --- |
| Type your answer here. |

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

|  |
| --- |
| Type your answer here. |

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

|  |
| --- |
| Type your answer here. |

**Firewalls**

1. **Describe** what is meant by the term ‘firewall’ software. **(PASS)**

|  |
| --- |
| Type your answer here. |

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

|  |
| --- |
| Type your answer here. |

1. **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. |

1. **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**

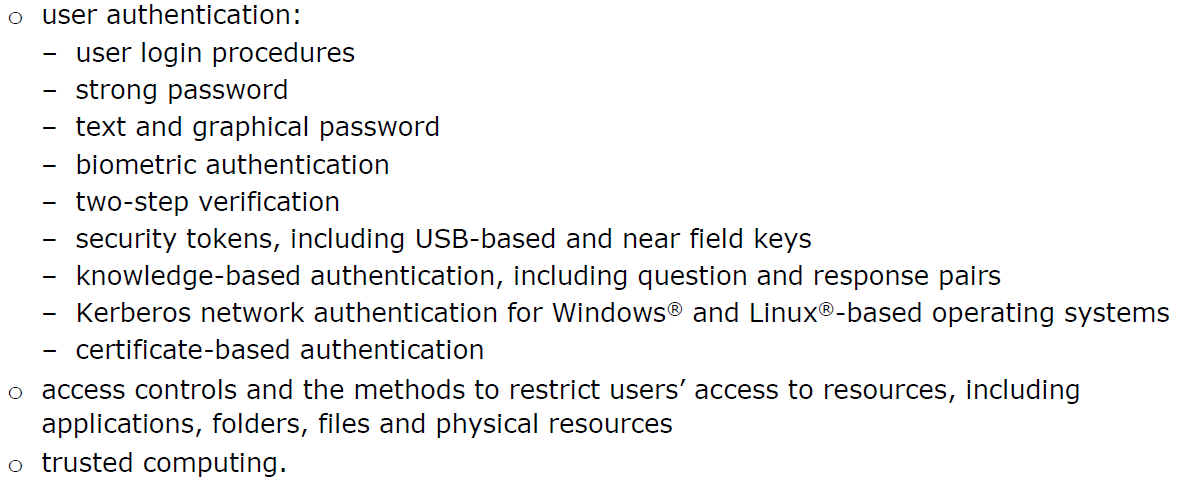
**User Authentication & Access Controls**

**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:**

****

**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. |

1. **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. |



1. **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**

1. **Describe** what is meant by the term ‘access control.’ **(PASS)**

|  |
| --- |
| Type your answer here. |

1. **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. |

1. **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**

1. **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**

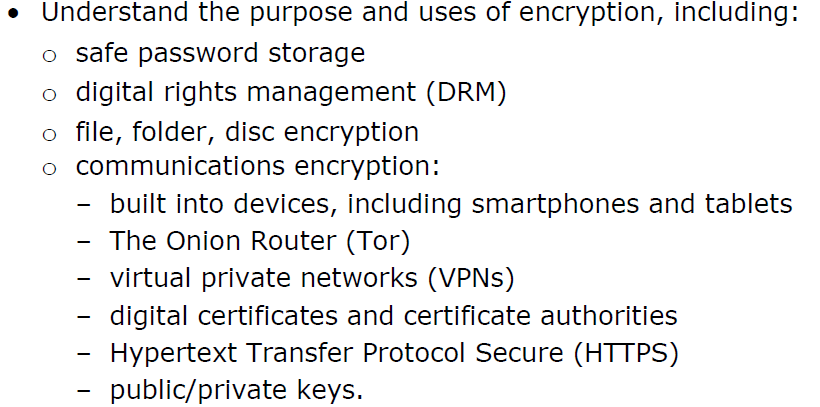
**Encryption**

**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:**

****

**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. |



1. **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. |



1. **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**

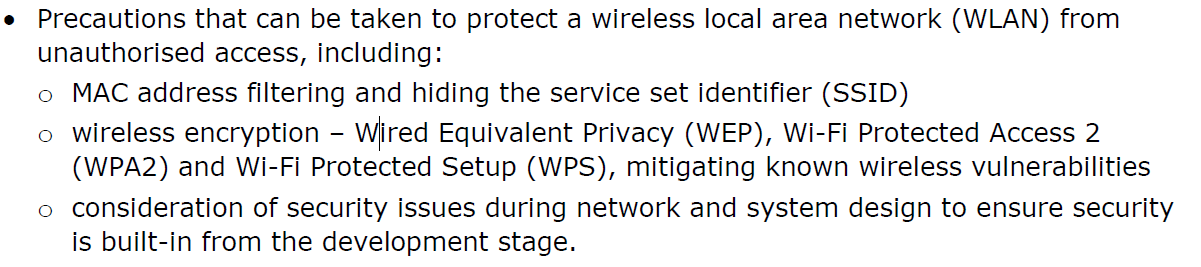
**Protecting Wireless Networks**

**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:**

****

**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. |



1. **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. |

1. **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**  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. |  |  |  |

**BTEC Level 3 National in Information Technology:**

**Unit 11**

Learner Workbook 2

**Learning Aim B:**

Use of networking architectures and principles for security

|  |  |
| --- | --- |
| 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](http://qualifications.pearson.com/en/qualifications/btec-nationals/information-technology-2016.html):   * Unit specification * Instructions for Conducting External Assessments (ICEA) * **Unit 11** Sample Assessment Materials (SAMs) * **Unit 11** Sample Marked Learner Work (SMLW) * **Unit 11** Scheme of work * **Unit 11** Delivery guide * **Unit 11** Scheme of work * **Unit 11** Administrative guide * **Unit 11** Templates * Any other new/updated documentation relevant to this unit   The information in this learner workbook is considered to be correct at the date of publication. |

**Start of Learning Aim B Review**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Topic** | **Checklist Item** | **Confidence** | | |
| **Low** | **Medium** | **High** |
| **Topic 1**  Network Types | I know the features of: LANs, WLANs, WANs, SANs, PANs and how to secure them. |  |  |  |
| I know the features of Intranets, Extranets, Internets and Cloud and how to secure them. |  |  |  |
| I know the difference between a Wired and Wireless network and why Wireless networks are more subject to attack. |  |  |  |
| **Topic 2**  Network Topologies | I know what is meant by the term physical topology. |  |  |  |
| I know what is meant by the following physical topologies: Star, Hierarchical, Wireless Mesh, Ad-hoc and how to secure them. |  |  |  |
| I know what is meant by the term logical topology and how to secure them. |  |  |  |
| **Topic 3**  Network Architectures | I know what is meant by the following network architectures: peer-to-peer, client-server and thin-client and how to secure them. |  |  |  |
| I know what is meant by the following modern trends: virtualisation, cloud computing, BYOD and SDN and how to secure them. |  |  |  |
| **Topic 4**  Network Hardware Components | I know different end-user devices and how to secure them. |  |  |  |
| I know different connectivity devices and how to secure them. |  |  |  |
| I know different connection devices and how to secure them. |  |  |  |
| I know different external media and storage and how to secure them. |  |  |  |
| **Topic 5**  Interpreting Network Diagrams | I can interpret the type of network used on a network diagram. |  |  |  |
| I can interpret the topology of a network on a network diagram. |  |  |  |
| I can interpret the architecture of a network on a network diagram. |  |  |  |
| I can interpret the hardware devices used on a network diagram. |  |  |  |

*Continued on the next page…..*

**Start of Learning Aim B Review Continued…**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Topic** | **Checklist Item** | **Confidence** | | |
| **Low** | **Medium** | **High** |
| **Topic 6**  Network Software Components | I know what is meant by the term network operating system and the security features they contain. |  |  |  |
| I know what is meant by the term network monitoring software and the security features they contain. |  |  |  |
| I know what is meant by the term network application software and the security features they contain. |  |  |  |
| **Topic 7**  Network Infrastructure & Resources | I know what is meant by the following network configuration services: TCP/IP, Ports, Packets, NAT |  |  |  |
| I know what is meant by the following network infrastructure services: DNS, DS, Authentication Services, DHCP, Routing and Remote Access |  |  |  |
| I know what is meant by the following resource services: File/Print and Web/Mail/Communications Services |  |  |  |

**Topic 1**

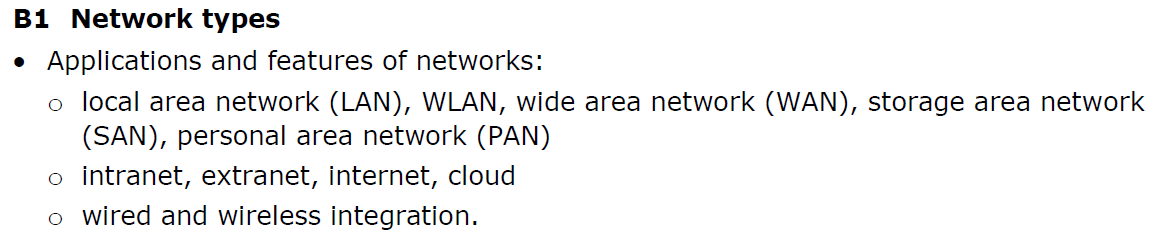
**Network Types**

**Topic 1: Network Types**

**Topic 1: Topic Objectives:**

* **Pass – Describe** the different applications and features of different types of networks.
* **Merit – Explain** potential security implications that each type of network faces.
* **Distinction- Discuss** methods that can be used to reduce the security risks faced by these different types networks.

**Topic 1: Specification Coverage:**

****

**Topic 1: Introductory Task:**

A network is two or more devices that are connected together to allow them to communicate.

However have you ever wondered how networks are structured? Have you ever come across the following terms: LAN, WAN, SAN, PAN?

Lookup what these acronyms stand for. **(PASS)**

|  |
| --- |
| Type your answer here. |

**Topic 1: Deeper Learning Activities:**

**Wired vs Wireless Networks**

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

|  |
| --- |
| Type your answer here. |

**LANs, WANs, SANs and PANs**

1. **Describe** the different features of the following networks and draw a diagram to illustrate how they are structured. **(PASS)**

|  |  |  |
| --- | --- | --- |
| **Type** | **Features** | **Diagram** |
| Local Area Network (LAN) | Type your answer here. | Draw your diagram here. |
| Wireless Local Area Network (WLAN) | Type your answer here. | Draw your diagram here. |
| Wide Area Network (WAN) | Type your answer here. | Draw your diagram here. |
| Storage Area Network  (SAN) | Type your answer here. | Draw your diagram here. |
| Personal Area Network (PAN) | Type your answer here. | Draw your diagram here. |

1. **Research** and **explain** potential security implications that each type of network faces **(MERIT)** and **discuss** methods that can be used to reduce them. **(DISTINCTION)**

|  |  |  |
| --- | --- | --- |
| **Type** | **Security Implications** | **Solutions** |
| Local Area Network (LAN) | Type your answer here. | Type your answer here. |
| Wireless Local Area Network (WLAN) | Type your answer here. | Type your answer here. |
| Wide Area Network (WAN) | Type your answer here. | Type your answer here. |
| Storage Area Network  (SAN) | Type your answer here. | Type your answer here. |
| Personal Area Network (PAN) | Type your answer here. | Type your answer here. |

**Intranets, extranets, internet and the cloud**

1. **Describe** the different features of the following networks. **(PASS)**

|  |  |
| --- | --- |
| **Type** | **Features** |
| Intranet | Type your answer here. |
| Extranet | Type your answer here. |
| Internet | Type your answer here. |
| Cloud | Type your answer here. |



1. **Research** and **explain** potential security implications that each type of network faces **(MERIT)** and **discuss** methods that can be used to reduce them. **(DISTINCTION)**

|  |  |  |
| --- | --- | --- |
| **Type** | **Security Implications** | **Solutions** |
| Intranet | Type your answer here. | Type your answer here. |
| Extranet | Type your answer here. | Type your answer here. |
| Internet | Type your answer here. | Type your answer here. |
| Cloud | Type your answer here. | Type your answer here. |

**Topic 1: Progress Check**

|  |  |  |
| --- | --- | --- |
| **Topic** | **Confident**  **(Tick)** | **Need to revisit**  **(Tick)** |
| I know the features of: LANs, WLANs, WANs, SANs, PANs and how to secure them. |  |  |
| I know the features of Intranets, Extranets, Internets and Cloud and how to secure them. |  |  |
| I know the difference between a Wired and Wireless network and why Wireless networks are more subject to attack. |  |  |

**Topic 1: Grade Yourself**

|  |  |
| --- | --- |
| **Grade Description** | **The statement that best describes my progress is…** |
| **Pass – Describe** the different applications and features of different types of networks. |  |
| **Merit – Explain** potential security implications that each type of network faces. |  |
| **Distinction- Discuss** methods that can be used to reduce the security risks faced by these different types networks. |  |
| **My strengths…..**  Type your answer here. | |
| **My areas for development…**  Type your answer here. | |

**Topic 2**

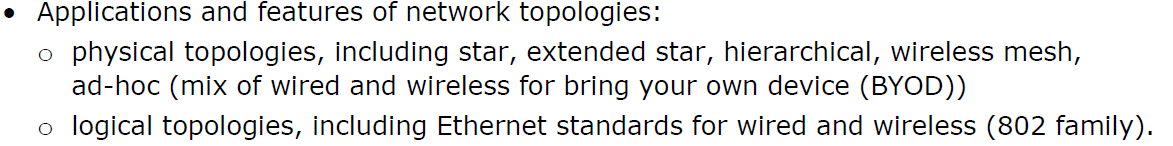
**Network Topologies**

**Topic 2: Network Topologies**

**Topic 2: Topic Objectives:**

* **Pass – Describe** the different applications and features of different network topologies.
* **Merit – Explain** potential security implications that each type of network topology faces.
* **Distinction- Discuss** methods that can be used to reduce the security risks faced by these network topologies.

**Topic 2: Specification Coverage:**

****

**Topic 2: Introductory Task:**

Lookup the term ‘network topology.’

