Sample Assessment Materials (SAMs)

NCFE Level 3 Technical Occupational Entry in Cyber Security (Diploma)
QN: 610/4004/6

Version: v1.1 September 2025

Contents

Scenario: Cyber security Technician Role in a Financial Institution

Role: Cyber security technician

Company: Ventrose Finance

Industry: Financial services

Scenario Description:

Ventrose Finance has been trading for several years and has a good reputation for services and practices. Over the past few months, they have acquired several smaller businesses, one of which is Bonvane Holdings, and have some concerns about the security measures implemented within them. To assist with this Ventrose Finance is extending its cyber security team and have hired you as a cyber security technician. Your primary objective is to support the implementation and upkeep of cybersecurity measures and identify potential vulnerabilities and risks that could arise throughout the mergers.

Upon commencing your employment, you become a member of Ventrose Finance's cyber security team, which comprises of security analysts, engineers, and the Chief Information Security Officer (CISO). The CISO takes the lead in providing you with an overview of the organisations existing cybersecurity infrastructure, policies, and procedures. They also outline your specific responsibilities as a cyber security technician and emphasise the utmost importance of maintaining a secure environment.

As part of the merger, our team of cybersecurity experts will inspect the following areas:

- Network Infrastructure: evaluating the compatibility of network architectures, identifying any security gaps, and assessing the risk of unauthorised access
- Data Security: examining the protection mechanisms in place for sensitive financial data and identifying potential vulnerabilities
- Access Controls: reviewing user access management systems and protocols to ensure appropriate control over privileged accounts
- System Integration: assessing the risks associated with merging different systems, applications, and databases
- Incident Response: ensuring that robust incident response plans are in place to address security breaches or incidents that may occur during the merger

As a cyber security technician, you will be expected to support with the merger, undertaking projects as directed by your line manager. You will be provided with a brief overview of each project at the start of each unit to provide contextualisation of requirements.

The purpose of these projects is to gather a portfolio of evidence that will demonstrate your ability to undertake tasks required to work as a cyber security technician. While completing these tasks you should include evidence of research / planning and any conclusions and / or

recommendations should be justified. To support the tasks, working examples should be used where possible.

Unit 01

Project scenario

Ventrose Finance currently employs more than 1000 employees across multiple branches and offices. As a result of recent mergers, human resources (HR) have highlighted concerns about the number of new staff and their varying levels of understanding about cyber security principles and key concepts.

Task 1 – training document

Your line manager has asked you to create a training document (for example, report or presentation) that can be used with new staff to highlight the key concepts of cyber security and why this is important in ensuring the security of the organisation's systems and customer details.

To complete this task your training document should cover the following:

- the definitions of Confidentiality, Integrity, Availability (CIA) and Identification, Authentication, Authorisation, and Accountability (IAAA) and their importance on cyber security (AC1.1)
- a brief explanation for each of the core terminologies used in cyber security (AC1.2):
    - assurance
    - reliability
    - non-repudiation
    - access control
    - threat
    - vulnerability
    - risk
    - security breach
    - information security
    - attack vectors
    - attack surface
- how the role of information, assurance, and governance (IAG) can (AC1.3):
    - guide the development and improvement of processes
    - support the auditing of policies and processes
    - provide confirmation of compliance (AC1.3).

Submission:

Training document.

Learning outcomes (LOs) The learner will:	**Assessment criteria (AC)**	**Pass** The learner will be able to:	**Merit** The learner will be able to:	**Distinction** The learner will be able to:
1. Understand the key concepts within cyber security	1.1 The key concepts and importance of cyber security: CIA triad: • confidentiality • integrity • availability IAAA: • identification • authentication • authorisation • accountability	Outline the concepts of cyber security (as identified in AC1.1).	Explain how the key core concepts in cyber security are used by an organisation to ensure the safety of data and assets.	Analyse the importance of cyber security and its key concepts for an organisation to ensure its safety of data and assets.
	1.2 The use of core terminology in cyber security: • assurance • reliability • non-repudiation • access control • threat • vulnerability • risk • security breach • information security • attack vectors • attack surface	Identify the use of core terminology in cyber security (as identified in AC1.2).		

Learning outcomes (LOs) The learner will:	**Assessment criteria (AC)**	**Pass** The learner will be able to:	**Merit** The learner will be able to:	**Distinction** The learner will be able to:
	1.3 The role of information assurance, and governance (IAG): • to guide the development and improvement of policies and processes • to support the auditing of policies and processes • to provide confirmation of compliance (for example, with International Organisation of Standardization (ISO) standards)	Outline the role of IAG (as identified in AC1.3).	Explain how IAG plays an important role in the development, improvement and auditing of policies and processes, ensuring legal and organisational compliance.	Evaluate the importance IAG plays in the development, improvement and auditing of policies and processes, ensuring legal and organisational compliance.

Task 2 – 'New Joiners' guide

As part of the Ventrose Finance's degree apprenticeship scheme there are new employees that join each year who may have limited knowledge of cyber security due to this being their first job role. Some of the apprentices will be working across some of the different businesses acquired in the recent mergers.

You have been asked to create a 'new joiners' guide that will help them quickly understand cyber security and the impact that not adhering to this may have on the organisation.

To complete this task, you must produce a 'new joiners' guide which includes:

- how cyber security cultures can differ between (AC2.1):
  - different organisation types
  - stakeholders that the apprentice may encounter
- the importance of maintaining an effective cyber security culture in protecting the confidentiality of the organisation's information (AC2.2)
- the components and importance of an effective security culture (AC2.3)

- the techniques used to build and maintain an effective security culture (AC2.4)
- the impact of the organisation having an inadequate cyber security culture (AC2.5).

Submission:

'New joiners' guide

Learning outcomes (LOs) The learner will:	**Assessment criteria (AC)**	**Pass** The learner will be able to:	**Merit** The learner will be able to:	**Distinction** The learner will be able to:
2. Understand effective cyber security culture	2.1 The influence of organisational structures on cyber security culture: • stakeholders (for example, internal or external) • organisational types (for example, public or private)	Outline the influence of organisational structures on cyber security culture (as identified in AC2.1).	Discuss how the influence of organisational structures impact maintaining an effective cyber security culture that protects the confidentiality of an organisation's information.	Evaluate the importance of building and maintaining an effective security culture for different organisations and the stakeholders involved.
	2.2 The importance of maintaining an effective cyber security culture in protecting the confidentiality of an organisation's information	Identify the importance of maintaining an effective cyber security culture in protecting the confidentiality of an organisation's information.		
	2.3 The components and importance of an effective security culture	Outline the components and importance of an effective security culture.	Explain the components and techniques used to build and maintain an effective security culture and the impact of not adhering to this.	
	2.4 The techniques used to build and maintain an	Identify techniques used to building and maintain an		

	effective security culture	effective security culture.		
	2.5 The impact of an inadequate cyber security culture on an organisation (for example, unauthorised distribution or loss of data, reputational damage)	Outline the impact of an inadequate cyber security culture on an organisation.		

Task 3

Due to the varying backgrounds and experience resulting from the mergers, the HR department are keen for all employees to have a similar level of understanding of cloud-based working. All staff have been tasked with undertaking continuous professional development (CPD) to ensure that they have up-to-date knowledge regarding the components of a secure organisational infrastructure and a cloud environment.

Task 3a – leaflet

To support staff with their CPD you have been asked to create an information leaflet that informs staff about the components of a secure infrastructure within Ventrose Finance.

To complete this task your leaflet should consider:

- the components of secure infrastructure within Ventrose Finance (AC3.1):
  - hardware
  - software
  - operating systems (OS)
  - network resources

Task 3b – overview document

The senior management team are looking at outsourcing some of the organisation's digital services and have asked you to provide an overview of the following cloud services.

