SQA Advanced Unit Specification

General information

Unit title: Network Security Concepts (SCQF level 7)

Unit code: HX00 47

Superclass:	CA
Publication date:	November 2017
Source:	Scottish Qualifications Authority
Version:	01

Unit purpose

The purpose of this unit is to introduce learners to the issues involved in designing and building secure computer systems and networks. It is a specialist unit, intended for learners undertaking a SQA Advanced qualification in Computing or a related area that requires an understanding of the concepts and practices underpinning computer and network security. The unit allows progression to more advanced study in the computing/computer networking field.

The unit covers the principal features of computer, network and operational security; common threats and vulnerabilities and the corresponding defences; implementation of basic application, data and host security techniques and implementation of basic cryptographic techniques. While the unit refers to computer science, it does not address the computer science aspects of the field in any depth.

The unit explores the types of threats that can endanger computer systems and networks, including malware and viruses, network, social engineering and application attacks, mitigation and deterrent techniques, penetration testing, vulnerability scanning and security threat avoidance. It also examines application and data security, authentication, authorisation and access control, security controls and account management and procedures for establishing host security, as well as cryptographic techniques, including public key infrastructure and certificate management.

The unit relates this to learners' vocational interests by examining how security impacts on systems they are familiar with, such as college systems and retail and banking systems. For example, they could consider the conflicts involved maintaining the security of personal information while meeting freedom of information requests.

Learners should also consider the social and ethical implications of network security including increasing government surveillance of communication and the role of activist groups in releasing classified information.

On completion of this unit, learners will understand the principal features of network security, the threats that exist and the ways of combatting them and they will be able to implement security and cryptographic techniques.

Outcomes

On successful completion of the unit the learner will be able to:

1 Describe the principal features of network security.
2 Describe common threats and vulnerabilities and the corresponding defences.
3 Implement basic application, data and host security techniques.
4 Implement basic encryption techniques.

Credit points and level

2 SQA credits at SCQF level 7: (16 SCQF credit points at SCQF level 7)

Recommended entry to the unit

Learners should possess basic IT skills before commencing this unit. This may be evidenced by possession of the Core Skill in *Information and Communication Technology (ICT)* at SCQF level 5 (or equivalent).

Core Skills

Opportunities to develop aspects of Core Skills are highlighted in the support notes for this unit specification.

There is no automatic certification of Core Skills or Core Skill components in this unit.

Context for delivery

If this unit is delivered as part of a group award, it is recommended that it should be taught and assessed within the subject area of the group award to which it contributes.

Equality and inclusion

This unit specification has been designed to ensure that there are no unnecessary barriers to learning or assessment. The individual needs of learners should be taken into account when planning learning experiences, selecting assessment methods or considering alternative evidence.

Further advice can be found on our website **www.sqa.org.uk/assessmentarrangements**.

SQA Advanced Unit Specification: Statement of standards

Unit title: Network Security Concepts (SCQF level 7)

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.

Where evidence for outcomes is assessed on a sample basis, the whole of the content listed in the knowledge and/or skills section must be taught and available for assessment. Learners should not know in advance the items on which they will be assessed and different items should be sampled on each assessment occasion.

Outcome 1

Describe the principal features of network security.

Knowledge and/or skills

- Functions of security
- Operational security
- Secure network administration
- Network ports, protocols and wireless technologies
- Network devices and associated technologies
- Risk concepts and mitigation strategies
- Incident response, disaster recovery and business continuity procedures
- Social and ethical implications of network security

Outcome 2

Describe common threats and vulnerabilities and the corresponding defences.

Knowledge and/or skills

- Malware and viruses
- Network, social engineering and application attacks
- Mitigation and deterrent techniques
- Penetration testing and vulnerability scanning
- Security threat avoidance techniques and approaches

Outcome 3

Implement basic application, data and host security techniques.

Knowledge and/or skills

- Application and data security
- Authentication, authorisation and access control
- Security controls and account management
- Procedures for establishing host security

Outcome 4

Implement basic encryption techniques.