How many network topologies can you find? What do they look like? **(PASS)**

|  |
| --- |
| Type your answer here. |

**Topic 2: Deeper Learning Activities:**

**Physical Topologies**

1. **Describe** what is meant by the term ‘physical topology.’ **(PASS)**

|  |
| --- |
| Type your answer here. |

1. **Describe** the different features of the following network topologies and draw a diagram to illustrate how they look. **(PASS)**

|  |  |  |
| --- | --- | --- |
| **Type** | **Features** | **Diagram** |
| Star / extended star | Type your answer here. | Draw your diagram here. |
| Hierarchical | Type your answer here. | Draw your diagram here. |
| Mesh | Type your answer here. | Draw your diagram here. |
| Ad-hoc | Type your answer here. | Draw your diagram here. |



1. **Research** and **explain** potential security implications that each type of network topology faces **(MERIT)** and **discuss** methods that can be used to reduce them. **(DISTINCTION)**

|  |  |  |
| --- | --- | --- |
| **Type** | **Security Implications** | **Solutions** |
| Star / extended star | Type your answer here. | Type your answer here. |
| Hierarchical | Type your answer here. | Type your answer here. |
| Mesh | Type your answer here. | Type your answer here. |
| Ad-hoc | Type your answer here. | Type your answer here. |

**Logical Topologies**

1. **Describe** what is meant by the term ‘logical topology.’ **(PASS)**

|  |
| --- |
| Type your answer here. |

1. **Describe** the Ethernet standards for wired and wireless networks (802 family). **(PASS)**

|  |
| --- |
| Type your answer here. |



1. **Research and explain** potential security implications that logical topologies face **(MERIT)** and **discuss** methods that can be used to reduce them. **(DISTINCTION)**

|  |
| --- |
| Type your answer here. |

**Topic 2: Progress Check**

|  |  |  |
| --- | --- | --- |
| **Topic** | **Confident**  **(Tick)** | **Need to revisit**  **(Tick)** |
| I know what is meant by the term physical topology. |  |  |
| I know what is meant by the following physical topologies: Star, Hierarchical, Wireless Mesh, Ad-hoc and how to secure them. |  |  |
| I know what is meant by the term logical topology and how to secure them. |  |  |

**Topic 2: Grade Yourself**

|  |  |
| --- | --- |
| **Grade Description** | **The statement that best describes my progress is…** |
| **Pass – Describe** the different applications and features of different network topologies. |  |
| **Merit – Explain** potential security implications that each type of network topology faces. |  |
| **Distinction- Discuss** methods that can be used to reduce the security risks faced by these network topologies. |  |
| **My strengths…..**  Type your answer here. | |
| **My areas for development…**  Type your answer here. | |

**Topic 3**

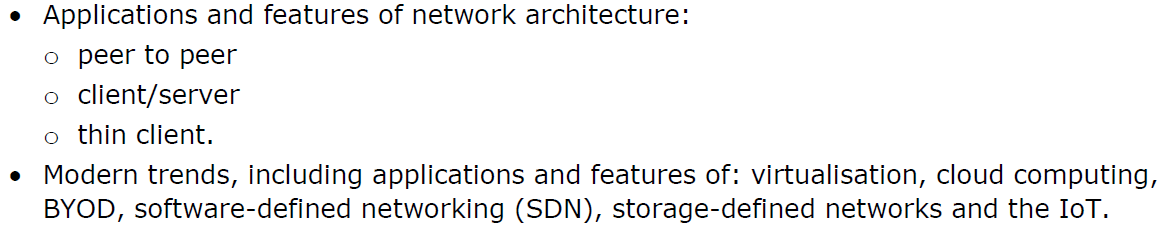
**Network Architectures**

**Topic 3: Network Architectures & Network Diagrams**

**Topic 3: Topic Objectives:**

* **Pass – Describe** the different applications and features of different network architectures.
* **Merit – Explain** potential security implications that each type of network architecture faces.
* **Distinction- Discuss** methods that can be used to reduce the security risks faced by these network architectures and how to secure them.

**Topic 3: Specification Coverage:**

****

**Topic 3: Introductory Task:**

Your teacher may give you a network diagram that is used in your centre.

What type of network does your centre have? What topology or topologies does your centre use? **(PASS)**

|  |
| --- |
| Type your answer here. |

**Topic 3: Deeper Learning Activities:**

**Network Architectures**

1. **Describe** what is meant by the term ‘network architecture.’ **(PASS)**

|  |
| --- |
| Type your answer here. |

1. **Describe** the different features of the following network architectures and draw a diagram to illustrate how they are structured. **(PASS)**

|  |  |  |
| --- | --- | --- |
| **Type** | **Features** | **Diagram** |
| Peer-to-Peer | Type your answer here. | Draw your diagram here. |
| Client-Server | Type your answer here. | Draw your diagram here. |
| Thin Client | Type your answer here. | Draw your diagram here. |



1. **Research** and **explain** potential security implications that each type of network architecture faces **(MERIT)** and **discuss** methods that can be used to reduce them. **(DISTINCTION)**

|  |  |  |
| --- | --- | --- |
| **Type** | **Security Implications** | **Solutions** |
| Peer-to-Peer | Type your answer here. | Type your answer here. |
| Client-Server | Type your answer here. | Type your answer here. |
| Thin Client | Type your answer here. | Type your answer here. |

**Modern Trends**

1. **Research** and **describe** the different features of the following modern network trends. **(PASS)**

|  |  |
| --- | --- |
| **Type** | **Features** |
| Virtualisation | Type your answer here. |
| Cloud Computing | Type your answer here. |
| Bring Your Own Device (BYOD) | Type your answer here. |
| Software-Defined Networking (SDN) | Type your answer here. |
| Storage-Defined Networks | Type your answer here. |



1. **Research** and **explain** potential security implications that each modern trend faces **(MERIT)** and **discuss** methods that can be used to reduce them. **(DISTINCTION)**

|  |  |  |
| --- | --- | --- |
| **Type** | **Security Implications** | **Solutions** |
| Virtualisation | Type your answer here. | Type your answer here. |
| Cloud Computing | Type your answer here. | Type your answer here. |
| Bring Your Own Device (BYOD) | Type your answer here. | Type your answer here. |
| Software-Defined Networking (SDN) | Type your answer here. | Type your answer here. |
| Storage-Defined Networks | Type your answer here. | Type your answer here. |

**Topic 3: Progress Check**

|  |  |  |
| --- | --- | --- |
| **Topic** | **Confident**  **(Tick)** | **Need to revisit**  **(Tick)** |
| I know what is meant by the following network architectures: peer-to-peer, client-server and thin-client and how to secure them. |  |  |
| I know what is meant by the following modern trends: virtualisation, cloud computing, BYOD and SDN and how to secure them. |  |  |

**Topic 3: Grade Yourself**

|  |  |
| --- | --- |
| **Grade Description** | **The statement that best describes my progress is…** |
| **Pass – Describe** the different applications and features of different network architectures. |  |
| **Merit – Explain** potential security implications that each type of network architecture faces. |  |
| **Distinction- Discuss** methods that can be used to reduce the security risks faced by these network architectures and how to secure them. |  |
| **My strengths…..**  Type your answer here. | |
| **My areas for development…**  Type your answer here. | |

**Topic 4**

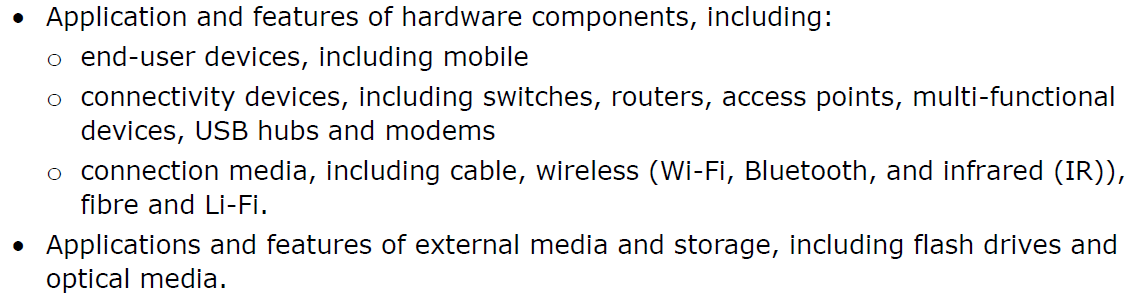
**Network Hardware Components**

**Topic 4: Network Hardware Components**

**Topic 4: Topic Objectives:**

* **Pass – Describe** the different applications and features of different end-user devices, connectivity devices, connection media and external storage devices.
* **Merit – Describe** different methods that can be used to secure these components.
* **Distinction - Discuss** the security implications of different network hardware components and how to secure them.

**Topic 4: Specification Coverage:**

****

**Topic 4: Introductory Task:**

Your teacher or network manager may give you a tour of your centre showing you the different **hardware** that makes up your network.

Make a note of what **hardware** you see what protection methods are in place to protect them. **(PASS)**

|  |
| --- |
| Type your answer here. |

**Topic 4: Deeper Learning Activities:**

**Connectivity Devices**

1. **Describe** the different features of the following connectivity devices. **(PASS)**

|  |  |
| --- | --- |
| **Type** | **Features** |
| Switches | Type your answer here. |
| Routers | Type your answer here. |
| Access points | Type your answer here. |
| Multi-functional devices | Type your answer here. |
| USB hubs | Type your answer here. |
| Modems | Type your answer here. |



1. **Research** and **explain** potential security implications that each device has **(MERIT)** and **discuss** methods that can be used to reduce them. **(DISTINCTION)**

|  |  |  |
| --- | --- | --- |
| **Type** | **Security Implications** | **Solutions** |
| Switches | Type your answer here. | Type your answer here. |
| Routers | Type your answer here. | Type your answer here. |
| Access points | Type your answer here. | Type your answer here. |
| Multi-functional devices | Type your answer here. | Type your answer here. |
| USB hubs | Type your answer here. | Type your answer here. |
| Modems | Type your answer here. | Type your answer here. |

**Connection Media Devices**

1. **Describe** the different features of the following connection media devices. **(PASS)**

|  |  |
| --- | --- |
| **Type** | **Features** |
| Cable | Type your answer here. |
| Wi-Fi | Type your answer here. |
| Bluetooth | Type your answer here. |
| Infrared | Type your answer here. |
| Fibre | Type your answer here. |
| Li-Fi | Type your answer here. |



1. **Research** and **explain** potential security implications that each device has **(MERIT)** and **discuss** methods that can be used to reduce them. **(DISTINCTION)**

|  |  |  |
| --- | --- | --- |
| **Type** | **Security Implications** | **Solutions** |
| Cable | Type your answer here. | Type your answer here. |
| Wi-Fi | Type your answer here. | Type your answer here. |
| Bluetooth | Type your answer here. | Type your answer here. |
| Infrared | Type your answer here. | Type your answer here. |
| Fibre | Type your answer here. | Type your answer here. |
| Li-Fi | Type your answer here. | Type your answer here. |

**External Media Devices**

1. **Describe** the different features of the following external media devices. **(PASS)**

|  |  |
| --- | --- |
| **Type** | **Features** |
| Flash drives | Type your answer here. |
| Optical media | Type your answer here. |



1. **Research** and **explain** potential security implications that each device has **(MERIT)** and **discuss** methods that can be used to reduce them. **(DISTINCTION)**

|  |  |  |
| --- | --- | --- |
| **Type** | **Security Implications** | **Solutions** |
| Flash drives | Type your answer here. | Type your answer here. |
| Optical media | Type your answer here. | Type your answer here. |

**Topic 4: Progress Check**

|  |  |  |
| --- | --- | --- |
| **Topic** | **Confident**  **(Tick)** | **Need to revisit**  **(Tick)** |
| I know different end-user devices and how to secure them. |  |  |
| I know different connectivity devices and how to secure them. |  |  |
| I know different connection devices and how to secure them. |  |  |
| I know different external media and storage and how to secure them. |  |  |

**Topic 4: Grade Yourself**

|  |  |
| --- | --- |
| **Grade Description** | **The statement that best describes my progress is…** |
| **Pass – Describe** the different applications and features of different end-user devices, connectivity devices, connection media and external storage devices. |  |
| **Merit – Describe** different methods that can be used to secure these components. |  |
| **Distinction - Discuss** the security implications of different network hardware components and how to secure them. |  |
| **My strengths…..**  Type your answer here. | |
| **My areas for development…**  Type your answer here. | |

**Topic 5**

**Interpreting Network Diagrams**

**Topic 5: Interpreting Network Diagrams**

**Topic 5: Topic Objectives:**

* **Pass – Interpret some** features of a network diagram.
* **Merit – Interpret most** features of a network diagram.
* **Distinction – Interpret all** features of a network diagram justify the decisions made by the organisation.

**Topic 5: Specification Coverage:**

****

**Interpreting Network Diagrams**

Research **three** different network diagrams on the internet.

Interpret each network by stating:

* What **type** of network is used (e.g. LAN, WAN etc)
* What **topology** is used (e.g. Star, Mesh etc)
* What **architecture** is used (e.g. Peer-to-Peer, Client-Server etc)
* What components are used (e.g. Servers, Switches etc)
* The **security weaknesses** in the design.

**Diagram 1:**

|  |
| --- |
| **Diagram here**  Put your network diagram here.  **Interpretation**  Type your answer here. |

**Diagram 2:**

|  |
| --- |
| **Diagram here**  Put your network diagram here.  **Interpretation**  Type your answer here. |

**Diagram 3:**

|  |
| --- |
| **Diagram here**  Put your network diagram here.  **Interpretation**  Type your answer here. |

**Topic 5: Progress Check**

|  |  |  |
| --- | --- | --- |
| **Topic** | **Confident**  **(Tick)** | **Need to revisit**  **(Tick)** |
| I can interpret the type of network used on a network diagram. |  |  |
| I can interpret the topology of a network on a network diagram. |  |  |
| I can interpret the architecture of a network on a network diagram. |  |  |
| I can interpret the hardware devices used on a network diagram. |  |  |

**Topic 5: Grade Yourself**

|  |  |
| --- | --- |
| **Grade Description** | **The statement that best describes my progress is…** |
| **Pass – Interpret some** features of a network diagram. |  |
| **Merit – Interpret most** features of a network diagram. |  |
| **Distinction – Interpret all** features of a network diagram justify the decisions made by the organisation. |  |
| **My strengths…..**  Type your answer here. | |
| **My areas for development…**  Type your answer here. | |

**Topic 6**

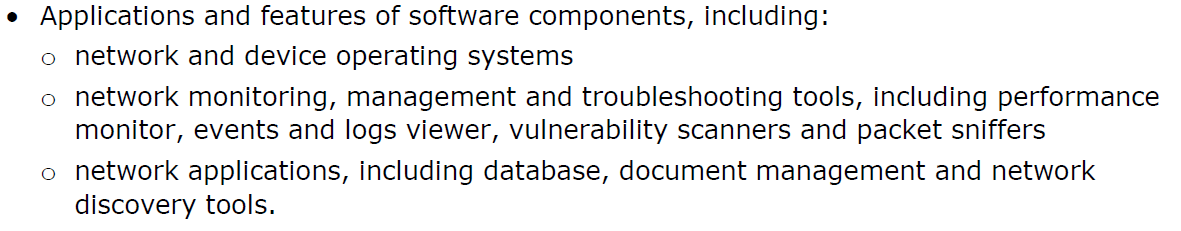
**Network Software Components**

**Topic 6: Network Software Components**

**Topic 6: Topic Objectives:**

* **Pass – Describe** the different applications and features of different network operating systems, network monitoring software and network applications.
* **Merit – Explain** how this software can be used to reduce security threats.
* **Distinction – Evaluate** the effectiveness of different network software and how well they keep networks safe.

**Topic 6: Specification Coverage:**

****

**Topic 6: Introductory Task:**

Your teacher or network manager may give you a talk about the different **network software** that is used to successfully manage your network and its users.