To complete this task you should provide an overview of each of the 3 cloud environments and consider the benefits that each one would offer to the organisation:

- the components of cloud environments (AC3.2):

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)

Submission:

Leaflet

Overview document

Learning outcomes (LOs) The learner will:	**Assessment criteria (AC)**	**Pass** The learner will be able to:	**Merit** The learner will be able to:	**Distinction** The learner will be able to:
3. Understand secure infrastructure and cloud environments	3.1 The components of a secure infrastructure within an organisation: • hardware • software • operating systems (Oss) • network resources.	Outline the components of a secure infrastructure within an organisation (as identified in AC3.1).	Explain the components of securing infrastructure and cloud environments within an organisation.	Analyse the benefits that secure infrastructure and cloud environments provide to cyber security.
	3.2 The components of cloud environments: • Infrastructure as a Service (IaaS) • Platform as a Service (PaaS) • Software as a Service (SaaS).	Outline the components of cloud environments (as identified in AC3.2).		

Unit 02

Project scenario

Ventrose Finance is aware of growing concerns in relation to the threat landscape and has decided to invest in a new project that will investigate a range of security measures that could be implemented for one of the newly acquired companies (Bonvane Holdings). Ventrose Finance does not want its current measures to influence this project so has requested that this investigation is conducted based on the assumption that there are currently no security measures in place.

Your line manager has requested that you support with the creation of a business case to request funding for your team to invest in the tools, systems and resources they will need. As part of this, you will need to produce a report that will form a supporting addition to the overall business case concerning possible threats to Bonvane Holdings, any vulnerabilities that are likely to arise from this, and subsequent risks.

Task 1a – business case report

This report will be considered by the senior management team (SMT) who are responsible for the allocation of funding. They will be non-specialists but will have a sharp eye for detail and will quickly find discrepancies.

Your report should include:

- an introduction to the threat intelligence lifecycle (AC1.1)
- an overview of how reliable sources can be used when gathering threat intelligence (AC1.2)
- identification of a range of threats, methods of identification and their potential impact on Bonvane Holdings (AC1.3 / AC1.4)
- identification of the different types and motivations of threat actors, including: (AC1.5):
    - nation state
    - script kiddies
    - cyber criminals
    - terrorist organisations
    - insiders
    - hacktivists
- a discussion of network reconnaissance techniques to identify threats, including: (AC1.6):
    - indicators of compromise (IOCs) from external threat intelligence sources
    - use of tools to scan and analyse network traffic
    - monitoring:
        - unusual volume of network traffic

- repeated attempts to access systems
- alerts from end points
- abnormal user behaviour
- unexpected system changes

Task 1b – threat intelligence gathering

Following a recent surge of cyber-attacks, your line manager has asked you to gather information about threats that could be a potential risk to Ventrose Finance. You will need to collate any information found and save this in an appropriate format.

To complete this task you must:

- perform routine threat intelligence gathering tasks using reliable sources and record the findings in a suitable format (AC1.7)

Submission:

Completed report

Evidence of threat intelligence gathering

Learning outcomes (LOs) The learner will:	**Assessment criteria (AC)**	**Pass** The learner will be able to:	**Merit** The learner will be able to:	**Distinction** The learner will be able to:
1. Understand cyber security threats and perform intelligence gathering	1.1 The function and features of the threat intelligence lifecycle	Outline the function and features of the threat intelligence lifecycle.	Explain the role of the threat intelligence lifecycle, clearly identifying the purpose of each phase.	Analyse potential threats and reconnaissance techniques, considering their motivations and impacts, and how the threat intelligence cycle can be used to anticipate and
	1.2 How to use reliable sources to contribute to threat intelligence gathering tasks (for example, MITRE ATT&CK®)	Outline how to use reliable sources to contribute to threat intelligence gathering tasks.		

Learning outcomes (LOs) The learner will:	**Assessment criteria (AC)**	**Pass** The learner will be able to:	**Merit** The learner will be able to:	**Distinction** The learner will be able to:
	1.3 The impact of threats on an organisation (for example, financial, data loss)	Identify the impact of threats on an organisation.	Explain the motivations of threat actors and the impact of different types of threats on organisations.	mitigate these threats.
	1.4 Types of threats and the methods used to identify them (for example, social engineering, ransomware, zero-day, commodity threat)	Identify the types of threats and the methods used to identify them.		
	1.5 The types and motivations of threat actors: • nation state • script kiddies • cyber criminals • terrorist organisations • insiders • hacktivists	Identify the types and motivations of threat actors (as identified in AC1.5).		
	1.6 The application of network reconnaissance techniques to identify threats: • indicators of compromise (IOCs) from external threat intelligence sources	Summarise the application of network reconnaissance techniques to identify threats (as identified in AC1.6).	Compare a range of network reconnaissance techniques and how these can be used to assist threat identification.	

Learning outcomes (LOs) The learner will:	**Assessment criteria (AC)**	**Pass** The learner will be able to:	**Merit** The learner will be able to:	**Distinction** The learner will be able to:

	• use of tools to scan and analyse network traffic
	• monitoring:
	  ○ unusual volume of network traffic
	  ○ repeated attempts to access systems
	  ○ alerts from end points
	  ○ abnormal user behaviour
	  ○ unexpected system changes			

	1.7 Perform routine threat intelligence gathering tasks using reliable sources	Demonstrate the ability to perform routine threat intelligence gathering tasks using reliable sources.		

Task 2 – training resource

You have been asked by your line manager to create an information security training and awareness resource, to remind staff of the characteristics of suspicious security activity.

To complete this task, you should create an information security training and awareness resource (AC2.3) which will include:

- a focus on the characteristics of unusual security activity and should consider both suspicious user and device behaviour, unauthorised system changes and any malware activity (AC2.1)
- a demonstration of how to follow information security procedures to maintain cyber security resilience (AC2.2)

Task 2b – monitoring effectiveness

Following the completion of the training resource your line manager has asked you to monitor the effectiveness of it on a minimum of three people.

To complete this task, you should:

- monitor the effectiveness of the resource by testing this on a minimum of three people and record any findings in an appropriate format (AC2.4)

Submission:

Information security training and awareness resource

Record of findings in an appropriate format of your choice

Learning outcomes (LOs) The learner will:	**Assessment criteria (AC)**	**Pass** The learner will be able to:	**Merit** The learner will be able to:	**Distinction** The learner will be able to:
2. Understand suspicious activities and potential breaches	2.1 The characteristics of unusual security activity: • suspicious user behaviour (for example, brute force attack) • suspicious device behaviour (for example, unusual network activity) • unauthorised system changes (for example, changes to network configuration) • malware activity (for example, IOCs)	Outline the characteristics of unusual security activity (as identified in AC2.1).	Explain how security procedures and training can be effective to increase awareness of a range of unusual security activity.	Evaluate the importance of understanding of how to identify unusual security activity and training methods for raising awareness with stakeholders.
	2.2 Follow information security procedures to maintain cyber security resilience	Demonstrate the ability to follow an information security procedure to maintain cyber security resilience.		

	2.3 Develop information security training and awareness resources to support good cyber security practice	Demonstrate the ability to develop information security training and awareness resources to support good cyber security practice.		
	2.4 Monitor the effectiveness of security awareness and training resources	Demonstrate the ability to monitor the effectiveness of security awareness and training resources.		

Task 3 – non-technical presentation

You are contacted by your line manger ahead of the meeting where the SMT will consider the business case for Bonvane Holdings. Some of SMT have asked for more information about cyber security issues to provide them with more detailed background information to assist them in understanding the business case. As the SMT are not subject experts, the information needs to be suitable for a non-technical audience.

