Next Generation Higher National Unit Specification

Cyber Security (SCQF level 7)

Unit code: J68N 47

SCQF level: 7 (16 SCQF credit points)

Valid from: session 2022–23

Prototype unit specification for use in pilot delivery only (version 1.0) May 2022

This unit specification provides detailed information about the unit to ensure consistent and transparent assessment year on year.

This unit specification is for teachers and lecturers and contains all the mandatory information required to deliver and assess the unit.

This edition: May 2022 (version 1)

Unit purpose

This non-specialist unit is designed for a wide range of learners with an interest in the key concepts and practices in cyber security. It is particularly suitable for learners with a vocational interest in STEM or progression to university to study cyber security or networking.

Learners should have appropriate IT literacy skills before doing this unit, but they do not need to have any previous experience of cyber security.

The aim of this unit is to introduce learners to the principles and fundamental concepts of cyber security, and provide essential practical skills in this field. Learners are introduced to the main types of vulnerabilities and attacks, and how they affect IT infrastructure. They also explore different types of systems at risk. Attacker motivation and risk and incident response planning is examined as well as the role of corporations, governments and individuals in the field of cyber security.

The unit also examines the main legislation and guidance on implementing secure systems. Throughout the unit, key terminology is introduced to help enforce an understanding of the subject.

On completion of this unit, learners may progress to the Cyber Security unit at SCQF level 8.

Unit outcomes

Learners who complete this unit can:

1 explain the principles of cyber security
2 explain the causes and effects of cyber threats and attacks
3 perform risk mitigation analysis
4 install a host-based intrusion detection system
5 install and secure a command line operating system

Evidence requirements

Learners must provide both knowledge and product evidence.

Knowledge evidence

Learners should produce the knowledge evidence for this without help. They must demonstrate that they have met all the knowledge points listed in the 'Knowledge and skills' section.

Product evidence

Product evidence comes from a number of practical tasks. These must include:

- installing a host-based intrusion detection system
- installing a command line operating system and implementing operating system security
- creating a risk impact matrix
- producing base common vulnerability scoring system (CVSS) scores

The standard of evidence should be consistent with the SCQF level of this unit.

Learners can produce evidence over an extended period under lightly controlled conditions. They must generate evidence without significant help.

Knowledge and skills

The following table shows the knowledge and skills covered by the unit outcomes:

Knowledge	Skills
Learners should understand: ♦ a brief overview of the history of cyber security ♦ publicised security breaches including the types of attack and their impact ♦ the terms 'risk', 'threat' and 'vulnerability' in a cyber security setting ♦ relevant legislation and ethics, including the tension between security and privacy ♦ the role of governments and large corporations ♦ the types of system that are vulnerable to cyber-attack ♦ the process of confidentiality, integrity and availability (CIA) in securing a system ♦ common attack vectors and mitigation ♦ types of cyber attacker ♦ common types of cyber-attack and mitigation ♦ common software vulnerabilities (secure coding) ♦ computer protection techniques ♦ types of risk, both internal and external ♦ risk mitigation ♦ end-user training	Learners can: ♦ perform the installation of a host-based intrusion detection system ♦ install a command line operating system and implement operating system security ♦ create risk impact matrices ♦ produce base CVSS scores

Meta-skills

Throughout the unit, learners develop meta-skills to enhance their employability in the computing sector.

Self-management

These meta-skills include:

- focusing: attention, filtering
- adapting: self-learning
- initiative: self-motivation

Social intelligence

These meta-skills include:

- communicating: receiving information, listening
- collaborating: teamworking and collaboration

Innovation

These meta-skills include:

- creativity: visualising
- sense-making: holistic thinking
- critical thinking: logical thinking, computational thinking

Literacies

Throughout this unit, learners have opportunities for the development of literacies.

Communication

Learners can develop their communication skills by producing reports.

Digital

This unit contributes towards learners' digital skills.