Make a note of what **network software** is mentioned and what it does. **(PASS)**

|  |
| --- |
| Type your answer here. |

**Topic 6: Deeper Learning Activities:**

**Network Operating Systems**

1. **Describe** what is meant by the term ‘Network Operating System.’ **(PASS)**

|  |
| --- |
| Type your answer here. |



1. **Research** and **describe** the different built-in security tools **(PASS)** and **explain** and how they can be used to reduce security threats. **(MERIT)**

|  |
| --- |
| Type your answer here. |

1. **Evaluate** how effectively network operating systems reduce security threats. **(DISTINCTION)**

|  |
| --- |
| Type your answer here. |

**Networking Monitoring Software**

1. **Describe** what is meant by the term ‘Network Monitoring Software.’ **(PASS)**

|  |
| --- |
| Type your answer here. |



1. **Research** and **describe** the different features of the following network monitoring software **(PASS)** and how they can be used to reduce security threats. **(MERIT)**

|  |  |  |
| --- | --- | --- |
| **Type** | **Features** | **Threat Reduction** |
| Troubleshooting tools | Type your answer here. | Type your answer here. |
| Performance monitoring | Type your answer here. | Type your answer here. |
| Events monitoring | Type your answer here. | Type your answer here. |
| Logs viewer | Type your answer here. | Type your answer here. |
| Vulnerability scanners | Type your answer here. | Type your answer here. |
| Packet sniffers | Type your answer here. | Type your answer here. |

1. **Evaluate** how effectively the following networking monitoring software reduces security threats. **(DISTINCTION)**

|  |  |
| --- | --- |
| **Type** | **Effectiveness** |
| Troubleshooting tools | Type your answer here. |
| Performance monitoring | Type your answer here. |
| Events monitoring | Type your answer here. |
| Logs viewer | Type your answer here. |
| Vulnerability scanners | Type your answer here. |
| Packet sniffers | Type your answer here. |

**Network Application Software**

1. **Describe** what is meant by the term ‘Network Application Software.’ **(PASS)**

|  |
| --- |
| Type your answer here. |



1. **Research** and **describe** the different features of the following network application software **(PASS)** and how they can be used to reduce security threats. **(MERIT)**

|  |  |  |
| --- | --- | --- |
| **Type** | **Features** | **Threat Reduction** |
| Database management | Type your answer here. | Type your answer here. |
| Document management | Type your answer here. | Type your answer here. |
| Network discovery tools | Type your answer here. | Type your answer here. |

1. **Evaluate** how effectively the following networking application software reduces security threats. **(DISTINCTION)**

|  |  |
| --- | --- |
| **Type** | **Effectiveness** |
| Database management | Type your answer here. |
| Document management | Type your answer here. |
| Network discovery tools | Type your answer here. |

**Topic 6: Progress Check**

|  |  |  |
| --- | --- | --- |
| **Topic** | **Confident**  **(Tick)** | **Need to revisit**  **(Tick)** |
| I know what is meant by the term network operating system and the security features they contain. |  |  |
| I know what is meant by the term network monitoring software and the security features they contain. |  |  |
| I know what is meant by the term network application software and the security features they contain. |  |  |

**Topic 6: Grade Yourself**

|  |  |
| --- | --- |
| **Grade Description** | **The statement that best describes my progress is…** |
| **Pass – Describe** the different applications and features of different network operating systems, network monitoring software and network applications. |  |
| **Merit – Explain** how this software can be used to reduce security threats. |  |
| **Distinction – Evaluate** the effectiveness of different network software components and how well they keep networks safe. |  |
| **My strengths…..**  Type your answer here. | |
| **My areas for development…**  Type your answer here. | |

**Topic 7**

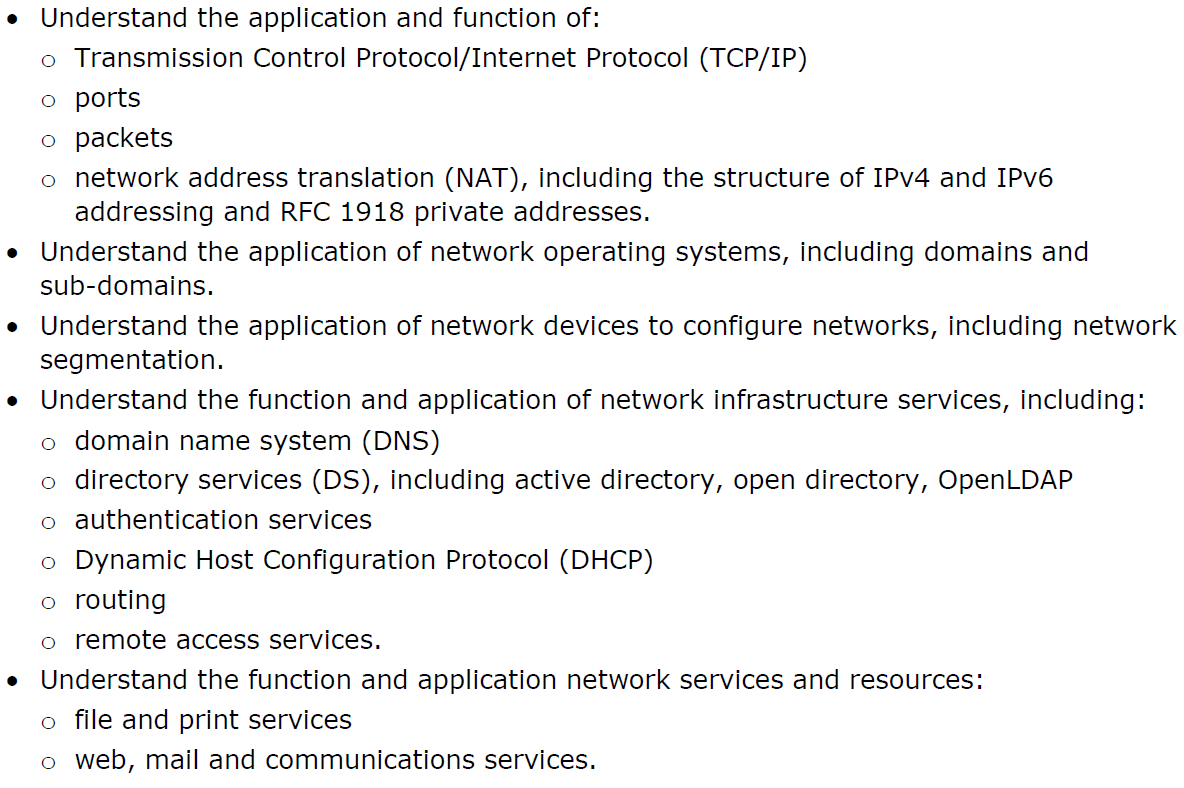
**Network Infrastructure & Resources**

**Topic 7: Network Infrastructure & Resources**

**Topic 7: Topic Objectives:**

* **Pass – Describe** the application and function of different network configurations, network infrastructures and resource services.
* **Merit – Explain** when each network configuration, infrastructure and resource service would be used.
* **Distinction- Discuss** how different network configuration, infrastructures and resource services are used within a specific organisational network.

**Topic 7: Specification Coverage:**

****

**Topic 7: Introductory Task:**

Your teacher or network manager may give you a talk about the different **network services** that are used to successfully manage the network and its users at your centre.

Make a note of what **network services** are mentioned and what they do. **(PASS)**

|  |
| --- |
| Type your answer here. |

**Topic 7: Deeper Learning Activities:**

**Network Configuration Services**

1. **Research** and **describe** the different network configuration services below **(PASS)** and **explain** why they would be used. **(MERIT)**

|  |  |  |
| --- | --- | --- |
| **Type** | **Description** | **Why Are They Used?** |
| Internet Protocol (TCP/IP) | Type your answer here. | Type your answer here. |
| Ports | Type your answer here. | Type your answer here. |
| Packets | Type your answer here. | Type your answer here. |
| Network Address Translation (NAT) | Type your answer here. | Type your answer here. |
| Domains | Type your answer here. | Type your answer here. |
| Sub-domains | Type your answer here. | Type your answer here. |
| Network segmentation | Type your answer here. | Type your answer here. |

**Network Infrastructure Services**

1. **Research and describe** the different infrastructure services below **(PASS)** and **explain** why they would be used. **(MERIT)**

|  |  |  |
| --- | --- | --- |
| **Type** | **Description** | **Why Are They Used?** |
| Domain Name System (DNS) | Type your answer here. | Type your answer here. |
| Directory Services (DS), | Type your answer here. | Type your answer here. |
| Authentication Services | Type your answer here. | Type your answer here. |
| Dynamic Host Configuration Protocol (DHCP) | Type your answer here. | Type your answer here. |
| Routing | Type your answer here. | Type your answer here. |
| Remote Access Services | Type your answer here. | Type your answer here. |

**Resource Services**

1. **Research** and **describe** the different resource services below **(PASS)** and **explain** when they would be used. **(MERIT)**

|  |  |  |
| --- | --- | --- |
| **Type** | **Description** | **Why Are They Used?** |
| File services | Type your answer here. | Type your answer here. |
| Print services | Type your answer here. | Type your answer here. |
| Web services | Type your answer here. | Type your answer here. |
| Mail services | Type your answer here. | Type your answer here. |
| Communications services | Type your answer here. | Type your answer here. |

**Distinction Task**

1. **Research** a network.

This can be the network used within your centre or another network. For your chosen network **discuss** how the organisation uses the following services to successfully manage their network and its users:

* Network Configuration Services
* Network Infrastructure Services
* Resource Services **(DISTINCTION)**

|  |
| --- |
| Type your answer here. |

**Topic 7: Progress Check**

|  |  |  |
| --- | --- | --- |
| **Topic** | **Confident**  **(Tick)** | **Need to revisit**  **(Tick)** |
| I know what is meant by the following network configuration services: TCP/IP, Ports, Packets, NAT |  |  |
| I know what is meant by the following network infrastructure services: DNS, DS, Authentication Services, DHCP, Routing and Remote Access |  |  |
| I know what is meant by the following resource services: File/Print and Web/Mail/Communications Services |  |  |

**Topic 7: Grade Yourself**

|  |  |
| --- | --- |
| **Grade Description** | **The statement that best describes my progress is…** |
| **Pass – Describe** the application and function of different network configurations, network infrastructures and resource services. |  |
| **Merit – Explain** when each network configuration, infrastructure and resource service would be used. |  |
| **Distinction- Discuss** how different network configuration, infrastructures and resource services are used within a specific organisational network. |  |
| **My strengths…..**  Type your answer here. | |
| **My areas for development…**  Type your answer here. | |

**End of Learning Aim B Review**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Topic** | **Checklist Item** | **Confidence** | | |
| **Low** | **Medium** | **High** |
| **Topic 1**  Network Types | I know the features of: LANs, WLANs, WANs, SANs, PANs and how to secure them. |  |  |  |
| I know the features of Intranets, Extranets, Internets and Cloud and how to secure them. |  |  |  |
| I know the difference between a Wired and Wireless network and why Wireless networks are more subject to attack. |  |  |  |
| **Topic 2**  Network Topologies | I know what is meant by the term physical topology. |  |  |  |
| I know what is meant by the following physical topologies: Star, Hierarchical, Wireless Mesh, Ad-hoc and how to secure them. |  |  |  |
| I know what is meant by the term logical topology and how to secure them. |  |  |  |
| **Topic 3**  Network Architectures | I know what is meant by the following network architectures: peer-to-peer, client-server and thin-client and how to secure them. |  |  |  |
| I know what is meant by the following modern trends: virtualisation, cloud computing, BYOD and SDN and how to secure them. |  |  |  |
| **Topic 4**  Network Hardware Components | I know different end-user devices and how to secure them. |  |  |  |
| I know different connectivity devices and how to secure them. |  |  |  |
| I know different connection devices and how to secure them. |  |  |  |
| I know different external media and storage and how to secure them. |  |  |  |
| **Topic 5**  Interpreting Network Diagrams | I can interpret the type of network used on a network diagram. |  |  |  |
| I can interpret the topology of a network on a network diagram. |  |  |  |
| I can interpret the architecture of a network on a network diagram. |  |  |  |
| I can interpret the hardware devices used on a network diagram. |  |  |  |

*Continued on the next page…..*

**End of Learning Aim B Review Continued…**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Topic** | **Checklist Item** | **Confidence** | | |
| **Low** | **Medium** | **High** |
| **Topic 6**  Network Software Components | I know what is meant by the term network operating system and the security features they contain. |  |  |  |
| I know what is meant by the term network monitoring software and the security features they contain. |  |  |  |
| I know what is meant by the term network application software and the security features they contain. |  |  |  |
| **Topic 7**  Network Infrastructure & Resources | I know what is meant by the following network configuration services: TCP/IP, Ports, Packets, NAT |  |  |  |
| I know what is meant by the following network infrastructure services: DNS, DS, Authentication Services, DHCP, Routing and Remote Access |  |  |  |
| I know what is meant by the following resource services: File/Print and Web/Mail/Communications Services |  |  |  |

**BTEC Level 3 National in Information Technology:**

**Unit 11**

Learner Workbook 3

**Learning Aim C:**

Cyber security protection plan

|  |  |
| --- | --- |
| 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](http://qualifications.pearson.com/en/qualifications/btec-nationals/information-technology-2016.html):   * Unit specification * Instructions for Conducting External Assessments (ICEA) * **Unit 11** Sample Assessment Materials (SAMs) * **Unit 11** Sample Marked Learner Work (SMLW) * **Unit 11** Scheme of work * **Unit 11** Delivery guide * **Unit 11** Scheme of work * **Unit 11** Administrative guide * **Unit 11** Templates * Any other new/updated documentation relevant to this unit   The information in this learner workbook is considered to be correct at the date of publication. |

**Start of Learning Aim C Review**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Topic** | **Checklist Item** | **Confidence** | | |
| **Low** | **Medium** | **High** |
| **Topic 1**  Assessment of System Vulnerabilities | I know what is meant by the following tools that can be used to assess vulnerabilities in computer systems: port scanners, registry checker, website vulnerability scanner, vulnerability and management software. |  |  |  |
| I know what is meant by a third-party review and the importance of reviewing a network design before its implemented. |  |  |  |
| I know what is meant by the term penetration testing and why it is used. |  |  |  |
| **Topic 2**  Risk Severity | I know what is meant by a risk severity matrix. |  |  |  |
| I know the meaning of a risk where the probability is: very likely, likely and unlikely. |  |  |  |
| I know the meaning of the following impact levels/values: minor, moderate and major. |  |  |  |
| **Topic 3**  Risk Assessment Approach | I know what a risk assessment is. |  |  |  |
| I know why a risk assessment should be carried out at the following stages: design, during the operation and following a security breach. |  |  |  |
| I know what the following methods are that are carried out at each stage: identify possibly threats, assess vulnerabilities, assess the impact level and determine the risk severity. |  |  |  |
| **Topic 4**  Creating a Cyber Security Plan | I know what is meant by the term cyber security plan. |  |  |  |
| I know what hardware protection measures would be included in a cyber security plan. |  |  |  |
| I know what software protection measures would be included in a cyber security plan. |  |  |  |
| I know what physical protection measures would be included in a cyber security plan. |  |  |  |
| **Topic 5**  Finalising the Cyber Security Plan | I know different technical constrains an organisation may face when trying to secure their network. |  |  |  |
| I know different financial constrains an organisation may face when trying to secure their network. |  |  |  |
| I know different legal constrains an organisation may face when trying to secure their network. |  |  |  |
| I know different usability and efficiency constraints an organisation may face when trying to secure their network. |  |  |  |

**Topic 1**

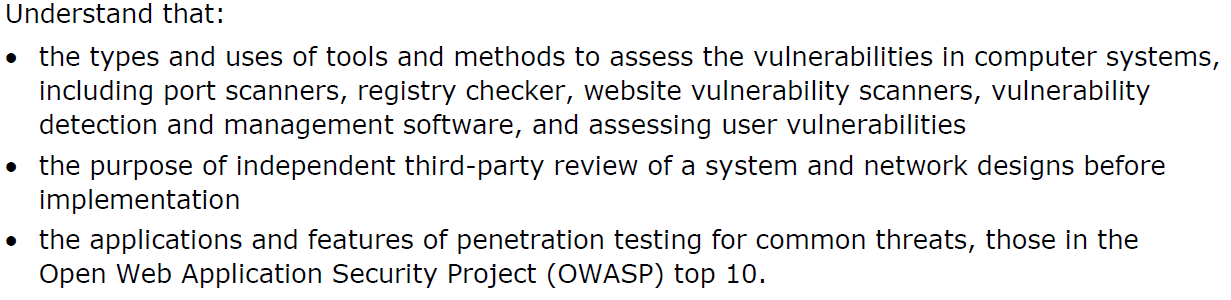
**Assessment of System Vulnerabilities**

**Topic 1: Assessment of System Vulnerabilities**

**Topic 1: Topic Objectives:**

* **Pass – Describe** the different tools that can be used to assess the vulnerabilities in computer systems.
* **Merit – Explain** the role of third-party reviews of network designs and penetration testing.
* **Distinction- Assess** the usefulness of different tools and methods in reducing the risks of unauthorised access.