You have been asked to create and record a 10 minute presentation to cover the following topics:

- a range of cyber security issues and how they are evolving. (AC3.1)
- identify how these issues can impact critical national infrastructure systems (AC3.2) including:
    - military and national defence
    - healthcare
    - transport
    - communication
    - utilities
    - supply chain
    - finance
    - operational technologies (OT)
- outline the importance of the threat landscape and the associated risks to internet of things (IoT) devices (AC3.3)

Submission:

Slides for presentation and a recording of the presentation

Learning outcomes (LOs) The learner will:	**Assessment criteria (AC)**	**Pass** The learner will be able to:	**Merit** The learner will be able to:	**Distinction** The learner will be able to:
3. Understand evolving cyber security issues	3.1 The types of cyber security issues and how these are evolving (for example, artificial intelligence (AI), quantum computing)	Identify types of cyber security issues and how these are evolving.	Explain how evolving cyber security risks and emerging technologies could impact critical national infrastructure and control systems.	Evaluate the threats that evolving cyber security risks and emerging technology may have on critical national infrastructure and control systems.
	3.2 How evolving cyber security issues can impact critical national infrastructure and control systems: • military and national defence (for example, leaking of classified information) • healthcare (for example, compromised confidentiality, ability to treat patients) • transport (for example, disruption to airlines, rail, smart motorways) • communication (for example, mass loss of service, interruptions	Identify how evolving cyber security issues can impact critical national infrastructure and control systems (as identified in AC3.2).		

	to business and society) • utilities (for example, water and sanitation, energy sources) • supply chain (for example, production of food) • finance (for example, disruption or failure of payment transactions) • operational technologies (OT) (for example, disruption to supervisory control and data acquisition (SCADA))			
	3.3 The importance of the threat landscape and the associated risks to internet of things (IoT) devices (for example, privacy, compromising other devices on network, trustworthy brand)	Outline the importance of the threat landscape and the associated risks to IoT devices.	Explain the importance of the threat landscape and the associated risks to IoT devices.	Evaluate the importance of the threat landscape and the associated risks to IoT devices.

Task 4a – report

Due to the recent mergers, there are now multiple approaches being used across the organisation for managing, storing and accessing digital assets.

Your line manager has asked you to write a report that identifies best practice for working with digital assets.

To complete this task the report should cover:

- the types of digital information assets and how they are securely stored and accessed in a controlled environment (AC4.1):
  - systems
  - services
  - devices
  - data storage

- how digital information assets are managed across cloud services (AC4.2)
- the importance and application of maintaining a digital information asset inventory (AC4.3)
- the importance and use of secure digital information asset disposal (AC4.4)

Task 4b – inventory log

It has been identified that one of the organisations, Bonvane Holdings, recently acquired by the merger, does not currently use an inventory log. Your line manager has asked you to design an inventory log and populate it with example information to demonstrate how this would be maintained.

To complete this task, you should include in the inventory log, as a minimum:

- example information relating to servers, computers and mobile devices (AC4.5)

Submission:

Report

Inventory log

Learning outcomes (LOs) The learner will:	**Assessment criteria (AC)**	**Pass** The learner will be able to:	**Merit** The learner will be able to:	**Distinction** The learner will be able to:
4. Understand and maintain digital information systems	4.1 The types of digital information assets and how they are securely stored and accessed in a controlled environment: • systems • services • devices • data storage	Outline of the types of digital information assets (as identified in AC4.1) and how they are securely stored and accessed in a controlled environment.	Compare a range of methods that may be implemented for storing and managing digital information assets and how they are managed across cloud services.	Evaluate a range of methods for storing and managing digital information assets, assessing their effectiveness and suitability across different cloud services.
	4.2 How digital information assets	Outline how digital information assets		

	are managed across cloud services	are managed across cloud services.		
	4.3 The importance and application of maintaining a digital information asset inventory (for example, compliance with ISO/IEC 27001 standard)	Outline the importance and application of maintaining a digital information asset inventory.	Discuss the importance of maintaining a digital information asset inventory and use of secure digital information asset disposal.	Evaluate the importance of maintaining an accurate inventory of digital information assets and implementing secure methods for their disposal to mitigate data loss and ensure compliance.
	4.4 The importance and use of secure digital information asset disposal (for example, data sanitisation)	Outline the importance and use of secure digital information asset disposal.		
	4.5 Maintain an inventory of digital information systems, services, devices and data storage	Demonstrate the ability to maintain an inventory of digital information systems, services, devices and data storage.		

Unit 03

The business case for funding has been approved and will provide the team with the tools needed to counter the potential threats that you have identified.

Prior to the funding approval it was identified that Bonvane Holdings has been operating a number of legacy systems. You need to identify how to assess the vulnerabilities of these current systems and how they can make sure that the current systems will work with any future systems that are procured. To manage this, the head of IT, who is a member of the Senior Management Team (SMT), has decided to set up a vulnerability assessment team, consisting of members of the IT department from Ventrose Finance and Bonvane Holdings. You have been seconded to work within this team. The vulnerability assessment team will examine existing systems and investigate potential new systems.

Task 1 information leaflet

As some of the SMT are unfamiliar with a wide range of cyber security vulnerabilities, you have been asked to create an information leaflet for them which covers:

- common vulnerability exposures and the impact these can have on an organisation (AC1.1):
  - software misconfiguration
  - broken access control and authentication
  - sensitive data exposure
  - injection vulnerabilities
  - using components with known vulnerabilities
  - insufficient logging and monitoring
  - security misconfiguration
  - incorrect cross-site validation

Submission:

Information leaflet

Learning outcomes (LOs) The learner will:	**Assessment criteria (AC)**	**Pass** The learner will be able to:	**Merit** The learner will be able to:	**Distinction** The learner will be able to:
1. Understand cyber security vulnerabilities	1.1 Common vulnerability exposures and the impact these can have on an organisation: • software misconfiguration (for example, authentication bypass, data loss) • broken access control and authentication (for example, unauthorised access) • sensitive data exposure (for example, reputational damage, fines) • injection vulnerabilities (for example, remote code execution, Denial of Service (DoS)) • using components with known vulnerabilities (for example, software security weakness) • insufficient logging and monitoring (for example, unacknowledged persistent threat)	Outline common vulnerability exposures (as identified in AC1.1) and the impact these can have on an organisation.	Compare a wide range of common vulnerability exposures, clearly identifying the impact each of these may have on an organisation.	Evaluate the impact cyber security vulnerabilities can have on an organisation.

Learning outcomes (LOs) The learner will:	Assessment criteria (AC)	Pass The learner will be able to:	Merit The learner will be able to:	Distinction The learner will be able to:
	• security misconfiguration (for example, lack of network restrictions or anti-virus protection) • incorrect cross-site validation (for example, session hijacking)			

Task 2

Bonvane Holdings IT team, needs to understand how to decide the scope of a risk assessment and which tools can be used to evaluate, manage and categorise the risk. Finally, they need to understand how to evaluate the results from an assessment that has been carried out and make recommendations based on this.

Task 2a – brief guide

Your line manager has asked you to produce a brief guide for using a risk matrix and risk register.