Delivery of unit

This unit introduces learners to cyber security and does not rely on them having any previous knowledge or skills. You can deliver this unit on a stand-alone basis; however, opportunities may exist for integration with networking units.

We suggest the following distribution of time:

Outcome 1 — Explain the principles of cyber security
(10 hours)
Outcome 2 — Explain the causes and effects of cyber threats and attacks
(10 hours)
Outcome 3 — Perform risk mitigation analysis
(20 hours)
Outcome 4 — Install a host-based intrusion detection system
(20 hours)
Outcome 5 — Install and secure a command line operating system
(20 hours)

Additional guidance

The guidance in this section is not mandatory.

You can deliver this unit on its own or as part of a group award. If you deliver it as part of a group award, you can combine assessment with other units within the award. Learners need a significant body of knowledge to carry out practical activities.

Learners should spend half of their time acquiring knowledge and half of their time applying knowledge. We recommend that you provide them with case studies of how cyber security is used in a wide range of vocational areas, such as finance and technology.

You can use a variety of software to carry out practical activities, such as IP or NF Tables, Kali Linux, Tripwire (or alternatives such as OSSEC or Splunk), CentOS/RHEL or Debian/Ubuntu.

You should explain the use cases for each type of software and introduce learners to common Command Line Interface techniques such as editing, updating and saving configuration files.

You can start the assessment when learners have the underpinning knowledge, and have gained experience of carrying out analyses.

Explain the principles of cyber security (outcome 1)

This is a broad outcome where learners can describe the history of cyber-attacks. You should include case studies of organisations that have been the subject of cyber-attacks and the cost to the organisation both directly and indirectly, such as reputational damage.

Learners should clearly define risk, threat and vulnerability:

- Threat: A potential attack or loss of data that might happen.
- Vulnerability: An inherent weakness that can be exploited.
- Risk: The metric used to understand loss. Risk can be calculated by using the formula: Risk = threat probability × potential loss ÷ impact.

In this outcome, learners should define the types of cyber-attack, and cover the laws that protect against data loss and cyber-attacks.

Explain the causes and effects of cyber threats and attacks (outcome 2)

This outcome covers the strategies developed by hackers to attack networks and the counter-measures deployed to prevent and defend against such attacks. You should cover system vulnerabilities, attack vectors and threat actors. Learners need to understand organisational security and how an effective security policy can help prevent, defend and recover from a cyber-attack.

Perform risk mitigation analysis (outcome 3)

This outcome covers risk as the likelihood of data loss, leading to potential reputational or financial loss. Learners should measure risk from zero, to low, medium, then high. They can quickly categorise risk with a red, amber, or green rating.

The three factors that feed into a risk vulnerability assessment are:

1 What is the threat?
2 How vulnerable is the system?
3 What is the reputational or financial damage if breached or made unavailable?

Learners can calculate cyber risk with the formula of cyber risk = threat × vulnerability × information value. The matrix is calculated based on a case study and can be used towards the relevant NIST or ISO standard.

Learners should use the CVSS during a risk mitigation analysis. The CVSS is a free and open industry standard for assessing the severity of computer system security vulnerabilities. There are publicly available CVSS score calculators that produce a base score and indicate the severity of a vulnerability.

Currently, there are free CVSS score calculators provided by FIRST, NIST and CISCO:

- Common Vulnerability Scoring System Version 3.1 Calculator (FIRST)
- NVD — CVSS v3 Calculator (NIST)
- Common Vulnerability Scoring System (CISCO)

Install a host-based intrusion detection system (outcome 4)

Learners should carry out the installation and configuration of a host-based intrusion detection system that is defined as an application monitoring a computer or network for suspicious activity.

This can include intrusions by external actors as well as misuse of resources or data by internal ones. For example:

- Tripwire — paid for
- OSSEC — open source
- Splunk — free version available
- Samhain — free

Install and secure a command line operating system (outcome 5)

This outcome requires learners to install and secure a command line operating system. We recommend that learners install a Linux build and secure the build. You should encourage them to run the CVSS before and after securing the build and compare the scores. The score should much improve after the system is secured.