**Topic 1: Specification Coverage:**

****

**Topic 1: Introductory Task:**

Have you ever heard of penetration testing?

Research different organisations that have successfully found flaws in their security using penetration testing. **(PASS)**

|  |
| --- |
| Type your answer here. |

**Topic 1: Deeper Learning Activities:**

**Penetration Testing**

1. **Explain** the role of a ‘penetration testing’ in the context of network security. **(PASS)**

|  |
| --- |
| Type your answer here. |



1. **Research** and **describe** the top 10 penetration testing tips found in the ‘Open Web Application Security Project (OWASP) Top 10.’ **(MERIT)**

|  |
| --- |
| Type your answer here. |

1. **Assess** the usefulness of penetration testing in reducing the risks of unauthorised access. **(DISTINCTION)**

|  |
| --- |
| Type your answer here. |

**Tools and Methods**

1. **Research** and **describe** the different tools and methods below **(PASS)** and **assess** the usefulness of each one in detecting possible security risk. **(MERIT/DISTINCTION)**

|  |  |  |
| --- | --- | --- |
| **Type** | **Description** | **Usefulness** |
| Port scanners | Type your answer here. | Type your answer here. |
| Registry  checker | Type your answer here. | Type your answer here. |
| Website vulnerability scanners | Type your answer here. | Type your answer here. |
| Vulnerability  detection and management software | Type your answer here. | Type your answer here. |

**Third-Party Reviews**

1. **Explain** the role of a ‘third party review’ in the context of network design. **(PASS)**

|  |
| --- |
| Type your answer here. |

1. **Assess** the usefulness of third-party reviews of network designs before the network is implemented to identify the possible risks. **(MERIT/DISTINCTION)**

|  |
| --- |
| Type your answer here. |

**Topic 1: Progress Check**

|  |  |  |
| --- | --- | --- |
| **Topic** | **Confident**  **(Tick)** | **Need to revisit**  **(Tick)** |
| I know what is meant by the following tools that can be used to assess vulnerabilities in computer systems: port scanners, registry checker, website vulnerability scanner, vulnerability and management software. |  |  |
| I know what is meant by a third-party review and the importance of reviewing a network design before its implemented. |  |  |
| I know what is meant by the term penetration testing and why it is used. |  |  |

**Topic 1: Grade Yourself**

|  |  |
| --- | --- |
| **Grade Description** | **The statement that best describes my progress is…** |
| **Pass – Describe** the different tools that can be used to assess the vulnerabilities in computer systems. |  |
| **Merit – Explain** the role of third-party reviews of network designs and penetration testing. |  |
| **Distinction- Assess** the usefulness of different tools and methods in reducing the risks of unauthorised access. |  |
| **My strengths…..**  Type your answer here. | |
| **My areas for development…**  Type your answer here. | |

**Topic 2**

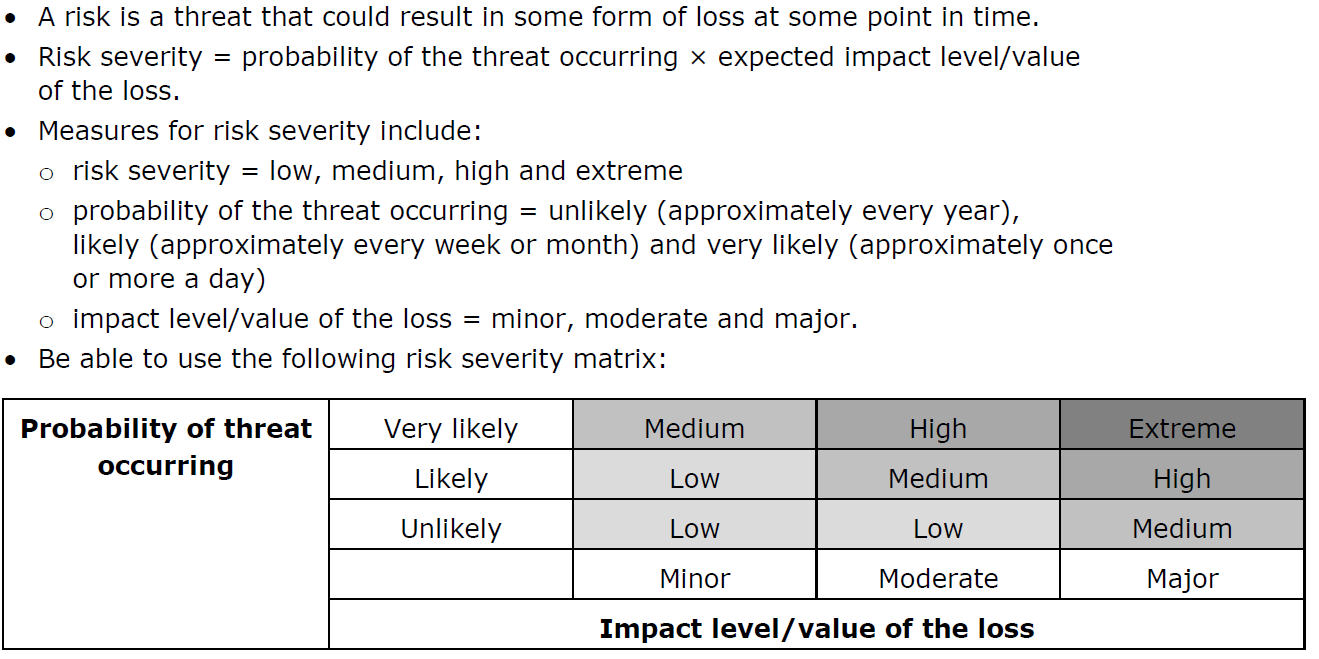
**Risk Severity**

**Topic 2: Risk Severity**

**Topic 2: Topic Objectives:**

* **Pass – Describe** what is meant by the following risk probabilities: Very likely, Medium, High and Extreme.
* **Merit – Describe** howthe probability of a threat occurring can be calculated using a risk severity matrix.
* **Distinction- Discuss** different risk severity matrixes and the suitability of each one.

**Topic 2: Specification Coverage:**

****

**Topic 2: Introductory Task:**

Describe **three** different events in everyday life where the probability of them occurring is:

* Unlikely
* Likely
* Very likely **(PASS)**

|  |
| --- |
| Type your answer here. |

**Topic 2: Deeper Learning Activities:**

**Risk Severity**

A risk is a threat that could result in some form of loss at some point in time.

The risk severity can be calculated by the **probability of the threat occurring** × **expected impact level/value of the loss**.

1. **Describe three** examples of a threat where the probability is unlikely, likely and very likely. **(PASS)**

|  |  |  |
| --- | --- | --- |
| **Type** | **Frequency** | **Examples** |
| Unlikely | Approximately every year | 1. Type your answer here. 2. Type your answer here. 3. Type your answer here. |
| Likely | Approximately every week or month | 1. Type your answer here. 2. Type your answer here. 3. Type your answer here. |
| Very Likely | Approximately once  or more a day | 1. Type your answer here. 2. Type your answer here. 3. Type your answer here. |

1. **Describe** what is meant by the following impact levels/values and give **three** example of each. **(PASS)**

|  |  |  |
| --- | --- | --- |
| **Type** | **Description** | **Examples** |
| Minor | Type your answer here. | 1. Type your answer here. 2. Type your answer here. 3. Type your answer here. |
| Moderate | Type your answer here. | 1. Type your answer here. 2. Type your answer here. 3. Type your answer here. |
| Major | Type your answer here. | 1. Type your answer here. 2. Type your answer here. 3. Type your answer here. |

1. **Describe** what is meant by the term ‘risk severity matrix.’ **(PASS)**

|  |
| --- |
| Type your answer here. |

1. **Describe** the contents of a risk severity matrix. **(PASS)**

|  |
| --- |
| Type your answer here. |

1. **Describe** howthe probability of a threat occurring can be calculated using a risk severity matrix. **(MERIT)**

|  |
| --- |
| Type your answer here. |

1. **Research** different examples of risk severity matrixes and **discuss** when each one would be used. **(DISTINCTON)**

|  |
| --- |
| Type your answer here. |

**Topic 2: Progress Check**

|  |  |  |
| --- | --- | --- |
| **Topic** | **Confident**  **(Tick)** | **Need to revisit**  **(Tick)** |
| I know what is meant by a risk severity matrix. |  |  |
| I know the meaning of a risk where the probability is: very likely, likely and unlikely. |  |  |
| I know the meaning of the following impact levels/values: minor, moderate and major. |  |  |

**Topic 2: Grade Yourself**

|  |  |
| --- | --- |
| **Grade Description** | **The statement that best describes my progress is…** |
| **Pass – Describe** what is meant by the following risk probabilities: Very likely, Medium, High and Extreme. |  |
| **Merit – Determine** the probability of a threat occurring using a risk severity matrix. |  |
| **Distinction- Discuss** different risk severity matrixes and the suitability of each one. |  |
| **My strengths…..**  Type your answer here. | |
| **My areas for development…**  Type your answer here. | |

**Topic 3**

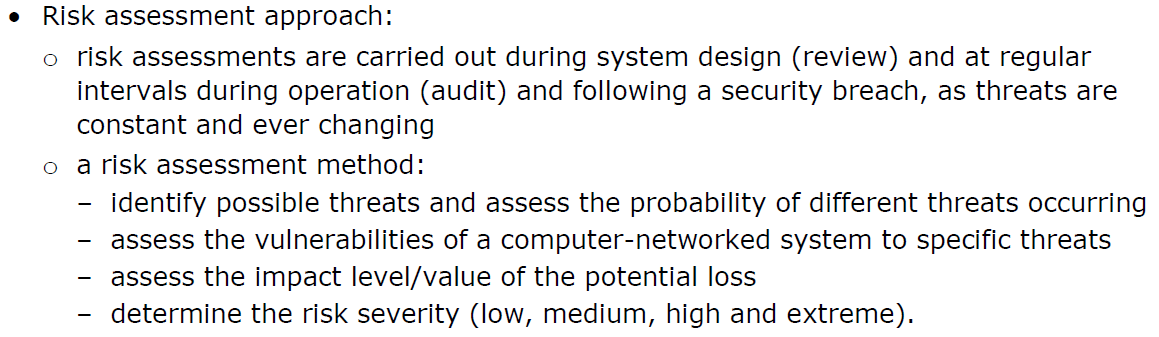
**Risk Assessment Approach**

**Topic 3: Risk Assessment Approach**

**Topic 3: Topic Objectives:**

* **Pass – Describe** when system risk assessments should be carried out.
* **Merit – Explain** why system risk assessments should be carried out at these times and the factors that will be considered.
* **Distinction- Discuss** the use of risk assessments within an actual organisational context.

**Topic 3: Specification Coverage:**

****

**Topic 3: Introductory Task:**

Read this statement:

***Organisations can be confident that once they have setup the necessary hardware, software and working practices that their network will be secured forever.***

Do you agree with this statement?

|  |
| --- |
| Type your answer here. |

**Topic 3: Deeper Learning Activities:**

**Risk Assessment Approach**

1. **Describe** what is meant by the term ‘risk assessment.’ **(PASS)**

|  |
| --- |
| Type your answer here. |

1. **Explain** why a risk assessment should be carried out at the following stages. **(MERIT)**

|  |  |
| --- | --- |
| **Approach** | **Explanation** |
| During the design of a system | Type your answer here. |
| At regular internals during operation | Type your answer here. |
| Following a security breach | Type your answer here. |

1. **Explain** why the different methods would be carried out at each stage. **(MERIT)**

|  |  |
| --- | --- |
| **Method** | **Explanation** |
| Identify possible threats and assess the probability of threats occurring | Type your answer here. |
| Identify the vulnerabilities of a computer-networked system to specific threats | Type your answer here. |
| Identify the impact level of the potential loss | Type your answer here. |
| Determine the risk severity | Type your answer here. |



1. **Research** and **discuss** how an organisation makes use of risk assessments. **(DISTINCTION)**

|  |
| --- |
| Type your answer here. |

**Topic 3: Progress Check**

|  |  |  |
| --- | --- | --- |
| **Topic** | **Confident**  **(Tick)** | **Need to revisit**  **(Tick)** |
| I know what a risk assessment is. |  |  |
| I know why a risk assessment should be carried out at the following stages: design, during the operation and following a security breach. |  |  |
| I know what the following methods are that are carried out at each stage: identify possibly threats, assess vulnerabilities, assess the impact level and determine the risk severity. |  |  |

**Topic 3: Grade Yourself**

|  |  |
| --- | --- |
| **Grade Description** | **The statement that best describes my progress is…** |
| **Pass – Describe** when system risk assessments should be carried out. |  |
| **Merit – Explain** why system risk assessments should be carried out at these times and the factors that will be considered. |  |
| **Distinction- Discuss** the use of risk assessments within an actual organisational context. |  |
| **My strengths…..**  Type your answer here. | |
| **My areas for development…**  Type your answer here. | |

**Topic 4**

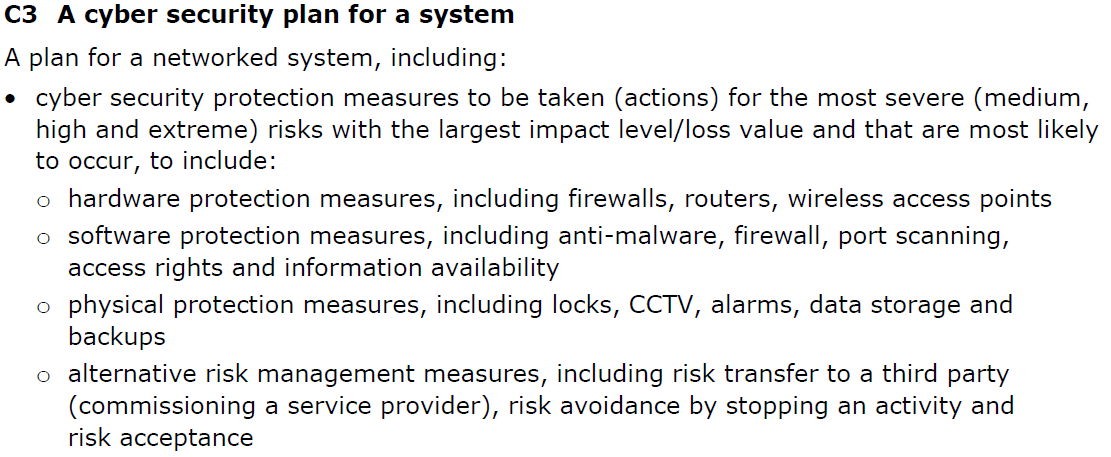
**Creating a Cyber Security Plan**

**Topic 4: Creating a Cyber Security Plan**

**Topic 4: Topic Objectives:**

* **Pass – Identify** the different components of a cyber security plan.
* **Merit – Explain** why the different components of a cyber security plan are required.
* **Distinction- Discuss** the use of cyber security planning within an actual organisational context.