To complete this task the guide should include:

- the process of risk management and risk assessment to categorise threats, vulnerabilities and risks (AC2.1):
  - identification of the scope of the risk assessment
  - assessment of the risk using a scoring matrix
  - categorisation of the risk rating
  - recording, responding or escalating as appropriate
  - completing of business impact analysis

Task 2b – risk assessment

Based on the scenario (provided by your tutor) perform a digital information risk assessment (AC2.3) which comprises of a risk matrix and risk register that:

- identifies and categorises threats, vulnerabilities and risks in preparation for response or escalation (AC2.2)
- identifies when and how to escalate information security events in accordance with relevant procedures and standards (AC2.4)

Submission:

Guide

Risk matrix

Risk register

Learning outcomes (LOs) The learner will:	**Assessment criteria (AC)**	**Pass** The learner will be able to:	**Merit** The learner will be able to:	**Distinction** The learner will be able to:
2. Understand and categorise cyber security risks for escalation	2.1 The process of risk management and risk assessment to categorise threats, vulnerabilities and risks: • identification of the scope of the risk assessment • assessment of the risk using a scoring matrix (for example, probability versus impact) • categorisation of the risk rating (for example, apply a red,	Outline of the process of risk management and risk assessment (as identified in AC2.1) to categorise threats, vulnerabilities and risks.	Explain how risk assessments are used to categorise vulnerabilities and threats through the application of a detailed and accurate risk matrix and risk register.	Analyse the risk management process and risk assessment techniques used to categorise and prioritise cybersecurity risks, threats, and vulnerabilities

	amber, green (RAG) rating) • recording, responding or escalating as appropriate • completion of a business impact analysis			
	2.2 Categorise threats, vulnerabilities and risks in preparation for response or escalation	Demonstrate the ability to identify and categorise threats, vulnerabilities and risks in preparation for response or escalation.		
	2.3 Perform digital information risk assessments	Demonstrate the ability to perform digital information risk assessments.		
	2.4 Use own initiative to identify when and how to escalate information security events in accordance with relevant procedures and standards	Demonstrate the ability to identify when and how to escalate information security events in accordance with relevant procedures and standards.		

Task 3a – How To Guide

Bonvane Holdings has been operating a number of legacy systems. As part of the newly formed vulnerability assessment team your line manager has asked you to produce a ‘How to Guide’ which outlines how to assess the vulnerabilities of these current systems and make recommendations based on findings.

In order to complete this task your guide must include:

- any considerations for a vulnerability assessment scope (AC3.1) in relation to:

  - networks
  - computers
  - servers
  - business units
  - applications
- the use of Common Vulnerabilities and Exposures (CVE) and the Common Vulnerability Scoring System (CVSS) to evaluate vulnerabilities (AC3.2)
- how to make recommendations based on evidence gained from vulnerability assessment tools (AC3.4), including:
  - severity of the vulnerability
  - potential impact and risk on business
  - availability of resources (for example, time, finances)
  - acceptance of risk
  - potential mitigations
  - scope of mitigation projects

Task 3b – vulnerability assessment

Before any vulnerability assessments are completed on Bonvane Holdings live network your line manager has suggested that you complete a vulnerability assessment on a virtual network (provided by your tutor).

In order to complete this task, you must:

- define the scope and objectives of the vulnerability assessment and undertake any required network scanning (AC3.3) which must be documented (for example, log file, video, annotated screenshots)
- give an evaluation (for example, report, video, annotated screenshots) of the results of the vulnerability assessment (AC3.5)

Submission:

How to Guide

Evidence of vulnerability assessment

Learning outcomes (LOs)	Assessment criteria (AC)	Pass The learner will be able to:	Merit The learner will be able to:	Distinction The learner will be able to:

The learner will:				
3. Understand and evaluate vulnerability assessments	3.1 The considerations for a vulnerability assessment scope: • networks • computers • servers • business units • applications	Identify the considerations for a vulnerability assessment scope (as identified in AC3.1).	Discuss key considerations when defining the scope of a vulnerability assessment, and the tools and techniques used to conduct the evaluation.	Evaluate the planning, execution, and outputs of a vulnerability assessment, considering the effectiveness of chosen tools and how the results may inform further actions.
	3.2 The use of tools and techniques to evaluate vulnerability assessments: • Common Vulnerabilities and Exposures (CVE) • Common Vulnerability Scoring System (CVSS)	Identify the use of tools and techniques to evaluate vulnerability assessments (as identified in AC3.2).		
	3.3 The scope and objectives of vulnerability assessment	Demonstrate the ability to define the scope and objectives of a cyber security vulnerability assessment.		
	3.4 How to make recommendations based on evidence from vulnerability assessment tools: • severity of the vulnerability	Identify how to make recommendations based on evidence from vulnerability assessment tools (as identified in AC3.4).	Discuss how recommendations can be made based on the severity and impact of the vulnerability with consideration for potential	

	• potential impact and risk on business • availability of resources (for example, time, finances) • acceptance of risk • potential mitigations • scope of mitigation projects		mitigation techniques and resource constraints.	
	3.5 How to interpret the results of a cyber security vulnerability assessment	Demonstrate the ability to interpret the results of a cyber security vulnerability assessment.		

Task 4 – Leaflet

As a financial institution, it is important that in the event of a cyber security incident that any evidence is not compromised or contaminated. Therefore, your line manager has asked you to create a leaflet which outlines the concept of computer forensic principles.

To complete this task your leaflet must explain:

- the concept of computer forensic principles (AC4.1):
  - identification
  - preservation
  - analysis
  - documentation
  - presentation
- the importance of ensuring evidence is not contaminated or compromised (AC4.2)

Submission:

Leaflet

Learning outcomes (LOs) The learner will:	**Assessment criteria (AC)**	**Pass** The learner will be able to:	**Merit** The learner will be able to:	**Distinction** The learner will be able to:
4. Understand computer forensics	4.1 The concept of computer forensic principles: • identification (for example, the evidence that is presented, where it is stored and how it can be accessed) • preservation (for example, isolating, securing and preserving evidence) • analysis (for example, evidence-based conclusions) • documentation (for example, retained in line with legal retention periods) • presentation (for example, evidence presented to law enforcement for further investigation)	Outline the concept of computer forensic principles (as identified in AC4.1).	Explain the concepts of computer forensic principles with a focus on the key elements (as identified in AC4.1) to ensure that evidence is not compromised.	Evaluate the concept of computer forensics and the importance of maintaining evidence integrity to prevent contamination or compromise during collection, analysis, and storage
	4.2 The importance of ensuring evidence is not	Outline the importance of		

	contaminated or compromised (for example, continuity of evidence to support court cases)	ensuring evidence is not contaminated or compromised.		

Unit 04

The number of cyber security incidents across the United Kingdom is increasing and the organisation wants to assess that staff are fully aware of how to report and respond in the event of an incident happening.

Task 1a – presentation

Your line manager is aware that many of the staff will have had little experience with cyber security incidents and has asked you to create a presentation that he could deliver to all staff to help them understand the area.

The presentation should cover:

- an overview of the phases and application of the incident response lifecycle (AC1.1):
  - preparation
  - detection and analysis
  - containment
  - eradication and recovery
  - post-event activity and lessons learned
- the process of exception reporting of incidents (AC1.2)
- the reasons for regular management reporting (AC1.3)

Task 1b – draft template

Your line manager has asked you to create a draft information management report template that can be used to capture incidents and responses.

The template should include sections and guidance (AC1.4) on:

- the incident (how it was detected and potential risk)
- budgets available for remediation and next steps
- the infrastructure penetrated and damage caused
- a plan for returning affected services or systems
- a summary of the incident including the impact this had on the organisation
- any additional information that is relevant

Submission:

Presentation

Draft template

Learning outcomes (LOs) The learner will:	**Assessment criteria (AC)**	**Pass** The learner will be able to:	**Merit** The learner will be able to:	**Distinction** The learner will be able to:
1. Understand and create incident response documentation	1.1 The phases and application of the incident response lifecycle: • preparation • detection and analysis • containment • eradication and recovery • post-event activity and lessons learned	Outline the phases and the application of the incident response lifecycle (as identified in AC1.1).	Explain the phases of the incident response lifecycle and the importance reporting plays in the process, highlighting where reporting plays an important part in the process.	Analyse the incident response lifecycle, highlighting the significance of timely and accurate reporting throughout each stage.
	1.2 The application of exception reporting: • reporting of incidents (for example, breaches of information security policy)	Outline the application of exception reporting.		
	1.3 The application of management reporting: • regular reporting (for example, recent events, threat landscape)	Outline the application of management reporting.		
	1.4 Create draft information management reports using standard formats to meet requirements	Demonstrate the ability to create draft information management reports using		

Learning outcomes (LOs) The learner will:	Assessment criteria (AC)	Pass The learner will be able to:	Merit The learner will be able to:	Distinction The learner will be able to:
		standard formats to meet requirements.		

