National Unit specification: general information

Unit title: Security Fundamentals (SCQF level 6)

Unit code: H2N5 12

Superclass: CB

Publication date: October 2012

Source: Scottish Qualifications Authority

Version: 01

Summary

This Unit introduces candidates to fundamental approaches to security in modern computing environments. The Unit looks at layers of security and how to secure operating systems. The Unit also looks at methods of applying security in computer networks and using software to secure systems.

This Unit is aimed at candidates who have at least a basic knowledge of computer hardware and computer software, and who are interested in security.

This is a mandatory Unit in the National Progression Award (NPA) in Professional Computer Fundamentals, but can also be taken as a freestanding Unit.

Outcomes

1 Demonstrate knowledge and understanding of security layers.
2 Demonstrate knowledge and understanding of operating system security.
3 Describe methods of applying security in computer networks using security software.

Recommended entry

While entry is at the discretion of the centre, it would be beneficial if candidates possessed basic ICT skills and had a working knowledge of computer hardware and software. This may be evidenced by achievement of the following, or equivalent Units:

F1KR 11 *Computing: Computer Hardware and Systems*
F3SY 12 *Computing: Computer Hardware and Systems*

It may also be beneficial for candidates to have some knowledge of computer networks. This may be evidenced by achievement of the following, or an equivalent Unit:

F1KH 11 *Computing: Computer Networking Fundamentals*

General information (cont)

Unit title: Security Fundamentals (SCQF level 6)

Credit points and level

1 National Unit credit at SCQF level 6: (6 SCQF credit points at SCQF level 6*)

**SCQF credit points are used to allocate credit to qualifications in the Scottish Credit and Qualifications Framework (SCQF). Each qualification in the Framework is allocated a number of SCQF credit points at an SCQF level. There are 12 SCQF levels, ranging from Access 1 to Doctorates.*

Core Skills

There is no automatic certification of Core Skills components in this Unit.

Opportunities for developing aspects of Core Skills are highlighted in the support notes of this Unit specification.

National Unit specification: statement of standards

Unit title: Security Fundamentals (SCQF level 6)

Acceptable performance in this Unit will be the satisfactory achievement of the standards set out in this part of the Unit specification. All sections of the statement of standards are mandatory and cannot be altered without reference to SQA.

Outcome 1

Demonstrate knowledge and understanding of security layers.

Performance Criteria

(a) Describe core security principles.
(b) Identify and explain different types of physical security.
(c) Explain the functions of internet security settings.
(d) Describe methods of wireless security.

Outcome 2

Demonstrate knowledge and understanding of operating system security.

Performance Criteria

(a) Identify and explain the methods of user authentication.
(b) Describe the process of accessing files and folders using permissions.
(c) Describe the purpose of password policies.
(d) Identify and explain methods of encryption.
(e) Identify and describe various types of malware.

Outcome 3

Describe methods of applying security in computer networks using security software.

Performance Criteria

(a) Identify a range of network security methods and techniques.
(b) Explain how client computers are secured and maintained using the identified methods and techniques.
(c) Explain how e-mail security and protection is achieved using the identified methods and techniques.
(d) Explain how servers are secured and maintained using the identified methods and techniques.

National Unit specification: statement of standards (cont)

Unit title: Security Fundamentals (SCQF level 6)

Evidence Requirements for this Unit

Evidence is required to demonstrate that candidates have achieved all Outcomes and Performance Criteria.

The evidence for all Outcomes should be obtained under controlled, supervised, closed-book conditions.

Evidence for Outcome 1 must include the following:

- Accurate description of the core security principles:
  - social engineering
  - confidentiality
  - availability
  - attack surface
- identification and explanation of at least four types of physical security from the following — site security; computer security; removable drives; access control; mobile device security
- explanation of configuring secure websites and internet security levels and zones using common browser options and settings

- Description of wireless security types and configurations:
  - encryption keys
  - SSID
  - MAC filters

Evidence for Outcome 2 must include the following:

- Identification and explanation of the following methods of user authentication:
  - smart cards
  - PKI
  - Biometrics
  - remote authentication servers

- Description of configuring security using permissions for:
  - file, folder and shared folder permissions; file system permissions; permission inheritance; delegation of control; determining effective permissions

- Description of the purpose of password policies to include complexity and length requirements, lockout policies and:
  - creating audit policies
  - considering what, where and how to audit

- Identification and explanation of the following methods of encryption:
  - PKI
  - certificate services
  - software based encryption
  - Virtual Private Networks (VPN)

- Identification and description of at least three types of malware.

National Unit specification: statement of standards (cont)

Unit title: Security Fundamentals (SCQF level 6)

Evidence for Outcome 3 must include the following:

- Identification of a range of network security methods and techniques for securing client computers to include antivirus software, operating updates, encrypting offline folders and software restriction policies.