**Topic 4: Specification Coverage:**

****

**Topic 4: Introductory Task:**

When an attack has occurred, an organisation will need to revert to their disaster recover policy in order to handle the attack. However in order to get the organisation back operational again they may need to:

1. Carryon as normal on the same site, but take immediate action to reduce the threat
2. Revert to a system backup
3. Carryout a whole system replacement

Which of the above options would an organisation most likely want to avoid? Why? **(PASS)**

|  |
| --- |
| Type your answer here. |

**Topic 4: Deeper Learning Activities:**

**Cyber Security Plan**

1. **Describe** what is meant by the term ‘cyber security plan.’ **(PASS)**

|  |
| --- |
| Type your answer here. |



1. **Research** and **explain** why the following items should be part of a cyber security plan **(MERIT)** and give **three more** examples of each. **(PASS)**

|  |  |  |
| --- | --- | --- |
| **Measure** | **Why is this included?** | **Examples** |
| Hardware protection measures | Type your answer here. | 1. Firewalls 2. Type your answer here. 3. Type your answer here. 4. Type your answer here. |
| Software protection measures | Type your answer here. | 1. Anti-malware 2. Type your answer here. 3. Type your answer here. 4. Type your answer here. |
| Physical protection measures | Type your answer here. | 1. CCTV 2. Type your answer here. 3. Type your answer here. 4. Type your answer here. |
| Alternative risk management measures | Type your answer here. | 1. Risk transfer to third party 2. Type your answer here. 3. Type your answer here. 4. Type your answer here. |



1. **Research** and **discuss** how an organisation has made use of cyber security planning. **(DISTINCTION)**

|  |
| --- |
| Type your answer here. |

**Topic 4: Progress Check**

|  |  |  |
| --- | --- | --- |
| **Topic** | **Confident**  **(Tick)** | **Need to revisit**  **(Tick)** |
| I know what is meant by the term cyber security plan. |  |  |
| I know what hardware protection measures would be included in a cyber security plan. |  |  |
| I know what software protection measures would be included in a cyber security plan. |  |  |
| I know what physical protection measures would be included in a cyber security plan. |  |  |

**Topic 4: Grade Yourself**

|  |  |
| --- | --- |
| **Grade Description** | **The statement that best describes my progress is…** |
| **Pass – Identify** the different components of a cyber security plan. |  |
| **Merit – Explain** why the different components of a cyber security plan are required. |  |
| **Distinction- Discuss** the use of cyber security planning within an actual organisational context. |  |
| **My strengths…..**  Type your answer here. | |
| **My areas for development…**  Type your answer here. | |

**Topic 5**

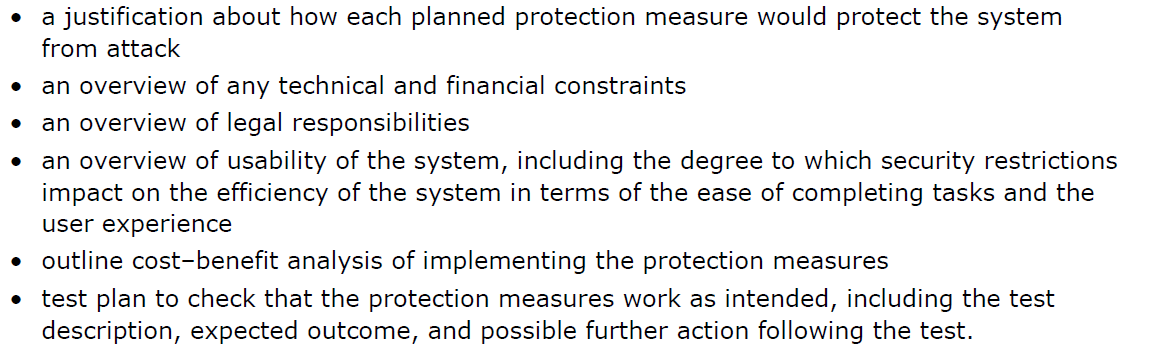
**Finalising the Cyber Security Plan**

**Topic 5: Finalising the Cyber Security Plan**

**Topic 7: Topic Objectives:**

* **Pass – Describe** some of the wider aspects of creating a cyber security plan.
* **Merit – Explain** the wider aspects of creating a cyber security plan and the impacts these have on an organisation.
* **Distinction- Discuss** how the security of an IT system could impact on the current network usage and performance.

**Topic 5: Specification Coverage:**

****

**Topic 5: Introductory Task:**

Think about the restrictions that are in place within your centre to protect the network.

Can you think about any genuine tasks or activities that you wanted to complete, however your network prevented you from completing them?

How did this impact on the efficiency of task that you wanted to carry out? **(PASS)**

|  |
| --- |
| Type your answer here. |

**Topic 5: Deeper Learning Activities:**

**Wider Implications**

1. **Describe** possible **financial constrains** an organisation may face when trying to secure their network **(PASS)** and **explain** how these may impact an organisation. **(MERIT)**

|  |  |
| --- | --- |
| **Constraint** | **Impact on the organisation** |
| Type your answer here. | Type your answer here. |
| Type your answer here. | Type your answer here. |
| Type your answer here. | Type your answer here. |
| Type your answer here. | Type your answer here. |

1. **Explain** possible **technical constrains** an organisation may face when trying to secure their network **(PASS)** and **explain** how these may impact an organisation. **(MERIT)**

|  |  |
| --- | --- |
| **Constraint** | **Impact on the organisation** |
| Type your answer here. | Type your answer here. |
| Type your answer here. | Type your answer here. |
| Type your answer here. | Type your answer here. |
| Type your answer here. | Type your answer here. |

1. **Explain** the **legal requirements** an organisation must adhere to when securing their network **(PASS)** and **explain** how these may impact an organisation. **(MERIT)**

|  |  |
| --- | --- |
| **Constraint** | **Impact on the organisation** |
| Type your answer here. | Type your answer here. |
| Type your answer here. | Type your answer here. |
| Type your answer here. | Type your answer here. |
| Type your answer here. | Type your answer here. |

1. **Describe** how **security that is in place** may impact on the efficiency of the network for legitimate users. **(MERIT)**

|  |
| --- |
| Type your answer here. |

1. **Discuss** the balance an organisation must take between the costs of securing their system, the wider implications above and the impacts on their organisation. **(DISTINCTION)**

|  |
| --- |
| Type your answer here. |

**Topic 5: Progress Check**

|  |  |  |
| --- | --- | --- |
| **Topic** | **Confident**  **(Tick)** | **Need to revisit**  **(Tick)** |
| I know different technical constrains an organisation may face when trying to secure their network. |  |  |
| I know different financial constrains an organisation may face when trying to secure their network. |  |  |
| I know different legal constrains an organisation may face when trying to secure their network. |  |  |
| I know different usability and efficiency constraints an organisation may face when trying to secure their network. |  |  |

**Topic 5: Grade Yourself**

|  |  |
| --- | --- |
| **Grade Description** | **The statement that best describes my progress is…** |
| **Pass – Describe** some of the wider aspects of creating a cyber security plan. |  |
| **Merit – Explain** the wider aspects of creating a cyber security plan and the impacts these have on an organisation. |  |
| **Distinction- Discuss** how the security of an IT system could impact on the current network usage and performance. |  |
| **My strengths…..**  Type your answer here. | |
| **My areas for development…**  Type your answer here. | |

**End of Learning Aim C Review**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Topic** | **Checklist Item** | **Confidence** | | |
| **Low** | **Medium** | **High** |
| **Topic 1**  Assessment of System Vulnerabilities | I know what is meant by the following tools that can be used to assess vulnerabilities in computer systems: port scanners, registry checker, website vulnerability scanner, vulnerability and management software. |  |  |  |
| I know what is meant by a third-party review and the importance of reviewing a network design before its implemented. |  |  |  |
| I know what is meant by the term penetration testing and why it is used. |  |  |  |
| **Topic 2**  Risk Severity | I know what is meant by a risk severity matrix. |  |  |  |
| I know the meaning of a risk where the probability is: very likely, likely and unlikely. |  |  |  |
| I know the meaning of the following impact levels/values: minor, moderate and major. |  |  |  |
| **Topic 3**  Risk Assessment Approach | I know what a risk assessment is. |  |  |  |
| I know why a risk assessment should be carried out at the following stages: design, during the operation and following a security breach. |  |  |  |
| I know what the following methods are that are carried out at each stage: identify possibly threats, assess vulnerabilities, assess the impact level and determine the risk severity. |  |  |  |
| **Topic 4**  Creating a Cyber Security Plan | I know what is meant by the term cyber security plan. |  |  |  |
| I know what hardware protection measures would be included in a cyber security plan. |  |  |  |
| I know what software protection measures would be included in a cyber security plan. |  |  |  |
| I know what physical protection measures would be included in a cyber security plan. |  |  |  |
| **Topic 5**  Finalising the Cyber Security Plan | I know different technical constrains an organisation may face when trying to secure their network. |  |  |  |
| I know different financial constrains an organisation may face when trying to secure their network. |  |  |  |
| I know different legal constrains an organisation may face when trying to secure their network. |  |  |  |
| I know different usability and efficiency constraints an organisation may face when trying to secure their network. |  |  |  |

**BTEC Level 3 National in Information Technology:**

**Unit 11**

Learner Workbook 4

**Learning Aim D:**

Cyber security documentation

|  |  |
| --- | --- |
| 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](http://qualifications.pearson.com/en/qualifications/btec-nationals/information-technology-2016.html):   * Unit specification * Instructions for Conducting External Assessments (ICEA) * **Unit 11** Sample Assessment Materials (SAMs) * **Unit 11** Sample Marked Learner Work (SMLW) * **Unit 11** Scheme of work * **Unit 11** Delivery guide * **Unit 11** Scheme of work * **Unit 11** Administrative guide * **Unit 11** Templates * Any other new/updated documentation relevant to this unit   The information in this learner workbook is considered to be correct at the date of publication. |

**Start of Learning Aim D Review**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Topic** | **Checklist Item** | **Confidence** | | |
| **Low** | **Medium** | **High** |
| **Topic 1**  General IT Policies | I know the purpose and content of the Plan-Do-Check-Act loop. |  |  |  |
| I know why the following policies are needed and likely statements they may contain: Internet policy, email policy, security policy, password procedures policy, staff responsibilities policy and staff training policy. |  |  |  |
| I know what is meant by the term security audit and why they are needed. |  |  |  |
| I know what is meant by the term backup policy, why it is needed and likely statement it may contain. |  |  |  |
| I know what is meant by the term data protection policy, why it is needed and likely statement it may contain. |  |  |  |
| **Topic 2**  Incident Response Policy Part 1 | I know the purpose of the Computer Security Incident Response Team (CSIRT). |  |  |  |
| I know the roles of different people with the CSIRT. |  |  |  |
| I know what constitutes a security incident. |  |  |  |
| I know how to identify if an attack is real. |  |  |  |
| I know how to identify the type of attack and its severity. |  |  |  |
| **Topic 3**  Incident Response Policy Part 2 | I know why it’s important to identify the nature, intent, origin and the files that have been compromised following an attack. |  |  |  |
| I know why it’s important to protect evidence of a cyber-attack. |  |  |  |
| I know external agencies that can be contacted to provide advice on how to handle a cyber-attack. |  |  |  |
| I know the importance of preserving and collating documentation that may be needed to prosecute offenders. |  |  |  |
| **Topic 4**  Disaster Recovery Policy | I know what is meant by the term disaster recovery plan. |  |  |  |
| I know the difference between recovery time objective (RTO) and recovery point objective (RPO). |  |  |  |
| I know what is meant by the term recovery procedures. |  |  |  |
| I know the typical items that are likely to be found on a disaster recovery plan. |  |  |  |

*Continued on the next page…*

**Start of Learning Aim D Review Continued…**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Topic 5**  External Service Providers | I know what is meant by the term External Service Provider (ESP). |  |  |  |
| I know typical services provided by cloud, hardware and software ESPs |  |  |  |
| I know the legal ownership and jurisdiction implications of using ESPs. |  |  |  |
| I know the security protection implications of using ESPs. |  |  |  |
| I know what is meant by the term dispute resolution and the statutory requirements by ESPs when dealing with disputes. |  |  |  |

**Topic 1**

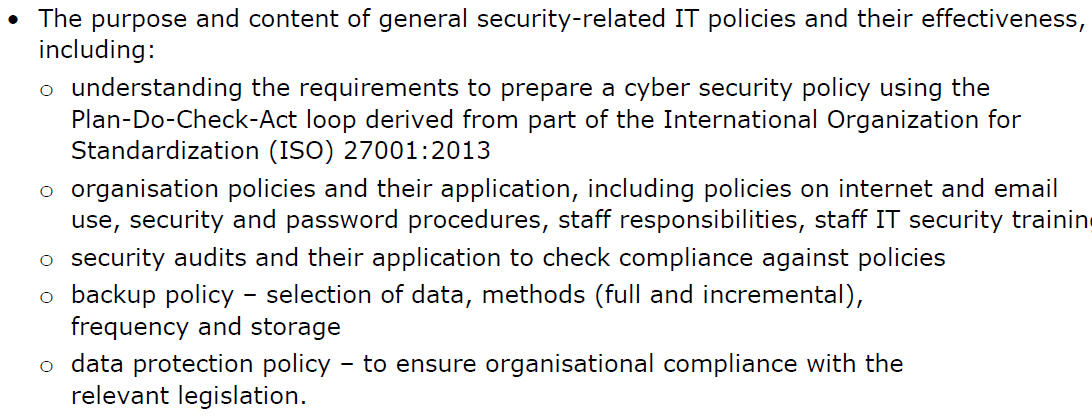
**General IT Policies**

**Topic 1: General IT Policies**

**Topic 1: Topic Objectives:**

* **Pass – Identify** different IT policies and documents that can be used to establish and maintain security and **identify** some of their contents.
* **Merit – Explain** the different IT policies and documents that organisations should make use of and how their contents establish and maintain security.
* **Distinction- Evaluate** how effectively different IT policies and documents secure an IT system on an ongoing basis.