Task 2a – training video

Now that the draft report has been reviewed and signed off by your line manager, it can be implemented by Bonvane Holdings. To support with this, your line manager has requested that you create a training video to accompany this.

In order to complete this task you will need to create a training video that demonstrates the following topics:

- the importance of maintaining an up-to-date cyber security incident log as part of a chain of evidence (AC2.1)
- using the template previously created in task 1b, complete the log for a cyber security event (detail provided by your tutor) ensuring you explain how you have preserved any evidence gathered (AC2.2)

Learning outcomes (LOs) The learner will:	Assessment criteria (AC)	Pass The learner will be able to:	Merit The learner will be able to:	Distinction The learner will be able to:
2. Understand and create cyber security incident information documentation	2.1 The importance of maintaining an up-to-date cyber security incident log as part of a chain of evidence	Outline the importance of maintaining an up-to-date cyber security incident log as part of a chain of evidence.	Discuss why it is important to maintain an up-to-date cyber incident log and how this forms part of the chain of evidence.	Evaluate the importance of maintaining an up-to-date cyber incident log as part of a chain of evidence.
	2.2 Create cyber security event	Demonstrate the ability to create a		

	information documents and preserve evidence to meet requirements	cyber security event information document and preserve evidence to meet requirements.		

Task 2b – supplementary video

Upon reviewing your video from task 2a, your line manager would like further information on the subject. They have instructed you to explore monitoring systems and then record an additional section on how these work. The marketing team will be combining this with the original video upon completion.

In order to complete this task, you will need to create a supplementary video that:

- explains how different monitoring systems can be used to identify information security events (AC3.1)

To help illustrate this you should demonstrate and explain the use of any monitoring tool and provide step by step instructions and report on findings (AC3.2).

Submission:

Training video

Supplementary video

Learning outcomes (LOs) The learner will:	**Assessment criteria (AC)**	**Pass** The learner will be able to:	**Merit** The learner will be able to:	**Distinction** The learner will be able to:
3. Understand and monitor systems to identify information security events	3.1 The application of monitoring systems to identify information security events (for example, monitoring alerts, checking logs)	Outline how monitoring systems (as identified in AC3.1) are used to identify information security events.	Explain how monitoring systems are effectively used within an organisation as a method to check for security events.	Analyse the importance of implementing monitoring systems to identify, track, and respond to security events.

	3.2 Monitor and report information security events to meet requirements	Demonstrate the ability to monitor and report information security events to meet requirements.		

Task 3a – article

Ventrose Finance's internal newsletter editor has asked your team for an article in the forthcoming edition which has a theme of 'Business Continuity'. The Chief Information Security Officer (CISO) asks you to write an informative article for the magazine to help the staff understand what this is and how your team is helping provide support.

To complete this task your article should cover:

- the use of disaster prevention and recovery methods to support continuity of service planning (AC4.1)
  - disaster recovery plan (DRP)
  - business continuity plan (BCP)
- the purpose and use of secure onsite and offsite backup and recovery techniques (AC4.2)

Submission:

Completed newsletter article

Learning outcomes (LOs) The learner will:	**Assessment criteria (AC)**	**Pass** The learner will be able to:	**Merit** The learner will be able to:	**Distinction** The learner will be able to:
4. Understand disaster prevention and recovery	4.1 The use of disaster prevention and recovery methods to support continuity of service planning:	Outline the use of disaster prevention and recovery methods (as identified in AC4.1) to support the continuity of service planning.	Discuss the use of disaster prevention and recovery methods to support continuity of service planning.	Evaluate the effectiveness of disaster prevention and recovery methods in ensuring continuity of service.

	• disaster recovery plan (DRP) • business continuity plan (BCP)			
	4.2 The purpose and use of secure onsite and offsite backup and recovery techniques (for example, incremental, air-gapped)	Outline the purpose and use of secure on-site and off-site backup and recovery techniques		

Unit 05

As legislation and governance is vital for all sectors, the Senior Management Team (SMT) have specified that they would like a training course that could be used with staff from any department. They have not identified a preferred format for this but have suggested the following could be considered:

- the training course should be split into six sections
- the sections could be a mixture of audio / video, presentations, facts and figures as appropriate to maintain variety

Section 1 – understand information security governance

This section should focus on:

- the purpose of organisational security governance in relation to providing a framework for managing compliance with legislation, standards, policies and processes whilst supporting risk management (AC1.1)

Section 2 – understand and review cyber security policies

This section should focus on:

- the value of an information security management system (ISMS) to support compliance with cyber security standards in relation to people, processes and technology: (AC 2.1)
- how an ISMS system supports compliance with cyber security standards (AC 2.2)
- a video which demonstrates how to review and comment upon cyber security policies, procedures, standards and guidelines (AC2.3)

Section 3 – knowledge of legislation relating to cyber security

This section should focus on:

- the use of the following legislation and standards to support cyber security (AC 3.1):
    - Data Protection Act 2018
    - Regulation of Investigatory Powers Act 2000
    - Human Rights Act 1998
    - Computer Misuse Act 1990
    - Freedom of Information Act 2000
    - Official Secrets Act 1989
    - Wireless and Telegraphy Act 2006

  - Payment Card Industry Data Security Standard (PCI-DSS)
- explain ways in which an individual can maintain knowledge of legislation and industry standards relating to cyber security (AC3.2)

Section 4 – ethical considerations and codes of conduct

This section should focus on:

- ethical considerations when processing and storing data (AC4.1):
  - consent
  - contract
  - legal obligations
  - vital interests
  - public interest
  - legitimate interests
- the attributes of ethical codes of conduct within cyber security (AC4.2):
  - UK Cyber Security Council Code of Ethics
  - British Computer Society Code of Conduct
  - Ethics for Incident Response and Security Teams (EthicsfIRST)

Section 5 – cyber security policies and compliance

This section should focus on:

- the purpose and application of the following information security policies (AC5.1):
  - acceptable use policy
  - incident management policy
  - bring your own device (BYOD) policy
  - access control policy
  - social media policy
  - password policy
  - patch management policy
  - antivirus policy
  - information security policy
  - data classification and handling policy
  - IT asset disposal policy

- the concept of cyber security compliance (AC5.2)
- the use of compliance monitoring techniques (AC5.3)

Section 6 – cyber security auditing and performing compliance checks

This section should focus on:

- the purpose and application of cyber security audit requirements in line with organisational procedures (AC6.1)
- the importance of obtaining and documenting evidence in an appropriate form for review by an internal or external auditor (AC6.2)
- a video which demonstrates how to document audit requirements and collate relevant information from log files, incident reports and appropriate data sources (AC6.3)
- a video which demonstrates how to perform cyber security compliance checks (AC6.4)

Submission:

Completed training course

Learning outcomes (LOs) The learner will:	**Assessment criteria (AC)**	**Pass** The learner will be able to:	**Merit** The learner will be able to:	**Distinction** The learner will be able to:
1. Understand information security governance	1.1 The purpose of organisational security governance: • provides a framework for managing compliance with legislation, standards, policies and processes • supports risk management	Outline the purpose of organisational security governance (as identified in AC1.1).	Explain the purpose of organisational security governance.	Evaluate information security governance and its impact on organisational security.
2. Understand and review	2.1 The value of an information security management system	Outline the value of an ISMS to support	Explain the benefits an ISMS offers by	Evaluate the importance of an ISMS system to

cyber security policies	(ISMS) to support compliance with cyber security standards: • people • processes • technology	compliance with cyber security standards (as identified in AC2.1).	providing a framework to managing security risks, paying attention to compliance, policies and procedures.	ensure compliance with cyber security standards.
	2.2 How an ISMS system supports compliance with cyber security standards (for example, International Standards Organization (ISO) standards)	Identify how an ISMS system supports compliance with cyber security standards.		
	2.3 Review and comment upon cyber security policies, procedures, standards and guidelines	Demonstrate the ability to review and comment upon cyber security policies, procedures, standards and guidelines.		
3. Understand knowledge of legislation relating to cyber security	3.1 The use of current legislation and standards to support cyber security: • Data Protection Act 2018 • Regulation of Investigatory Powers Act 2000 • Human Rights Act 1998 • Computer Misuse Act 1990 • Freedom of Information Act 2000	Outline the use of current legislation and standards to support cyber security (as identified in AC3.1).	Discuss how current legislation and standards are used to guide cyber security within an organisation including methods used to maintain currency of knowledge.	Analyse how current legislation and standards influence cyber security within an organisation.

	• Official Secrets Act 1989 • Wireless Telegraphy Act 2006 • Payment Card Industry Data Security Standard (PCI DSS)			
	3.2 How to maintain knowledge of legislation and industry standards relating to cyber security	Outline how to maintain knowledge of legislation and industry standards relating to cyber security.		
4. Understand ethical considerations and codes of conduct	4.1 Ethical considerations when processing and storing data: • consent • contract • legal obligations • vital interests • public interest • legitimate interests	Outline the ethical considerations when processing and storing data (as identified in AC4.1).	Discuss codes of conduct may support with ethical considerations	Analyse the extent that codes of conduct support ethical considerations.
	4.2 The attributes of ethical codes of conduct within cyber security: • UK Cyber Security Council Code of Ethics • British Computer Society (BCS) Code of Conduct • Ethics for Incident Response and	Identify the attributes of ethical codes of conduct within cyber security (as identified in AC4.2).		

	Security Teams (EthicsfIRST)			
5. Understand cyber security policies and compliance	5.1 The purpose and application of common information security policies: • acceptable use policy • incident management policy • bring your own device (BYOD) policy • access control policy • social media policy • password policy • patch management policy • antivirus policy • information security policy • data classification and handling policy • IT asset disposal policy	Outline the purpose and application of common information security policies (as identified in AC5.1).	Discuss how policies are applied within an organisation and the techniques used to ensure cyber security compliance.	Evaluate the extent to which information security policies contribute to ensuring cyber security compliance, focusing on their effectiveness in mitigating risks, meeting requirements, and safeguarding assets.
	5.2 The concept of cyber security compliance (for example, compliance with legal or internal policy requirements)	Outline the concept of cyber security compliance.		
	5.3 The use of compliance monitoring	Identify the use of compliance		

	techniques (for example, audits)	monitoring techniques.		
6. Understand cyber security auditing and perform compliance checks	6.1 The purpose and application of cyber security audit requirements in line with organisational procedures (for example, scoping, planning)	Outline the purpose and application of cyber security audit requirements in line with organisational procedures.	Discuss the importance of cyber security audits and the techniques used to ensure these are conducted in line with organisational procedures to ensure these are in an appropriate format.	Evaluate the benefits of auditing and compliance and the techniques used within an organisation.
	6.2 The importance of obtaining and documenting evidence in an appropriate form for review by an internal or external auditor	Identify the importance of obtaining and documenting evidence in an appropriate form for review by an internal or external auditor.		
	6.3 Document audit requirements and collate relevant information from log files, incident reports and appropriate data sources	Demonstrate the ability to document audit requirements and collate relevant information from log files, incident reports and appropriate data sources.		
	6.4 Perform cyber security compliance checks	Demonstrate the ability to perform cyber security compliance checks.		

Unit 06

Due to staff shortages in Bonvane Holdings IT department, you have been seconded to their IT service desk for a month to:

- assist and to help raise the level of cyber security awareness among the other service desk staff as in the past there have been several instances where the service desk request has been incorrectly handled
- support with raising awareness of how customer information is secured within the organisation
- develop a sandbox that allows colleagues to develop their understanding of user access controls

Task 1 – knowledge base article

You have been asked to produce a knowledge base article that will be published on the service desk's knowledge base which is used as a source of information for handling incidents.

This article should include:

- the purpose and use of service desk delivery in resolving security issues (AC1.1)
- how and when to escalate a security ticket to a higher level (AC1.2)
- the importance of communicating accurately and appropriately during escalation (AC1.3)

Submission:

Knowledge base article

Learning outcomes (LOs) The learner will:	**Assessment criteria (AC)**	**Pass** The learner will be able to:	**Merit** The learner will be able to:	**Distinction** The learner will be able to:
1. Understand service desk delivery	1.1 The purpose and use of service desk delivery in resolving security issues	Outline the purpose and use of service desk delivery in resolving security issues.	Explain the purpose and use of service desk delivery in resolving security issues.	Analyse the importance of service desk delivery in resolving issues including accurate

Learning outcomes (LOs) The learner will:	**Assessment criteria (AC)**	**Pass** The learner will be able to:	**Merit** The learner will be able to:	**Distinction** The learner will be able to:
	1.2 How and when to escalate a security ticket to a higher level	Identify how and when to escalate a security ticket to a higher level.	Explain how and when to escalate a security ticket to a higher level.	communication when escalating tickets.
	1.3 The importance of communicating accurately and appropriately during escalation (for example, technical or non-technical audience)	Outline the importance of communicating accurately and appropriately during escalation.	Explain the importance of communicating accurately and appropriately during escalation.	

Task 2a – set of knowledge base articles

Staff have found the article that you produced very useful and they have requested more knowledge base articles that the team can use.

To complete this task, you must create a set of knowledge base articles that the service desk staff can use as required.

The knowledge base article should cover:

- the types of physical, procedural and technical cyber security controls (AC2.1)
- the use of common cyber security measures and tools in relation to (AC2.2):
  - patching
  - software updates
  - access control
  - password management
  - firewalls
  - security incident and event management (SIEM) tools
  - protection tools:

  - antivirus
  - anti-malware
  - anti-spam
- technical management and monitoring tools

Task 2b – user access controls

Your line manager wants to assess the ability of Bonvane Holdings IT staff to work effectively with user access controls so has requested that you set up a sandbox network that can be used to develop their skills. You have been provided with the following information.

For the exercise you will need access to two servers and two computers. These can be either physical or virtual machines (provided by course leader).

In order to complete this task, you will set up and configure the system for multiple users (AC2.4). For the purpose of this exercise any Internet Protocol (IP) address range can be used (or your course leader may provide this).

Evidence for this task can be screenshots or photos showing each step of the task completed and the observation checklist that should be signed by your course leader.

Task (covers AC2.3 / AC 2.5 / AC4.4)	**Completed**
Install a server operating system on the two servers. Use the most appropriate settings.	
Install an operating system on the two computers. Use the most appropriate settings.	
Install and configure Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) as required.	
Install and configure a directory service.	

All devices should be assigned an IP address using DHCP as appropriate.