Knowledge and/or skills

- ♦ General cryptography concepts
- ♦ Cryptographic tools
- ♦ Public key infrastructure and certificate management
- ♦ Drive, file/folder, messaging and wireless encryption

Evidence requirements for this unit

Learners will need to provide evidence to demonstrate their knowledge and/or skills across all outcomes. The evidence requirements for this unit will take two forms:

1 knowledge evidence (for Outcomes 1, 2, 3 and 4)
2 product evidence (for Outcomes 3 and 4)

Note that Outcomes 1 and 2 cover only cognitive competences while Outcomes 3 and 4 cover both cognitive and practical competencies. Each of the knowledge and/or skills items listed in Outcomes 3 and 4 is practical in nature but has an underlying cognitive competence that must be evidenced.

The knowledge evidence will be the explicit and implicit knowledge required for Outcomes 1, 2, 3 and 4. The product evidence will be artefacts showing the use of security as required for Outcomes 3 and 4.

Evidence is normally required for all of the knowledge and skills in every outcome. This means that every knowledge and skills statement should be evidenced. However, sampling may be used in a specific circumstance (see below).

The amount of evidence should be the minimum consistent with the defined knowledge and skills.

Evidence may be wholly or partly produced under controlled conditions. When evidence is produced in uncontrolled or loosely controlled conditions it must be authenticated. The *Guide to Assessment* provides further advice on methods of authentication.

There are no time limitations on the production of evidence (but see exception below). The evidence may be produced at any time during the life of the unit. Learners may use reference materials when undertaking assessment (but see exception below).

Sampling is permissible when the written/oral evidence for Outcomes 1, 2, 3 and 4 is produced by a test of knowledge and understanding. The test may take any form (including oral) but must be supervised, unseen and timed. The contents of the test must sample broadly and proportionately from the contents of Outcomes 1, 2, 3 and 4 with approximately equal weighting for each outcome. Access to reference material is not appropriate for this type of assessment.

Practical tasks should be documented in an appropriate manner, eg a report (paper or electronic), a logbook or a blog. Possible practical tasks (at least one per outcome) could include the following:

Outcome 3

Implement at least one secure home or small business network incorporating both wired and wireless elements.

Manipulate operating system and application security settings, use access control lists (authentication, authorisation and access control) and security policies.

Outcome 4

Configure email/messaging, wireless, file/folder and/or drive encryption.

SQA Advanced Unit support notes

Unit title: Network Security Concepts (SCQF level 7)

Unit support notes are offered as guidance and are not mandatory.

While the exact time allocated to this unit is at the discretion of the centre, the notional design length is 80 hours.

Guidance on the content and context for this unit

This unit is intended for anyone with an interest in computer and network security, who wishes to gain a deeper understanding of these topics. It is particularly appropriate for learners undertaking a SQA Advanced qualification in Computing, Computer Networking or a related area.

The aim of the unit is to provide learners with a broad knowledge of the concepts of computer and network security, along with a conceptual understanding of many elements of modern computer security practices.

The unit incorporates practical elements. To allow learners to perform these practical tasks, centres will require suitable resources.

Although the unit is expressed in generic terms, it should be related to a context that will be familiar to learners, eg how secure wireless networks and topologies, along with the implementation of addressing schemes and associated tools.

The practical elements may be done as individual tasks or carried out as part of a larger case study/project requirement.

Please note that this section is not a teaching syllabus and does not seek to explain each knowledge/skills statement. This section seeks to clarify the statement of standards (within this unit specification) where it is potentially ambiguous. It also focuses on non-apparent teaching and learning issues that may be over-looked, or not emphasised, during unit delivery. As such, it is not representative of the actual time spent teaching or learning specific competences or the relative importance of each competence.

Although this unit contains a significant body of knowledge, it is recommended that it is delivered in a practical context through exemplification of the principles and practice of computer and network security.

During the delivery of this unit it is important that every opportunity is taken to introduce real-world examples, opportunities for whole-class and group discussion and practical demonstrations wherever possible. Concepts and terminology should be presented in context throughout the unit. Video presentations should be used where appropriate for providing an alternative explanation of a difficult topic, or as a focus for class discussion or group work. Wherever possible theoretical learning should be re-enforced using practical labs/demonstrations, for example to demonstrate the use of particular tools, the lecturer could capture relevant packets using a suitable packet sniffer tool.

Although not formally taught in this unit, learners should be aware of the health and safety risks to themselves and others that can arise when working with electrical equipment. Safe working practices should be explained and demonstrated.