**Topic 1: Specification Coverage:**

****

**Topic 1: Introductory Task:**

Your centre may have an Acceptable Use Policy (AUP).

Consider the following questions:

* What does it contain?
* Did you know it was in place?
* How did you agree to abide by it?
* Are there any network constraints that you disagree with?
* What are the implications if you do not follow it? **(PASS)**

|  |
| --- |
| Type your answer here. |

**Topic 1: Deeper Learning Activities:**

**Preparing a cyber security policy**

1. **Describe** what is meant by the term ‘policy.’ **(PASS)**

|  |
| --- |
| Type your answer here. |



1. **Research** the requirements of the Plan-Do-Check-Act loop derived from the International Organisation for Standardization (ISO). **(PASS)**

|  |  |
| --- | --- |
| **Stage** | **Requirements** |
| Plan | Type your answer here. |
| Do | Type your answer here. |
| Check | Type your answer here. |
| Act | Type your answer here. |

**Organisational policies**

1. **Research** and **describe** the purpose of the following organisational policies and give example statements of what they may contain. **(PASS)**

|  |  |  |
| --- | --- | --- |
| **Stage** | **Description** | **Example Statements** |
| Internet Policy | Type your answer here. | Type your answer here. |
| Email Policy | Type your answer here. | Type your answer here. |
| Security Policy | Type your answer here. | Type your answer here. |
| Password Procedures Policy | Type your answer here. | Type your answer here. |
| Staff Responsibilities Policy | Type your answer here. | Type your answer here. |
| Staff Training Policy | Type your answer here. | Type your answer here. |

**Security audits**

1. **Describe** what is meant by the term ‘security audit.’ **(PASS)**

|  |
| --- |
| Type your answer here. |

1. **Complete** the different areas a security audit may include **(PASS)** and give example statements of what each area may say. **(MERIT)**

|  |  |
| --- | --- |
| **Area** | **Example Statements** |
| Person responsible. | Type your answer here. |
| Date of next audit | Type your answer here. |
| Type your answer here. | Type your answer here. |
| Type your answer here. | Type your answer here. |

**Backup policy**

1. **Describe** what is meant by the term ‘backup policy.’ **(PASS)**

|  |
| --- |
| Type your answer here. |

1. **Complete** the different areas a backup policy may include **(PASS)** and give example statements of what each area may say. **(MERIT)**

|  |  |
| --- | --- |
| **Area** | **Example Statements** |
| Person responsible | Type your answer here. |
| Data to be backed up | Type your answer here. |
| Type your answer here. | Type your answer here. |
| Type your answer here. | Type your answer here. |

**Data protection policy**

1. **Describe** what is meant by the term ‘data protection policy.’ **(PASS)**

|  |
| --- |
| Type your answer here. |

1. **Complete** the different areas a data protection policy may include and give example statements of what each area may say. **(PASS)**

|  |  |
| --- | --- |
| **Area** | **Example Statements** |
| What security is in place to secure data | Type your answer here. |
| Individual rights to access their own data | Type your answer here. |
| Type your answer here. | Type your answer here. |
| Type your answer here. | Type your answer here. |

**Distinction Task:**

1. **Evaluate** how effectively the different policies and documents covered in this topic secure an IT system on an ongoing basis. **(DISTINCTION)**

|  |
| --- |
| Type your answer here. |

**Topic 1: Progress Check**

|  |  |  |
| --- | --- | --- |
| **Topic** | **Confident**  **(Tick)** | **Need to revisit**  **(Tick)** |
| I know the purpose and content of the Plan-Do-Check-Act loop. |  |  |
| I know why the following policies are needed and likely statements they may contain: Internet policy, email policy, security policy, password procedures policy, staff responsibilities policy and staff training policy. |  |  |
| I know what is meant by the term security audit and why they are needed. |  |  |
| I know what is meant by the term backup policy, why it is needed and likely statement it may contain. |  |  |
| I know what is meant by the term data protection policy, why it is needed and likely statement it may contain. |  |  |

**Topic 1: Grade Yourself**

|  |  |
| --- | --- |
| **Grade Description** | **The statement that best describes my progress is…** |
| **Pass – Identify** different IT policies and documents that can be used to establish and maintain security and **identify** some of their contents. |  |
| **Merit – Explain** the different IT policies and documents that organisations should make use of and how their contents establish and maintain security. |  |
| **Distinction- Evaluate** how effectively different IT policies and documents secure an IT system on an ongoing basis. |  |
| **My strengths…..**  Type your answer here. | |
| **My areas for development…**  Type your answer here. | |

**Topic 2**

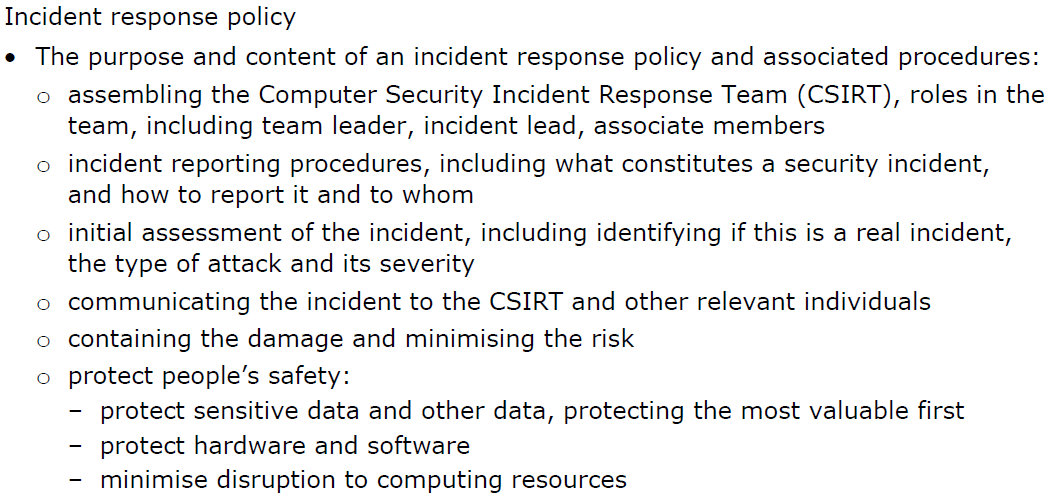
**Incident Response Policy Part 1**

**Topic 2: Incident Reponses Policy Part 1**

**Topic 2: Topic Objectives:**

* **Pass – Identify** the purpose of an incident response policy and associated procedures.
* **Merit – Explain** the different procedures that will follow a security incident.
* **Distinction- Discuss** the reasons why an incident response policy should be well planned and in place before threats occur.

**Topic 2: Specification Coverage:**

****

**Topic 2: Introductory Task:**

Imagine you own your own organisation. During a trip away, you get a phone call informing you that your organisation has suffered a cyber-attack.

What would your initial reaction be? **(PASS)**

|  |
| --- |
| Type your answer here. |

**Topic 2: Deeper Learning Activities:**

**Assembling the CSIRT**

1. **Describe** what is meant by the term ‘Computer Security Incident Response Team (CSIRT).’ **(PASS)**

|  |
| --- |
| Type your answer here. |

1. **Describe** the roles of the following members of the CSIRT. **(PASS)**

|  |  |
| --- | --- |
| **Member** | **Role** |
| Team Leader | Type your answer here. |
| Incident Lead | Type your answer here. |
| Associate Members | Type your answer here. |



1. **Research** and **describe** the tools an organisation can use to determine if a threat is real, the type of attack and the severity. **(MERIT)**

|  |
| --- |
| Type your answer here. |



1. **Research** and **explain** what constitutes a security incident that would start a cyber security investigation. **(MERIT)**

|  |
| --- |
| Type your answer here. |

1. **Explain** why an organisation would want to contain the damage and minimise the risk. **(PASS)**

|  |
| --- |
| Type your answer here. |

1. **Explain** why the protection of the following areas would be checked following an attack. **(PASS)**

|  |  |
| --- | --- |
| **Area** | **Why would this be checked?** |
| Sensitive data | Type your answer here. |
| Hardware and software | Type your answer here. |
| Disruption to other computing resources | Type your answer here. |

**Topic 2: Progress Check**

|  |  |  |
| --- | --- | --- |
| **Topic** | **Confident**  **(Tick)** | **Need to revisit**  **(Tick)** |
| I know the purpose of the Computer Security Incident Response Team (CSIRT). |  |  |
| I know the roles of different people with the CSIRT. |  |  |
| I know what constitutes a security incident. |  |  |
| I know how to identify if an attack is real. |  |  |
| I know how to identify the type of attack and its severity. |  |  |

**Topic 2: Grade Yourself**

|  |  |
| --- | --- |
| **Grade Description** | **The statement that best describes my progress is…** |
| **Pass – Identify** the purpose of an incident response policy and associated procedures. |  |
| **Merit – Explain** the different procedures that will follow a security incident. |  |
| **Distinction- Discuss** the reasons why an incident response policy should be well planned and in place before threats occur. |  |
| **My strengths…..**  Type your answer here. | |
| **My areas for development…**  Type your answer here. | |

**Topic 3**

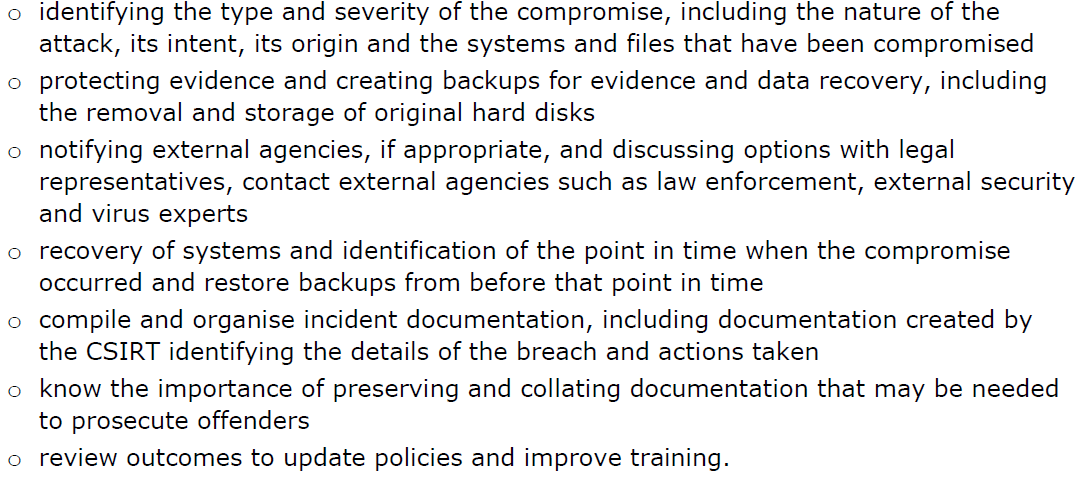
**Incident Response Policy Part 2**

**Topic 3: Incident Response Policy Part 2**

**Topic 3: Topic Objectives:**

* **Pass – Identify** the purpose of an incident response policy and associated procedures.
* **Merit – Explain** the different procedures that will follow a security incident.
* **Distinction- Discuss** the reasons why an incident response policy should be well planned and in place before threats occur.

**Topic 3: Specification Coverage:**

****

**Topic 3: Introductory Task:**

Imagine you own your own organisation that has suffered a cyber-attack.

Who would you consult in order to get advice on how to deal with the attack? **(PASS)**

|  |
| --- |
| Type your answer here. |

**Topic 3: Deeper Learning Activities:**

**Incident Response**

1. **Describe** why it is important to identify the following areas after an attack has occurred. **(PASS)**

|  |  |
| --- | --- |
| **Area** | **Why would this be checked?** |
| Nature of attack | Type your answer here. |
| Intent | Type your answer here. |
| Origin | Type your answer here. |
| Systems and files that have been compromised | Type your answer here. |

1. **Complete** the table below with different external agencies an organisation may contact following an attack **(PASS)** and explain why. **(MERIT)**

|  |  |
| --- | --- |
| **External Agency** | **Why may these be contacted?** |
| Legal representatives | Type your answer here. |
| Virus experts | Type your answer here. |
| Type your answer here. | Type your answer here. |
| Type your answer here. | Type your answer here. |

1. **Explain** why the following areas are required following an attack. **(PASS)**

|  |  |
| --- | --- |
| **Area** | **Why is this needed?** |
| Protecting evidence and creating backups of evidence | Type your answer here. |
| Recovery of systems to when the compromise  occurred | Type your answer here. |
| Compile and organise incident documentation | Type your answer here. |
| Preserving documentation that will be used to prosecute offenders | Type your answer here. |
| Update policies and improve training | Type your answer here. |



1. **Research** and **discuss** the reasons why an incident response policy should be well planned and in place before threats occur. **(DISTINCTION)**

|  |
| --- |
| Type your answer here. |

**Topic 3: Progress Check**

|  |  |  |
| --- | --- | --- |
| **Topic** | **Confident**  **(Tick)** | **Need to revisit**  **(Tick)** |
| I know why it’s important to identify the nature, intent, origin and the files that have been compromised following an attack. |  |  |
| I know why it’s important to protect evidence of a cyber-attack. |  |  |
| I know external agencies that can be contacted to provide advice on how to handle a cyber-attack. |  |  |
| I know the importance of preserving and collating documentation that may be needed to prosecute offenders. |  |  |

**Topic 3: Grade Yourself**

|  |  |
| --- | --- |
| **Grade Description** | **The statement that best describes my progress is…** |
| **Pass – Identify** the purpose of an incident response policy and associated procedures. |  |
| **Merit – Explain** the different procedures that will follow a security incident. |  |
| **Distinction- Discuss** the reasons why an incident response policy should be well planned and in place before threats occur. |  |
| **My strengths…..**  Type your answer here. | |
| **My areas for development…**  Type your answer here. | |

**Topic 4**

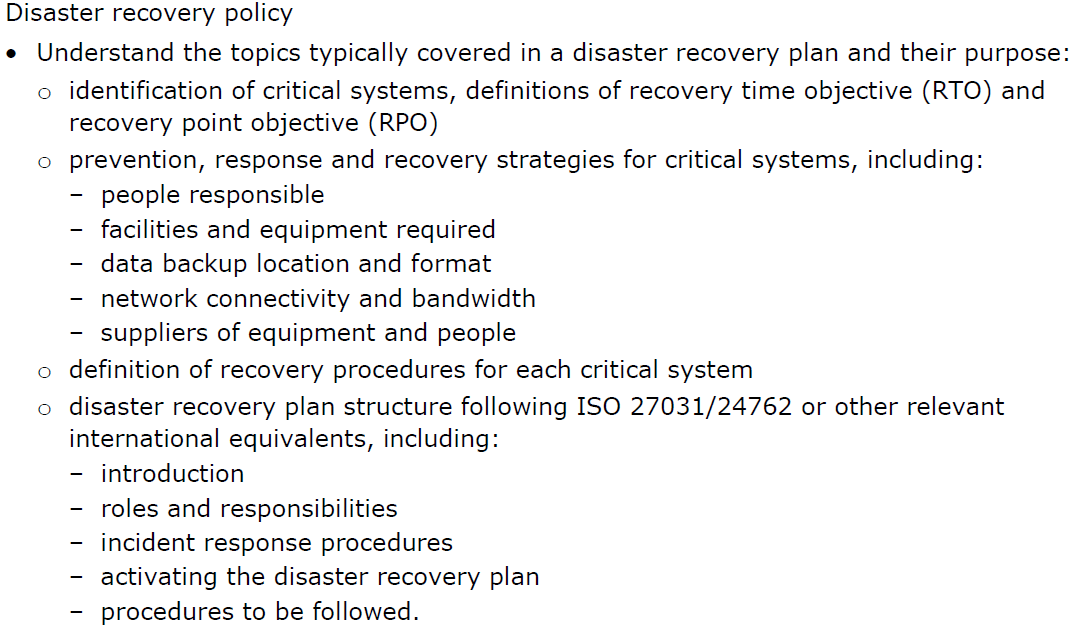
**Disaster Recovery Policy**

**Topic 4: Disaster Recovery Policy**

**Topic 4: Topic Objectives:**

* **Pass – Describe** the purpose of a disaster recovery policy and identify the typical topics that should be included.
* **Merit – Explain** why the different topics typically covered in a disaster recovery plan are needed.
* **Distinction- Discuss** how a disaster recovery policy can impact on the recovery time and the organisational impact of an attack.