Create the following groups in the directory service:

All staff
Marketing
HR
Reception
IT
SMT

Add the following users (additional users can be added as required):

John Doe	Administrator	IT
Jane Lynch	Standard User	HR
Jo Anne	Standard User	Marketing
Bill Lodly	Standard User	Reception
Jack Nimble	Standard User	SMT

Add Marketing, HR, Reception, IT and SMT to the ‘All staff’ group.

Create a suitable folder structure so that each group can have its own folder (based on the privileges identified below).

Apply the following privileges:

IT	Access all folders	Read and write
Marketing	Marketing folders	Read and write
HR	HR folders	Read and write
Reception	Reception folders	Read and write
SMT	HR folders Access all other folders	Read and write Read only
All staff	Shared drive	Read and write

Add a text file to each of the folders and test the access and privileges granted. Each user should be able to edit the text file that relates to their

access. You should provide evidence for each user, group and access rights.	

Student/tutor declaration: I confirm that all tasks have been completed and have been demonstrated to the tutor.

Student signature:
……

Tutor signature:
……

Submission:

Knowledge base article

Completed checklist and supporting evidence

Learning outcomes (LOs) The learner will:	**Assessment criteria (AC)**	**Pass** The learner will be able to:	**Merit** The learner will be able to:	**Distinction** The learner will be able to:
2. Understand, maintain and install cyber security controls	2.1 The types of cyber security controls: • physical (for example, door access) • procedural (for example, acceptable use policy, vulnerability management policy, security incident response procedure)	Outline the types of cyber security controls (as identified in AC2.1).	Compare the various types of security control along with the associated measures and tools used to implement them effectively.	Analyse the different types of security controls and the effectiveness of associated measures and tools in addressing specific cybersecurity threats.

	• technical (for example, firewalls, applications, user access control)			

	2.2 The application of common cyber security measures and tools:
	• patching
	• software updates
	• access control
	• password management
	• firewalls
	• security incident and event management (SIEM) tools
	• protection tools:
	  ○ anti-virus
	  ○ anti-malware
	  ○ anti-spam
	• technical management and monitoring tools (for example, cloud security posture management (CSPM), cloud-native application
		Outline the application of common cyber security measures and tools (as identified in AC2.2).		

	protection platform (CNAPP))			
	2.3 Maintain information security controls and measures	Demonstrate the ability to maintain information security controls and measures.		
	2.4 Use a structured approach to manage and assess the validity of security requests from a range of stakeholders	Demonstrate the ability to use a structured approach to manage and assess the validity of security requests from a range of stakeholders.		
	2.5 Use technical procedures to install and maintain technical security controls	Demonstrate the ability to use technical procedures to install and maintain technical security controls.		

Task 3 – infographic

Ventrose Finance wants to reassure all customers that they take cyber security seriously. They have decided to email out an infographic to their customers highlighting key information around the use of cryptography and digital certificates to ensure the security of their customers details.

To complete this task, you should produce an infographic document that includes information on:

- the purpose of cryptography in (AC3.1):
  - prevention of eavesdropping of information

  - prevention of tampering of information to ensure integrity of data
  - assurance of authenticity of information
  - secure storage of sensitive data
- types of cryptographic techniques used (AC3.2):
  - hashing
  - symmetric encryption
  - asymmetric encryption
- the use of digital certificates (AC3.3):
  - to verify identity of users
  - to verify servers
  - to sign data to prove authenticity
  - to secure communications in transit
- the purpose of certificate management tools to (AC3.4):
  - generate certificate signing requests
  - sign new certificates
  - secure management of keys
  - track expired certificates
  - revoke compromised certificates

Submission:

Infographic

Learning outcomes (LOs) The learner will:	**Assessment criteria (AC)**	**Pass** The learner will be able to:	**Merit** The learner will be able to:	**Distinction** The learner will be able to:
3. Understand cryptography and digital certificates	3.1 The purpose of cryptography in cyber security: • eavesdropping of information	Outline the purpose of cryptography in cyber security (as identified in AC3.1).	Explain the purpose of cryptography in cyber security and the different types and techniques	Evaluate the effectiveness of cryptography and digital certificates in maintaining a secure and

	• prevention of tampering of information to ensure integrity of data • assurance of authenticity of information • secure storage of sensitive data		used to ensure confidentiality.	trustworthy environment.
	3.2 Types of cryptographic techniques in cyber security: • hashing • symmetric encryption (for example, Blowfish, Twofish) • asymmetric encryption (for example, Rivest Shamir Adleman (RSA), Diffie-Hellman)	Outline the types of cryptography in cyber security (as identified in AC3.2).		
	3.3 The use of digital certificates: • to verify the identity of users • to verify servers • to sign data to prove authenticity	Outline the use of digital certificates (as identified in AC3.3).	Explain the reasons for using digital certificates and discuss the tools used to manage these.	

	• to secure communications in transit			
	3.4 The purpose of certificate management tools: • generating certificate signing requests • signing new certificates • secure management of keys • tracking expired certificates • revoking compromised certificates	Outline the purpose of certificate management tools (as identified in AC3.4).		

Task 4 – presentation

To address the staffing issues previously identified, the IT Department has assigned two apprentices to the service desk. As they are new to this role, you have been asked by your line manager to create a presentation that will help them understand the purpose of modifying and using access controls.

To complete this task, you must create a short presentation to cover the following:

- the principles of identity and access management including authentication, authorisation and federation (AC4.1)
- the types and application of the following access controls (AC4.2):
  - mandatory access control (MAC)
  - discretionary access control (DAC)
  - attribute-based access control (ABAC)
  - role-based access control (RBAC)
  - rule-based access control (RuBAC)
- the relationship between privacy and access rights and access control (4.3)

Submission:

Presentation

Learning outcomes (LOs) The learner will:	**Assessment criteria (AC)**	**Pass** The learner will be able to:	**Merit** The learner will be able to:	**Distinction** The learner will be able to:
4. Understand and modify access controls	4.1 The principles of identity and access management: • authentication • authorisation and federation	Outline the principles of identity and access management (as identified in AC4.1).	Discuss the role access management and access controls mechanisms play in securing systems and data.	Evaluate the significance of access management and access control practices in maintaining robust cyber security.
	4.2 The types and application of access control: • mandatory access control (MAC) • discretionary access control (DAC) • attribute-based access control (ABAC) • role-based access control (RBAC) • rule-based access control (RuBAC)	Outline the types and application of access control (as identified in AC4.2).		
	4.3 The relationship between privacy and access rights and access control	Outline the relationship between privacy and access rights and access control.		
	4.4 Review and modify access rights to digital information systems, services, devices or data	Demonstrate the ability to review and modify access		

		rights to digital information systems, services, devices or data.		

AC4.4 is met in Task 2b

Unit 07

Project scenario

As the merger with Bonvane Holdings has been successfully completed, your line manager has nominated you as a member of a new multidisciplinary team, which will focus on a holistic approach to digital transformation throughout the organisation and on supporting staff through their ongoing continuous professional development (CPD) to ensure currency and reliability of their knowledge.

Task 1 – report on digital transformation

Now the merger is complete, a digital transformation project is being undertaken for the purchase of a new service desk. Your line manager has asked you to investigate the impact that this digital transformation project could have on the IT team and how the data gained from this can be used to improve stakeholder relationships. They have asked you to create a report to be shared with all heads of department across the company.

In order to complete this task, you will need to create a report that discusses the impact that the new service desk could have on day-to-day operations (AC1.1).