Given the theoretical nature of this unit, it is intended that a significant amount of time will be made available as a central part of the course for revision, tutorials and formative assessment exercises. Learners should be strongly encouraged to undertake further reading, opportunities for individual or group research should be provided.

Guidance on approaches to delivery of this unit

Although this unit contains a significant body of knowledge, it is recommended that it is delivered in a practical context through exemplification installation and management of database servers.

It is recommended that the unit is delivered in the sequence of the outcomes, since each outcome requires the underpinning knowledge and skills of earlier outcomes. A suggested distribution of time, across the outcomes, is:

Outcome 1:	8 hours
Outcome 2:	8 hours
Outcome 3:	12 hours
Outcome 4:	12 hours

Summative assessment should be carried out towards the end of the unit, although learners could begin to generate the evidence at an earlier stage. However, if a report is used, it should not be assessed until it is complete and the learner is satisfied with it.

There are opportunities to carry out formative assessment at various stages in the life of the unit. For example, formative assessment could be carried out upon the completion of each outcome to ensure that learners have grasped the knowledge and skills contained within each outcome. This would provide assessors with an opportunity to diagnose misconceptions and intervene to remedy them before progressing to the next outcome.

Guidance on approaches to assessment of this unit

Evidence can be generated using different types of assessment. The following are suggestions only. There may be other methods that would be more suitable to learners.

Centres are reminded that prior verification of centre-devised assessments would help to ensure that the national standard is being met. Where learners experience a range of assessment methods, this helps them to develop different skills that should be transferable to work or further and higher education.

Summative assessment should take place towards the end of unit when learners will be required to document the practical tasks completed. It is recommended that these are linked to their vocational interests.

Assessments could consist of a single multiple-choice test alongside one or more practical assignments.

The practical elements could be done as individual tasks or carried out as part of a larger case study/project requirement. The latter may lead to an enriched learner experience. These tasks will be open-book with time allocated, being at the discretion of the centre.

Practical tasks may be carried out under loosely controlled conditions. For example, parts of them may not be done under the supervision of the assessor. In this scenario, authentication would be required, which could take the form of oral questioning.

The single multiple-choice assessment should be conducted in unseen closed-book, supervised and timed conditions. The assessment may be carried out using e-assessment or paper based. To pass learners should answer 60% of the questions correctly.

If a learner requires to be reassessed, a different selection of questions must be used. At least half the questions in the reassessment must be different from those used in the original test.

The suggested time allocation for a multiple-choice assessment is two minutes for each question plus five minutes starting-up time and five minutes finishing-off time, thus a total of 90 minutes should be allocated for a 40-question end-of-unit test.

In the event that e-assessment is deployed, centres may also utilise other types of questioning, eg drag and drop or mix and match. The level of this unit would prohibit the use of true/false type questions.

Multiple-choice questions could come from the following areas — these are not prescriptive.

Outcome 1: Describe the principal features of network security.

Functions of security:

- Protection against illicit access / modification, intrusion, identity theft, viruses, malware

Operational security:

- Physical access, environmental threats

Secure network administration:

- Firewall rules, VLANs, router configurations, access control lists, port security, network segmentation, log analysis

Network devices and associated technologies:

- Firewalls, routers, switches, proxies, gate ways, 802.11, VPN technology, protocol analysers/sniffers, filtering and packet inspection, DMZ, subnetting, VLANs, NAT, telephony, virtualization/cloud computing

Network ports, protocols and wireless technologies:

- IPSec, SSL, SSH, HTTPS, SFTP, SCP, SNMP, WPA, WPA2, WEP, MAC filtering, SSID broadcasts, TKIP, channelling

Risk concepts and mitigation strategies:

- Controlling, reduction: privacy/acceptable use/security/mandatory policies, risk calculation, change/incident management, user permission reviews, auditing

Incident response, disaster recovery and business continuity procedures:

- Basic forensic procedures, damage/loss control, chain of custody, incident response, impact analysis, continuity planning, disaster recovery, environmental controls (fire suppression, shielding, temperature control, CCTV monitoring)

Social and ethical implications, eg right to privacy, freedom of information legislation, government surveillance.

Outcome 2: Identify and describe threats and vulnerabilities.