**Topic 4: Specification Coverage:**

****

**Topic 4: Introductory Task:**

Read the following statement:

***When an attack has taken place, the first thing an organisation should do is to create a disaster recovery policy in order to deal with the attack.***

Do you agree or disagree with this statement? Why? **(PASS)**

|  |
| --- |
| Type your answer here. |

**Topic 4: Deeper Learning Activities:**

**Disaster Recovery Policy**

1. **Describe** what is meant by the term ‘disaster recovery plan.’ **(PASS)**

|  |
| --- |
| Type your answer here. |

1. **Describe** the term ‘Recovery Time Objective (RTO).’ **(PASS)**

|  |
| --- |
| Type your answer here. |

1. **Describe** the term ‘Recovery Point Objective (RPO).’  **(PASS)**

|  |
| --- |
| Type your answer here. |

1. Describe the prevention strategies and possible recovery strategies for the following systems. **(PASS)**

|  |  |  |
| --- | --- | --- |
| **System** | **Prevention Strategies** | **Recovery Strategies** |
| People responsible | Type your answer here. | Type your answer here. |
| Facilities and equipment required | Type your answer here. | Type your answer here. |
| Data backup location and format | Type your answer here. | Type your answer here. |
| Network connectivity and bandwidth | Type your answer here. | Type your answer here. |
| Suppliers of equipment and people | Type your answer here. | Type your answer here. |

1. **Describe** the following areas of a disaster recovery plan **(PASS)** and explain why they are needed. **(MERIT)**

|  |  |  |
| --- | --- | --- |
| **Area** | **What is this?** | **Why is this needed?** |
| Introduction | Type your answer here. | Type your answer here. |
| Roles & responsibilities | Type your answer here. | Type your answer here. |
| Incident response procedures | Type your answer here. | Type your answer here. |
| Activating the disaster recovery plan | Type your answer here. | Type your answer here. |
| Procedures to be followed | Type your answer here. | Type your answer here. |



1. **Research** and **discuss** how a disaster recovery policy can impact on the recovery time and the organisational impact of an attack. **(DISTINCTION)**

|  |
| --- |
| Type your answer here. |

**Topic 4: Progress Check**

|  |  |  |
| --- | --- | --- |
| **Topic** | **Confident**  **(Tick)** | **Need to revisit**  **(Tick)** |
| I know what is meant by the term disaster recovery plan. |  |  |
| I know the difference between recovery time objective (RTO) and recovery point objective (RPO). |  |  |
| I know what is meant by the term recovery procedures. |  |  |
| I know the typical items that are likely to be found on a disaster recovery plan. |  |  |

**Topic 4: Grade Yourself**

|  |  |
| --- | --- |
| **Grade Description** | **The statement that best describes my progress is…** |
| **Pass – Describe** the purpose of a disaster recovery policy and identify the typical topics that should be included. |  |
| **Merit – Explain** why the different topics typically covered in a disaster recovery plan are needed. |  |
| **Distinction- Discuss** how a disaster recovery policy can impact on the recovery time and the organisational impact of an attack. |  |
| **My strengths…..**  Type your answer here. | |
| **My areas for development…**  Type your answer here. | |

**Topic 5**

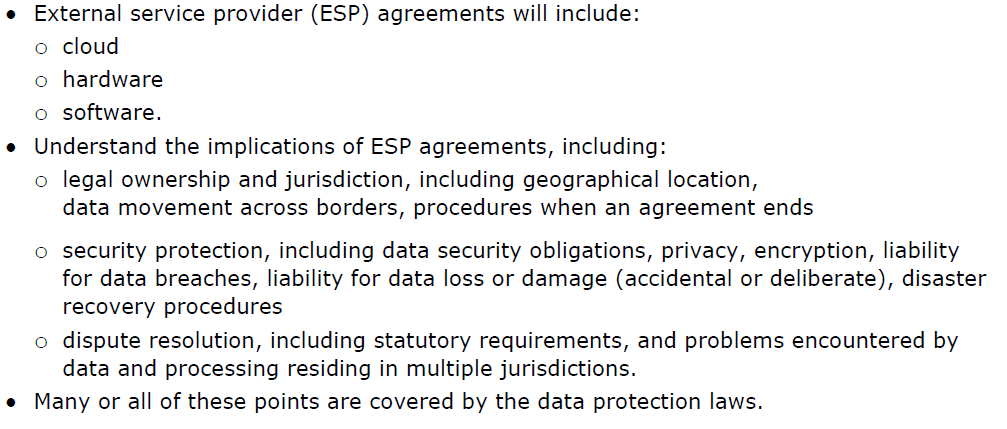
**External Service Providers**

**Topic 5: Implications of External Service Providers**

**Topic 5: Topic Objectives:**

* **Pass – Describe** what is meant by different external service providers including cloud, hardware and software and typical agreements that organisations have to follow.
* **Merit – Explain** the implications of using external service providers.
* **Distinction- Discuss** the wider implications of using external service providers and the possible problems that an organisation may face during a dispute.

**Topic 5: Specification Coverage:**

****

**Topic 5: Introductory Task:**

An External Service Provider is an organisation that provides a service to individuals.

Can you list **five** External Service Providers that you make use of inside and outside your home? **(PASS)**

|  |
| --- |
| Type your answer here. |

**Topic 5: Deeper Learning Activities:**

**External Service Providers**

1. **Describe** what is meant by the term ‘External Service Provider (ESP).’ **(PASS)**

|  |
| --- |
| Type your answer here. |

1. **Describe** what is meant by the term ‘External Service Provider Agreement’ **(PASS)**

|  |
| --- |
| Type your answer here. |

1. Describe what is meant by the following External Providers and give three examples of each. **(PASS)**

|  |  |  |
| --- | --- | --- |
| **External Service Provider** | **Description** | **Examples** |
| Cloud | Type your answer here. | 1. Type your answer here. 2. Type your answer here. 3. Type your answer here. |
| Hardware | Type your answer here. | 1. Type your answer here. 2. Type your answer here. 3. Type your answer here. |
| Software | Type your answer here. | 1. Type your answer here. 2. Type your answer here. 3. Type your answer here. |

1. **Explain** the following **legal ownership and jurisdiction** implications of using External Service Provider. **(MERIT)**

|  |  |
| --- | --- |
| **Point** | **Implication** |
| Geographical location | Type your answer here. |
| Data movement across borders | Type your answer here. |
| Procedures when an agreement ends | Type your answer here. |

1. **Explain** the following **security protection** implications of using External Service Provider. **(MERIT)**

|  |  |
| --- | --- |
| **Point** | **Implication** |
| Data security obligations | Type your answer here. |
| Privacy | Type your answer here. |
| Encryption | Type your answer here. |
| Liability for data breaches | Type your answer here. |
| Liability for data loss or damage (accidental or deliberate) | Type your answer here. |
| Disaster recovery procedures | Type your answer here. |

1. **Explain** what is meant by the term ‘dispute resolution.’ **(PASS)**

|  |
| --- |
| Type your answer here. |



1. **Research** and **describe** the statutory requirements that ESPs must follow during dispute resolution **(MERIT)**

|  |
| --- |
| Type your answer here. |



1. **Research** and **discuss** the problems organisations may face when using External Service Providers which can lead to jurisdictions. **(DISTINCTION)**

|  |
| --- |
| Type your answer here. |

**Topic 5: Progress Check**

|  |  |  |
| --- | --- | --- |
| **Topic** | **Confident**  **(Tick)** | **Need to revisit**  **(Tick)** |
| I know what is meant by the term External Service Provider (ESP). |  |  |
| I know typical services provided by cloud, hardware and software ESPs |  |  |
| I know the legal ownership and jurisdiction implications of using ESPs. |  |  |
| I know the security protection implications of using ESPs. |  |  |
| I know what is meant by the term dispute resolution and the statutory requirements by ESPs when dealing with disputes. |  |  |

**Topic 5: Grade Yourself**

|  |  |
| --- | --- |
| **Grade Description** | **The statement that best describes my progress is…** |
| **Pass – Describe** what is meant by different external service providers including cloud, hardware and software and typical agreements that organisations have to follow. |  |
| **Merit – Explain** the implications of using external service providers. |  |
| **Distinction- Discuss** the wider implications of using external service providers and the possible problems that an organisation may face during a dispute. |  |
| **My strengths…..**  Type your answer here. | |
| **My areas for development…**  Type your answer here. | |

**End of Learning Aim D Review**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Topic** | **Checklist Item** | **Confidence** | | |
| **Low** | **Medium** | **High** |
| **Topic 1**  General IT Policies | I know the purpose and content of the Plan-Do-Check-Act loop. |  |  |  |
| I know why the following policies are needed and likely statements they may contain: Internet policy, email policy, security policy, password procedures policy, staff responsibilities policy and staff training policy. |  |  |  |
| I know what is meant by the term security audit and why they are needed. |  |  |  |
| I know what is meant by the term backup policy, why it is needed and likely statement it may contain. |  |  |  |
| I know what is meant by the term data protection policy, why it is needed and likely statement it may contain. |  |  |  |
| **Topic 2**  Incident Response Policy Part 1 | I know the purpose of the Computer Security Incident Response Team (CSIRT). |  |  |  |
| I know the roles of different people with the CSIRT. |  |  |  |
| I know what constitutes a security incident. |  |  |  |
| I know how to identify if an attack is real. |  |  |  |
| I know how to identify the type of attack and its severity. |  |  |  |
| **Topic 3**  Incident Response Policy Part 2 | I know why it’s important to identify the nature, intent, origin and the files that have been compromised following an attack. |  |  |  |
| I know why it’s important to protect evidence of a cyber-attack. |  |  |  |
| I know external agencies that can be contacted to provide advice on how to handle a cyber-attack. |  |  |  |
| I know the importance of preserving and collating documentation that may be needed to prosecute offenders. |  |  |  |
| **Topic 4**  Disaster Recovery Policy | I know what is meant by the term disaster recovery plan. |  |  |  |
| I know the difference between recovery time objective (RTO) and recovery point objective (RPO). |  |  |  |
| I know what is meant by the term recovery procedures. |  |  |  |
| I know the typical items that are likely to be found on a disaster recovery plan. |  |  |  |

*Continued on the next page…*

**End of Learning Aim D Review Continued…**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Topic 5**  External Service Providers | I know what is meant by the term External Service Provider (ESP). |  |  |  |
| I know typical services provided by cloud, hardware and software ESPs |  |  |  |
| I know the legal ownership and jurisdiction implications of using ESPs. |  |  |  |
| I know the security protection implications of using ESPs. |  |  |  |
| I know what is meant by the term dispute resolution and the statutory requirements by ESPs when dealing with disputes. |  |  |  |

**BTEC Level 3 National in Information Technology:**

**Unit 11**

Learner Workbook 5

**Learning Aim E:**

Forensic procedures

|  |  |
| --- | --- |
| 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](http://qualifications.pearson.com/en/qualifications/btec-nationals/information-technology-2016.html):   * Unit specification * Instructions for Conducting External Assessments (ICEA) * **Unit 11** Sample Assessment Materials (SAMs) * **Unit 11** Sample Marked Learner Work (SMLW) * **Unit 11** Scheme of work * **Unit 11** Delivery guide * **Unit 11** Scheme of work * **Unit 11** Administrative guide * **Unit 11** Templates * Any other new/updated documentation relevant to this unit   The information in this learner workbook is considered to be correct at the date of publication. |

**Start of Learning Aim E Review**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Topic** | **Checklist Item** | **Confidence** | | |
| **Low** | **Medium** | **High** |
| **Topic 1**  Desktop Forensics | I know what is meant by the term desktop forensics. |  |  |  |
| I know the different desktop forensic tools that can be used by an organisation to solve crimes. |  |  |  |
| I know the challenges of using live forensics data when analysing data. |  |  |  |
| **Topic 2**  Network Forensics | I know what is meant by the term network forensics. |  |  |  |
| I know the different network forensic tools that can be used by an organisation to solve crimes. |  |  |  |
| I know the impacts that network forensics may have on the performance of a network. |  |  |  |
| **Topic 3**  Systematic Forensic Analysis | I know why it’s important to ensure evidence about an attack is accurate. |  |  |  |
| I know why it’s important to gather evidence immediately after an attack. |  |  |  |
| I know why it’s important to record all findings and consider how reliable the evidence is. |  |  |  |
| I know why it’s important to collect evidence about an attack that is relevant and correct. |  |  |  |
| I know why it’s important to record the facts and not opinions when collecting evidence about an attack. |  |  |  |
| I know why it’s important to evaluate evidence first before making recommendations on how to improve the security of a system. |  |  |  |

**Topic 1**

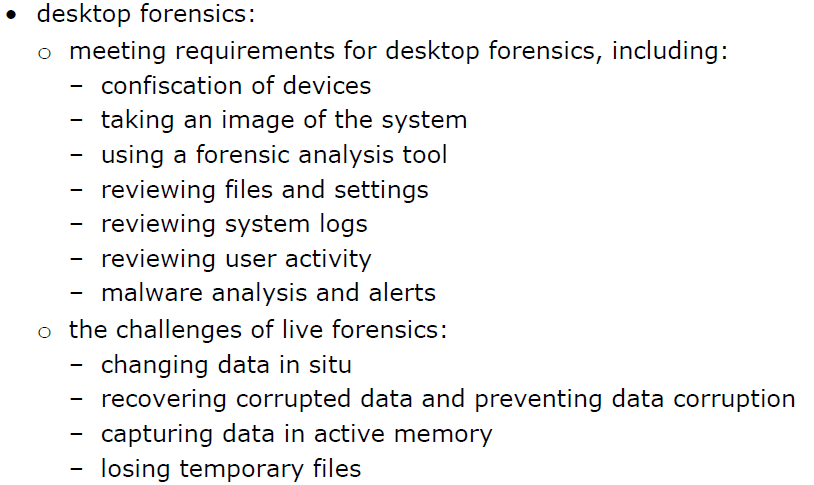
**Desktop Forensics**

**Topic 1: Desktop Forensics**

**Topic 1: Topic Objectives:**

* **Pass – Describe** the term forensics and the purpose of different desktop forensic tools.
* **Merit – Explain** why different desktop forensics tools would be used.
* **Distinction- Assess** how different evidence gathered by desktop forensics can help solve computer related crimes.