This report should consider:

- customer issues and problems
- business value
- brand awareness
- cultural/diversity awareness
- internal and external stakeholders:
    - user experience
    - accessibility
    - level of technical knowledge

Submission:

Report

Learning outcomes (LOs) The learner will:	**Assessment criteria (AC)**	**Pass** The learner will be able to:	**Merit** The learner will be able to:	**Distinction** The learner will be able to:

1. Understand digital transformation	1.1 The impact of digital transformation (for example, new IT system) on cyber security occupations and within an overall business context:
	• customer issues and problems
	• business value
	• brand awareness
	• cultural/diversity awareness
	• internal and external stakeholders:
	  ○ user experience
	  ○ accessibility
	  ○ level of technical knowledge
		Outline the impact of digital transformation on cyber security roles and business operations.	Discuss ways in which the impact of digital transformation can be managed effectively, ensuring minimal disruption.	Evaluate the impact of digital transformation on cyber security occupations and its broader impact on business operations.

Task 2 – cyber security occupations

HR wants to standardise all the cyber occupations across all the newly merged companies within Ventrose Finance. For this they need to get a clearer understanding of what these occupations entail and have requested information from your department. Your line manager has asked you to research and collate information in an appropriate format of your choosing.

In order to complete this task, your response must:

- identify a range of cyber security occupations and the skills required within each of these (AC2.1)

- explore how these different occupations interact with other roles in the digital sector (AC2.1)
- consider how current regulatory requirements influence the range of cyber security occupations (AC2.2)
- discuss how current regulations may evolve and the impact this could have on cyber security occupations (AC2.3)

Submission:

Research information in a format of your choice

Learning outcomes (LOs) The learner will:	**Assessment criteria (AC)**	**Pass** The learner will be able to:	**Merit** The learner will be able to:	**Distinction** The learner will be able to:
2. Understand cyber security occupations and regulatory requirements	2.1 The skill requirements for different cyber security occupations and how these fit into the wider digital landscape	Outline the skill requirements for different cyber security occupations and how these fit into the wider digital landscape.	Compare different cyber security occupations, considering the influence regulatory requirements may have on them and how these may evolve over time.	Analyse the impact of regulatory requirements on various cyber security occupations and how these roles may evolve in response to this.
	2.2 The influence of current regulatory requirements on cyber security occupations	Outline the influence of current regulatory requirements on cyber security occupations.		
	2.3 How cyber security regulations may evolve in the future	Identify how cyber security regulations may evolve in the future.		

Task 3 – CPD

Ventrose Finance recognises the importance of self-reflection and continuous professional development (CPD) and expects all staff to regularly assess their own development needs. This is a three-step process which is repeated on a yearly basis.

To complete this task, you must complete the following three steps (in an appropriate format of your choosing):

Step 1

- you should explain how learning techniques such as self-reflection and evaluation support and contribute to your own CPD (AC3.1)

Step 2

- you should explain how professional networks and academic journals can be used to improve your own CPD – you should also consider any other sources of knowledge that can be used to improve your knowledge and skills (AC3.2)

Step 3

- you should explore the skills and knowledge required for a range of cyber security roles and then complete a skills gap analysis that would review your own development needs to meet these roles – you should consider how you would develop these skills over the next 12 months (AC3.3)

Submission:

CPD document

Learning outcomes (LOs) The learner will:	**Assessment criteria (AC)**	**Pass** The learner will be able to:	**Merit** The learner will be able to:	**Distinction** The learner will be able to:
3. Understand learning techniques and sources of knowledge	3.1 How learning techniques (for example, evaluation and reflection) contribute to continuing	Outline how learning techniques contribute to CPD of cyber	Compare different types of learning techniques that contribute to	Evaluate the effectiveness of different types of learning techniques that contribute to CPD

and review own development needs	professional development (CPD) of cyber security occupations	security occupations.	CPD in the field of cyber security.	in the field of cyber security.
	3.2 A range of sources of knowledge and verified information applicable to cyber security occupations (for example, professional networks, academic publications)	Identify a range of sources of knowledge and verified information applicable to cyber security occupations.	Discuss a range of sources of knowledge and verified information used to support own professional development in the field of cyber security.	Analyse a range of sources of knowledge and verified information used to support own professional development in the field of cyber security.
	3.3 Review own development needs to keep up to date with emerging technologies and trends within cyber security	Demonstrate the ability to review own development needs to keep up-to-date with emerging technologies and trends within cyber security.		

Task 4 – information poster

As this is a newly formed team, your line manager has asked you to create an informational poster to be displayed on all internal notice boards to outline the purpose and roles of the multidisciplinary team whilst considering some of its values.

To complete this task, your information poster must contain the following:

- the purpose of a multidisciplinary team (AC4.1)
- how the roles within a multidisciplinary team are identified (AC4.2)
- the value of communication within multidisciplinary teams (AC4.3)

Submission:

Information poster

Learning outcomes (LOs) The learner will:	**Assessment criteria (AC)**	**Pass** The learner will be able to:	**Merit** The learner will be able to:	**Distinction** The learner will be able to:
4. Understand multidisciplinary teams and apply communication skills to share information	4.1 The purpose of a multidisciplinary team	Outline the purpose of a multidisciplinary team.	Explain the benefits and limitations of implementing multidisciplinary teams using relevant working examples.	Evaluate how effectively multidisciplinary teams can address cyber security challenges.
	4.2 How the roles within a multidisciplinary team are identified	Outline how the roles within a multidisciplinary team are identified.		
	4.3 The value of communication within multidisciplinary teams	Outline the value of communication within multidisciplinary teams.	Explain the benefits and limitations of applying communication skills using appropriate technical and non-technical terminology to share information with stakeholders.	Evaluate the effective application of communication skills using appropriate technical and non-technical terminology; teams can address cyber security challenges.
	4.4 Apply communication skills using appropriate technical and non-technical terminology to share information with stakeholders (for example, within a multidisciplinary team)	Demonstrate the ability to apply communication skills using appropriate technical and non-technical terminology to share information with stakeholders.		

AC4.4 is met through the following two tasks:

Unit 2 task 3 (AC3.1 / AC3.2 / AC3.3) – non-technical presentation to SMT

Unit 4 task 2a (AC2.2) – use of technical terminology within the incident report log.

Task 5 – training video

Following on from the recent mergers, HR have refreshed the values and behaviours policy. To support staff in their ongoing CPD, they have requested the creation of an updated training video.

To complete this task, you must create a short training video which covers the following areas:

- the value of working independently and taking responsibility for your own actions (AC5.1)
- how to manage own time to meet deadlines and manage stakeholder expectations (AC5.2)
- the importance of treating all stakeholders fairly and with respect without bias or discrimination (AC5.3)

Submission:

Training video

Learning outcomes (LOs) The learner will:	**Assessment criteria (AC)**	**Pass** The learner will be able to:	**Merit** The learner will be able to:	**Distinction** The learner will show evidence of:
5. Understand independent working, time management and stakeholder engagement	5.1 The value of working independently and taking responsibility for own actions	Outline the value of working independently and taking responsibility for own actions.	Explain how to work independently, manage own time to meet deadlines and manage stakeholder expectations.	Evaluate the benefits of working independently, manage time effectively to meet deadlines, and handle stakeholder expectations in cyber security projects.
	5.2 How to manage own time to meet deadlines and manage stakeholder expectations	Outline how to manage own time to meet deadlines and manage stakeholder expectations.		
	5.3 The importance of treating all stakeholders fairly and with respect without bias or discrimination	Outline the importance of treating all stakeholders fairly and with respect without bias or discrimination.	Explain the importance of treating all stakeholders fairly and with respect, without bias or discrimination.	Evaluate the importance of treating all stakeholders fairly and with respect, without bias or discrimination.

Change history record

Version	Description of change	Date of Issue
v0.1	First draft	May 2023
V0.2	Second draft	April 2025
V1.0	First publication	August 2025
V1.1	Grade descriptors update following publication	September 2025