Sample Assessment Materials (SAMs) (holistic)

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

Version: 1.0 August 2025

Contents

Evidence of a holistic approach to SAMs for L3 Cyber Security

In this specific example unit 7 AC4.4 (“apply communication skills using appropriate technical and non-technical terminology to share information with stakeholders (for example, within a multidisciplinary team”)) is met within the following previous units:

- Unit 1 task 1 (AC1.1 / AC1.2) – training document
- Unit 2 task 3 (AC3.1 / AC3.2 / AC3.3) – non-technical presentation to Senior Management Team (SMT)
- Unit 4 task 2a (AC2.2) – use of technical terminology within the incident report log.

Whilst the units themselves are numbered there is no requirement to deliver the content sequentially. Centres may find that the delivery order of units may influence the most effective holistic assessment opportunities.

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 data.

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

- the definitions of Confidentiality, Integrity and Availability (CIA) and Identification, Authentication, Authorisation, and Accountability (IAAA) and their importance on cyber security (Unit 1 AC1.1 / Unit 7 AC4.4)
- an explanation for each of the core terminologies used in cyber security (Unit 1 AC1.2 / Unit 7 AC4.4):
    - 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 (Unit 1 AC1.3):
    - guide the development and improvement of processes
    - support the auditing of policies and processes
    - provide confirmation of compliance (Unit 1 AC 1.3)

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 and importance 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 Organization 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.

Unit 02

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 (Unit 2 AC3.1 / Unit 7 AC4.4)
- how these issues can impact critical national infrastructure systems (Unit 2 AC3.2 / Unit 7 AC4.4) 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 (Unit 2 AC3.3 / Unit 7 AC4.4)

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	3.1 The types of cyber security issues and how these are evolving (for example, artificial	Identify types of cyber security issues and how these are evolving.	Explain how evolving cyber security risks and emerging technologies	Evaluate the threats that evolving cyber security risks

security issues	intelligence (AI), quantum computing)		could impact critical national infrastructure and control systems.	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 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))	Identify how evolving cyber security issues can impact critical national infrastructure and control systems (as identified in AC3.2).		
	3.3 The importance of the threat landscape and the	Outline the importance of	Explain the importance of	Evaluate the importance of

	associated risks to internet of things (IoT) devices (for example, privacy, compromising other devices on network, trustworthy brand)	the threat landscape and the associated risks to IoT devices.	the threat landscape and the associated risks to IoT devices.	the threat landscape and the associated risks to IoT devices.

Unit 04

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 it.

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 (Unit 4 AC2.1)
- using the template previously created in task 1b of the unitised SAMs, complete the log for a cyber security event (detail provided by your tutor) ensuring you explain how you have preserved any evidence gathered (Unit 4 AC2.2 / Unit 7 AC4.4)

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 explain 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 information documents and preserve evidence to meet requirements	Demonstrate the ability to create a cyber security event information document and preserve evidence to meet requirements.		

Unit 07

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	4.4 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.	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.

AC4.4 is met through the following three tasks:

Unit 1 task 1 (AC1.1 / 1.2) – training document

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

Unit 4 task 2a (AC 2.2) – use of technical terminology within the incident report log.

Change history record

Version	Description of change	Approval	Date of Issue
V0.1	First draft (holistic SAMs)		November 2023
V0.2	Second draft		April 2025
V1.0	First publication		August 2025