**Topic 1: Specification Coverage:**

****

**Topic 1: Introductory Task:**

We often hear the word ‘forensics.’

What is your interpretation of this word? What types of crimes do you know that would require the use of forensics? **(PASS)**

|  |
| --- |
| Type your answer here. |

**Topic 1: Deeper Learning Activities:**

**Desktop Forensics**

1. **Describe** what is meant by the term ‘desktop forensics.’ **(PASS)**

|  |
| --- |
| Type your answer here. |

1. **Describe** what is meant by the following desktop forensics **(PASS) and** explain why they would be used. **(MERIT)**

|  |  |  |
| --- | --- | --- |
| **Desktop Forensic** | **Description** | **Why would this be used?** |
| Confiscation of devices | Type your answer here. | Type your answer here. |
| Taking an image of the system | Type your answer here. | Type your answer here. |
| Using a forensic analysis tool | Type your answer here. | Type your answer here. |
| Reviewing files and settings | Type your answer here. | Type your answer here. |
| Reviewing system logs | Type your answer here. | Type your answer here. |
| Reviewing user activity | Type your answer here. | Type your answer here. |
| Reviewing user activity | Type your answer here. | Type your answer here. |

1. **Explain** what is meant by the following challenges when using live forensics. **(MERIT)**

|  |  |
| --- | --- |
| **Live Forensic** | **Challenge** |
| Changing data in situ | Type your answer here. |
| Recovering corrupted data | Type your answer here. |
| Capturing data in active memory | Type your answer here. |
| Losing temporary files | Type your answer here. |



1. **Research** and **assess** the effectiveness of different desktop forensics used by an organisation to gather evidence about an attack to bring offenders to justice. **(DISTINCTION)**

|  |
| --- |
| Type your answer here. |

**Topic 1: Progress Check**

|  |  |  |
| --- | --- | --- |
| **Topic** | **Confident**  **(Tick)** | **Need to revisit**  **(Tick)** |
| I know what is meant by the term desktop forensics. |  |  |
| I know the different desktop forensic tools that can be used by an organisation to solve crimes. |  |  |
| I know the challenges of using live forensics data when analysing data. |  |  |

**Topic 1: Grade Yourself**

|  |  |
| --- | --- |
| **Grade Description** | **The statement that best describes my progress is…** |
| **Pass – Describe** the term forensics and the purpose of different desktop forensic tools. |  |
| **Merit – Explain** why different desktop forensics tools would be used. |  |
| **Distinction- Assess** how different evidence gathered by desktop forensics can help solve computer related crimes. |  |
| **My strengths…..**  Type your answer here. | |
| **My areas for development…**  Type your answer here. | |

**Topic 2**

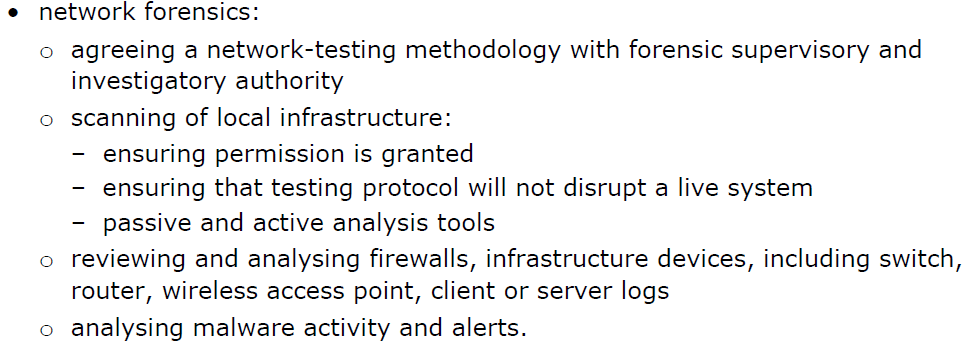
**Network Forensics**

**Topic 2: Network Forensics**

**Topic 2: Topic Objectives:**

* **Pass – Describe** the purpose of different network forensic tools.
* **Merit – Explain** the different network forensics tools that can be used to gather evidence about a security incident.
* **Distinction- Discuss** the possible impacts that network forensics will have on a network.

**Topic 2: Specification Coverage:**

****

**Topic 2: Introductory Task:**

Your tutor or network manager may give you a talk on the different tools used by your centre to respond to incidents.

They may tell you how they know when users have broken network procedures and how they monitor individuals.

Make a note of the points raised.

|  |
| --- |
| Type your answer here. |

**Topic 2: Deeper Learning Activities:**

**Network Forensics**

1. **Describe** what is meant by the term ‘network forensics.’ **(PASS)**

|  |
| --- |
| Type your answer here. |

1. **Describe** what is meant by the following network forensics **(PASS) and** explain why they would be used. **(MERIT)**

|  |  |  |
| --- | --- | --- |
| **Network Forensic** | **Description** | **Why would this be used?** |
| Reviewing firewalls | Type your answer here. | Type your answer here. |
| Reviewing switches | Type your answer here. | Type your answer here. |
| Reviewing routers | Type your answer here. | Type your answer here. |
| Reviewing wireless access points | Type your answer here. | Type your answer here. |
| Reviewing client or server logs | Type your answer here. | Type your answer here. |
| Reviewing malware activity alerts | Type your answer here. | Type your answer here. |

1. **Discuss** why these areas are needed when scanning hardware within a network:

* Ensuring permission is granted
* Ensuring that the testing protocol will not cause disruption
* Use of passive and active analysis tools **(DISTINCTION)**

|  |
| --- |
| Type your answer here. |

**Topic 2: Progress Check**

|  |  |  |
| --- | --- | --- |
| **Topic** | **Confident**  **(Tick)** | **Need to revisit**  **(Tick)** |
| I know what is meant by the term network forensics. |  |  |
| I know the different network forensic tools that can be used by an organisation to solve crimes. |  |  |
| I know the impacts that network forensics may have on the performance of a network. |  |  |

**Topic 2: Grade Yourself**

|  |  |
| --- | --- |
| **Grade Description** | **The statement that best describes my progress is…** |
| **Pass – Describe** the purpose of network forensics. |  |
| **Merit – Explain** the different network forensics tools that can be used to gather evidence about a security incident. |  |
| **Distinction- Discuss** the possible impacts that network forensics will have on a network. |  |
| **My strengths…..**  Type your answer here. | |
| **My areas for development…**  Type your answer here. | |

**Topic 3**

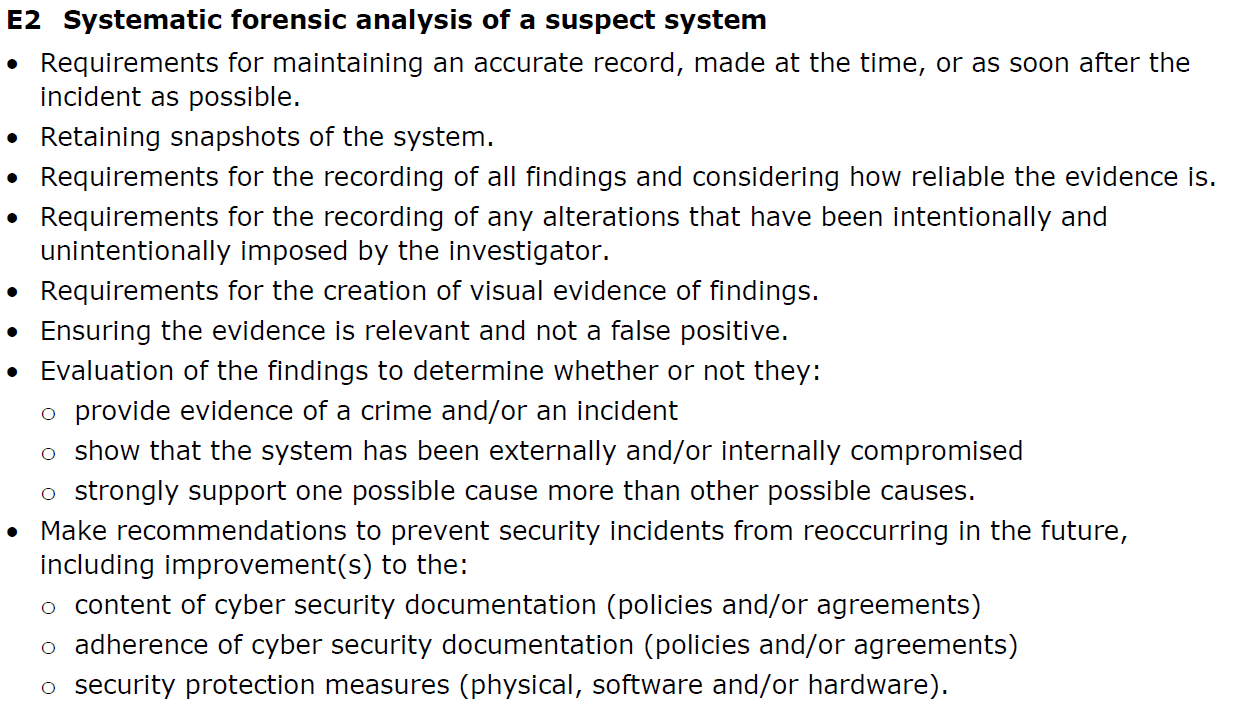
**Systematic Forensic Analysis**

**Topic 3: Forensic Analysis**

**Topic 3: Topic Objectives:**

* **Pass – Describe** how to ensure the outcomes from a systematic forensic analysis are trustworthy.
* **Merit – Explain** the importance of gathering evidence that is correct, reliable, relevant and not intentionally imposed by the investigator.
* **Distinction- Discuss** the benefits and drawbacks of allowing external agencies to investigate computer crimes or incidents.

**Topic 3: Specification Coverage:**

****

**Topic 3: Deeper Learning Activities:**

**Forensic Analysis**

Very often, evidence is gathered to bring criminal charges against those responsible for an attack or incident.

1. **Explain** why the following are important when documenting a computer related attack or incident. **(PASS/MERIT)**

|  |  |
| --- | --- |
| **Area** | **Importance** |
| Maintaining an accurate record of what happened | Type your answer here. |
| Maintaining an accurate record of who was involved | Type your answer here. |
| Collecting evidence as soon as possible | Type your answer here. |
| Recording all findings | Type your answer here. |
| Considering how reliable the evidence is | Type your answer here. |
| Not intentionally imposing alterations to the evidence | Type your answer here. |
| Ensuring all evidence is relevant | Type your answer here. |
| Ensuring all evidence is correct | Type your answer here. |
| Ensuring all evidence is within legal requirements | Type your answer here. |

**Recommendations & Conclusions**

1. **Explain** why the evidence gathered must be assessed to ensure if it meets the following requirements. **(PASS/MERIT)**

|  |  |
| --- | --- |
| **Requirements** | **Importance** |
| Provide evidence of a crime and/or an incident | Type your answer here. |
| Show that the system has been externally and/or internally compromised | Type your answer here. |
| Strongly support one possible cause more than other possible causes | Type your answer here. |

1. **Explain** why it’s important to make improvements to the following practices when an attack has occurred. **(PASS/MERIT)**

|  |  |
| --- | --- |
| **Practices** | **Importance** |
| Content of cyber security policies | Type your answer here. |
| Adherence of cyber security policies | Type your answer here. |
| Security protection measures (e.g. hardware and software) | Type your answer here. |

1. **Discuss** the benefits and drawbacks of allowing external agencies to investigate computer crimes or incidents. **(DISTINCTION)**

|  |
| --- |
| Type your answer here. |

**Topic 3: Progress Check**

|  |  |  |
| --- | --- | --- |
| **Topic** | **Confident**  **(Tick)** | **Need to revisit**  **(Tick)** |
| I know why it’s important to ensure evidence about an attack is accurate. |  |  |
| I know why it’s important to gather evidence immediately after an attack. |  |  |
| I know why it’s important to record all findings and consider how reliable the evidence is. |  |  |
| I know why it’s important to collect evidence about an attack that is relevant and correct. |  |  |
| I know why it’s important to record the facts and not opinions when collecting evidence about an attack. |  |  |
| I know why it’s important to evaluate evidence first before making recommendations on how to improve the security of a system. |  |  |

**Topic 3: Grade Yourself**

|  |  |
| --- | --- |
| **Grade Description** | **The statement that best describes my progress is…** |
| **Pass – Describe** how to ensure the outcomes from a systematic forensic analysis are trustworthy. |  |
| **Merit – Explain** the importance of gathering evidence that is correct, reliable, relevant and not intentionally imposed by the investigator. |  |
| **Distinction- Discuss** the benefits and drawbacks of allowing external agencies to investigate computer crimes or incidents. |  |
| **My strengths…..**  Type your answer here. | |
| **My areas for development…**  Type your answer here. | |

**End of Learning Aim E Review**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Topic** | **Checklist Item** | **Confidence** | | |
| **Low** | **Medium** | **High** |
| **Topic 1**  Desktop Forensics | I know what is meant by the term desktop forensics. |  |  |  |
| I know the different desktop forensic tools that can be used by an organisation to solve crimes. |  |  |  |
| I know the challenges of using live forensics data when analysing data. |  |  |  |
| **Topic 2**  Network Forensics | I know what is meant by the term network forensics. |  |  |  |
| I know the different network forensic tools that can be used by an organisation to solve crimes. |  |  |  |
| I know the impacts that network forensics may have on the performance of a network. |  |  |  |
| **Topic 3**  Systematic Forensic Analysis | I know why it’s important to ensure evidence about an attack is accurate. |  |  |  |
| I know why it’s important to gather evidence immediately after an attack. |  |  |  |
| I know why it’s important to record all findings and consider how reliable the evidence is. |  |  |  |
| I know why it’s important to collect evidence about an attack that is relevant and correct. |  |  |  |
| I know why it’s important to record the facts and not opinions when collecting evidence about an attack. |  |  |  |
| I know why it’s important to evaluate evidence first before making recommendations on how to improve the security of a system. |  |  |  |