Malware and viruses:

- Adware, viruses, worms, spyware, trojans, ransomware, rootkits, backdoors, botnets

Network, social engineering and application attacks:

- Man-in-the-middle, DDoS, smurf, spoofing, spamming, phishing, DNS poisoning, shoulder surfing, tailgating, hoaxes, impersonation, packet sniffing, war chalking, war driving, cross site scripting, SQL injections, LDAP injections, buffer overflows, cookies, session hijacks

Mitigation and deterrent techniques:

- Electronic bypassing, system/security/access logs, physical security, hardening, intrusion detection, risk/threat/vulnerability assessing, baseline reporting

Penetration testing and vulnerability scanning:

- Threat verification, exploiting vulnerabilities, passive testing, white/black/grey box testing

Security threat avoidance:

- Protocol analysers, sniffers, port scanners, honeypots

Outcome 3: Identify and implement basic application, data, host security and access control mechanisms.

Application and data security:

- Hardening, patch management, secure coding, data loss prevention, encryption

Authentication, authorisation and access control:

- Identification/authentication, RADIUS, TACACS, LDAP, Kerberos, Biometrics, Tokens, Smartcards, SSO, ACLs, mandatory/discretionary access control

Security controls and account management:

- Password complexity, recovery, length, lockout, privileges

Procedures for establishing host security:

- Operating system security settings, anti-malware/virus, patch management, baselining, mobile devices, physical hardware security

Outcome 4: Identify and implement suitable methods of encryption.

General cryptography concepts:

- Symmetric/asymmetric, transport encryption, hashing, steganography, digital signatures

Cryptographic tools and concepts:

- Wireless technology, MD5, SHA, AES, DES, 3DES, RSA, PAP/CHAP, blowfish, transport encryption

Public key infrastructure:

- PKI, Public key, private keys, recovery agents, certificate management, certificate authorities

Encryption of files, folders and e-mail/messaging:

- OS encryption, third-party tools, PGP

Opportunities for 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 learner evidence and that conditions of assessment as specified in the evidence requirements are met, regardless of the mode of gathering evidence. The most up-to-date guidance on the use of e-assessment to support SQA's qualifications is available at **www.sqa.org.uk/e-assessment**.

Opportunities for developing Core and other essential skills

There are opportunities to develop the Core Skills of *Information and Communication Technology.*

History of changes to unit

Version	Description of change	Date

SQA acknowledges the valuable contribution that Scotland's colleges have made to the development of SQA Advanced Qualifications.

FURTHER INFORMATION: Call SQA's Customer Contact Centre on 44 (0) 141 500 5030 or 0345 279 1000. Alternatively, complete our Centre Feedback Form.

General information for learners

Unit title: Network Security Concepts (SCQF level 7)

This section will help you decide whether this is the unit for you by explaining what the unit is about, what you should know or be able to do before you start, what you will need to do during the unit and opportunities for further learning and employment.

This SCQF level 7 unit is aimed at providing you with fundamental skills in the concepts of network security and associated techniques and is aimed at learners undertaking a SQA Advanced Certificate or SQA Advanced Diploma in Computing with Networking or Technical Support that require an understanding of the concepts underpinning network security.

On completion of this unit you should be able to:

- Describe the principal features of network security.
- Describe common threats and vulnerabilities and the corresponding defences.
- Implement basic application, data and host security techniques.
- Implement basic encryption techniques.

Outcome 1 focuses on the fundamentals of network security and design, devices, ports, protocols, risk management concepts disaster recovery and environmental controls.

Outcome 2 focuses on threats and vulnerabilities such as malware, spyware, social engineering techniques and penetration testing that can be used for security threat avoidance and ethical hacking techniques.

Outcome 3 focuses on application, data, host and access control mechanisms along with authentication services, operating system security controls account and password management.

Outcome 4 focuses on encryption techniques, such as cryptographic tools, public key/private key infrastructure, digital signatures, certificate management, and data encryption tools and techniques for files, folders and e-mail/messaging.

There may be one closed-book restricted-response assessment covering the knowledge and understanding in all outcomes. You will be presented with a total of 40 questions and expected to answer 60% of these correctly. You may also be expected to keep a log book, or equivalent, recording the practical tasks you have carried out during the unit. You must satisfy the requirements for these assessments to achieve the unit.