- Explanation of how client computers are secured and maintained using the identified methods and techniques, related to:
  - types and characteristics of hardware firewalls
  - comparisons with software firewalls
  - the role of firewalls
  - network isolation techniques
  - secure network protocols
- identification of methods of network isolation such as — VLANs; routing; perimeter networks; NAT; VPN
- identification of methods of securing protocols such as spoofing, tunnelling; network sniffing
- explanation of how e-mail security and protection is achieved using the identified methods and techniques to address spam, spoofing and phishing

- Explanation of how servers are secured and maintained using the identified methods and techniques through:
  - operating system updates
  - security analysis tools
  - DNS updates
  - management VLANs

National Unit specification: support notes

Unit title: Security Fundamentals (SCQF level 6)

This part of the Unit specification is offered as guidance. The support notes are not mandatory.

While the exact time allocated to this Unit is at the discretion of the centre, the notional design length is 40 hours.

Guidance on the content and context for this Unit

This is a mandatory Unit in the National Progression Award in Professional Computer Fundamentals, but can also be taken as a freestanding Unit. The Unit may be useful for any candidates who are preparing to undertake the Microsoft Technology Associate (MTA) exam, Security Fundamentals (exam number: 98-367).

It is expected that the following content would be relevant to the delivery of Outcome 1:

- core security principles such as social engineering, confidentiality, availability and attack surface
- common physical security approaches such as site security; computer security; removable drives; access control; mobile device security
- configuring secure websites and internet security levels and zones using common browser options and settings
- common wireless security types and configurations such as encryption keys, SSID and MAC filters

It is expected that the following content would be relevant to the delivery of Outcome 2:

- user authentication methods such as smart cards, PKI, biometrics, and remote authentication servers
- configuring security using permissions — file, folder and shared folder permissions; file system permissions; permission inheritance; delegation of control; determining effective permissions
- creating password policies which include complexity and length requirements as well as lockout policies
- creating audit policies — considering what, where and how to audit
- methods and types of encryption — PKI, certificate services, software based encryption and Virtual Private Networks (VPNs)
- types of malware such as Trojans, spyware and worms

It is expected that the following content would be relevant to the delivery of Outcome 3:

- types and characteristics of hardware firewalls
- comparisons with software firewalls
- methods of network isolation such as — VLANs; routing; perimeter networks; NAT; VPN
- methods of securing protocols such as spoofing, tunnelling; network sniffing
- methods of securing client computers such as antivirus software, operating updates, encrypting offline folders and software restriction policies
- e-mail security issues such as spam, spoofing and phishing

- server protection methods such as operating system updates, security analysis tools, DNS updates and management VLANs

National Unit specification: support notes (cont)

Unit title: Security Fundamentals (SCQF level 6)

Guidance on learning and teaching approaches for this Unit

Whilst this Unit is largely theoretical in its content, hands-on practical exercises should be used where possible, to engage candidates and exemplify key concepts. It is suggested that practical exercises and/or demonstrations would be particularly relevant and beneficial when teaching the following:

Outcome 1

- configuration of internet options
- wireless security configurations

Outcome 2

- applying permissions to files and folders
- defining local security policies
- encrypting files and folders

Outcome 3

- configuring a basic firewall
- basic routing
- configuring antivirus software
- securing e-mail
- updating operating systems

The use of simulation and/or virtual machines could be used for teaching and assessment of parts of this Unit.

Guidance on approaches to assessment for this Unit

All Outcomes could be assessed by using a single 30 question multiple choice test, with 10 questions generated for each Outcome, covering the topics given in the Evidence Requirements.

Evidence for all Outcomes will be obtained under closed-book conditions. Where re-assessment is required, a different Instrument of Assessment should be used.

Opportunities for the use of e-assessment

E-assessment may be appropriate for some assessments in this Unit. By e-assessment we mean assessment which is supported by Information and Communication Technology (ICT), such as e-testing or the use of e-portfolios or social software. Centres which wish to use e-assessment must ensure that the national standard is applied to all candidate evidence and that conditions of assessment as specified in the Evidence Requirements are met, regardless of the mode of gathering evidence. Further advice is available in *SQA Guidelines on Online Assessment for Further Education (AA1641, March 2003), SQA Guidelines on e-assessment for Schools (BD2625, June 2005)*.

National Unit specification: support notes (cont)

Unit title: Security Fundamentals (SCQF level 6)

Opportunities for developing Core Skills

In this Unit candidates will develop skills in installing, testing and troubleshooting a network.

Candidates will:

- describe core security principles and types of physical security
- configure internet security settings and wireless security settings
- describe methods of user authentication
- apply permissions to allow access to files and folders
- configure and implement password policies
- describe methods of encryption
- configure basic firewalls
- describe network isolation techniques
- describe how to secure network protocols
- secure and maintain client computers
- configure e-mail security
- secure and maintain servers

This means that as they are doing this Unit, candidates may develop aspects of the Core Skills of *Information and Communication Technology*, *Communication* and *Problem Solving*.

Disabled candidates and/or those with additional support needs

The additional support needs of individual candidates should be taken into account when planning learning experiences, selecting assessment instruments, or considering whether any reasonable adjustments may be required. Further advice can be found on our website **www.sqa.org.uk/assessmentarrangements**

History of changes to Unit

Version	Description of change	Date