To secure the system, we recommend that learners install at least the following:

- anti-virus software
- anti-malware software
- a firewall

Approaches to assessment

Learners can generate knowledge and skills evidence with two reports, one theoretical and one practical.

The theoretical report involves the design of a security recommendation document for management, given a scenario of a company that describes a variety of systems.

This report should refer to the history of cyber security and the publicised security breaches that led us to where we are now. Learners should clearly define the terms ‘risk’, ‘threat’ and ‘vulnerability’ and outline relevant industry best-practice, legislation and the role of governments and large corporations.

Reports should take the information from the case study and discuss the following in context:

- types of system vulnerable to cyber-attack
- types of cyber-attacker
- common types of cyber-attack and mitigation
- common attack vectors and mitigation
- the process of confidentiality, integrity and availability (CIA) in securing a system
- common software vulnerabilities (secure coding)
- computer protection techniques
- types of risk, both internal and external
- risk mitigation
- end-user training

The practical report could involve the implementation of a secure operating system. It should also include the configuration of a stateful firewall and a host-based intrusion detection system (HIDS). The report should include evidence of completion of the tasks, such as screenshots and/or logs of the installation and security tasks.

Learners can produce their reports over a period and under lightly controlled conditions, allowing them to refer to notes. A suggested minimum word count is 1000 words.

Alternatively, learners could maintain a portfolio of digital artefacts throughout the life of the unit. They would produce the portfolio over the life of the unit, adding their best work as and when produced. They can do this under lightly controlled conditions, in which case authentication is vital.

Equality and inclusion

This unit is designed to be as fair and as accessible as possible with no unnecessary barriers to learning or assessment.

You should take into account the needs of individual learners when planning learning experiences, selecting assessment methods or considering alternative evidence.

Guidance on assessment arrangements for disabled learners and/or those with additional support needs is available on the assessment arrangements web page: www.sqa.org.uk/assessmentarrangements.

Information for learners

Cyber Security (SCQF level 7)

This section explains:

- what the unit is about
- what you should know or be able to do before you start
- what you need to do during the unit
- opportunities for further learning and employment

Unit information

This is a non-specialist unit, designed for a wide range of learners with an interest in the key concepts and practices in cyber security. It is particularly suitable if you have a vocational interest in STEM or progression to university to study cyber security or networking. You should have appropriate IT literacy skills before doing this unit, however you do not need previous experience of cyber security.

The aim of this unit is to introduce you to the principles and fundamental concepts of cyber security, and provide essential practical skills in this field.

You are introduced to the main types of vulnerabilities and attacks, and how they affect IT infrastructure. You also explore different types of systems at risk. You examine attacker motivation and risk and incident response planning, as well as the role of corporations, governments and individuals in the field of cyber security.

The unit also covers the main legislation and guidance provided for implementation of secure systems.

Throughout the unit, you are introduced to key terminology that helps to enforce your understanding of the subject.

During this unit you learn about:

- the principles of cyber security
- the causes and effects of cyber threats and attacks
- performing risk mitigation analysis
- installing a host-based intrusion detection system (HIDS)
- installing and securing a command line operating system

Your knowledge of the subject and your practical skills are assessed and there are various ways to do this. One method is to create two reports, one theoretical and one practical, to assess your skills and knowledge.

Throughout the unit, you develop meta-skills. Meta-skills are timeless, higher-order skills that support the development of additional skills and promote future success. These meta-skills include self-management (such as focusing, adapting and initiative), social intelligence (such as communicating and collaborating), and innovation (such as creativity, sense-making and critical thinking).

Administrative information

Published: May 2022 (version 1.0)

Superclass: CB

History of changes

Version	Description of change	Date

Note: please check SQA's website to ensure you are using the most up-to-date version of this document.