Higher National Unit Specification

General information for centres

Unit title: Security Concepts

Unit code: DG02 34

Unit purpose: This Unit is designed to introduce candidates to the issues involved in designing and constructing secure computer networks. It is intended for candidates undertaking an HNC or HND in Computing, Computer Networking or a related area who require an understanding of network security.

On completion of the Unit candidates should be able to:

1. Describe the general concepts of network security.
2. Describe the features of communication security.
3. Describe the features of infrastructure security.
4. Describe the basics of cryptography.
5. Describe operational and organisational security.

Credit value: 2 HN credits at SCQF level 7: (16 SCQF credit points at SCQF level 7)

**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.*

Recommended prior knowledge and skills: Access to this Unit will be at the discretion of the Centre. There are no specific requirements but candidates would benefit from knowledge of computer networks. This may be demonstrated by the possession of HN Units such as DG0K 33 Hardware Concepts, DF9L 33 Operating System Concepts and DF9P 34 Network Concepts.

Core skills: There may be opportunities to gather evidence towards core skills in this Unit, although there is no automatic certification of core skills or core skills components.

Context for delivery: This Unit is included in the framework of a number of HNC and HND group awards. It is recommended that it should be taught and assessed within the context of the particular group award to which it contributes.

General information for centres (cont)

Assessment: Evidence for the knowledge and/or skills for the entire Unit must be produced using a set of 50 restricted-response questions to assess candidates' knowledge and understanding. This may be administered as a single end-of unit test, or as several subtests, each covering one or more outcomes.

Candidates must answer at least 70% of the questions correctly in order to obtain a pass. If subtests are used, they must also score at least 70% in each subtest.

Testing must take place in a closed-book environment where candidates have no access to books, handouts, notes or other learning material. Testing can be done in either a machine-based or paper-based format and must be invigilated by a tutor or mentor. There must be no communication between candidates and communication with the invigilator must be restricted to matters relating to the administration of the test.

If a candidate 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.

If an outcome has a practical component, this must be assessed by having the candidate use a logbook to record the practical tasks successfully completed. The logbook can be in paper or electronic form and must be authenticated by the tutor or mentor.

For some outcomes only a sample of the practical tasks needs to be completed and recorded for assessment purposes, e.g. three out of five. This is clearly indicated in the logbook instructions for the outcomes involved. Where this occurs, tutors must inform candidates of the tasks to be completed.

Higher National Unit specification: statement of standards

Unit title: Security Concepts

Unit code: DG02 34

The sections of the Unit stating the Outcomes, knowledge and/or skills, and evidence requirements are mandatory.

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. Candidates 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 general concepts of network security.

Knowledge and/or skills

- Recognise access control models.
- Authentication methods.
- Disable non-essential services and protocols.
- Combat attacks.
- Recognise malicious code.
- Describe auditing techniques.

Evidence requirements

Restricted response test

The knowledge and skills component of Outcome 1 must be examined by fifteen questions, two being derived from each of three of the six items listed below and three derived from each of the remaining three items. Each question must be derived from a single item.

1. Recognise access control models.

   MAC / DAC / RBAC

2. Authentication methods.

   Kerberos, CHAP, certificates, username/password, tokens, multi-factor, mutual authentication, biometrics

3. Disable non-essential services and protocols.

   disabling unnecessary systems / processes / programs.

4. Combat attacks.

   DOS/DDOS, back door, spoofing, man in the middle, replay, TCP/IP hijacking, weak keys, mathematical, social engineering, birthday, password guessing (brute force and dictionary) software exploitation

5. Recognise malicious code.

   Viruses, trojan horses, logic bombs and worms.

6. Describe auditing techniques.

   Logging, system scanning

The test may be administered on its own as a subtest or be combined with other outcome subtests in the Unit.

Alternatively, the 15 questions for this outcome may contribute towards a single end-of-unit test of 50 questions.

Logbook

The logbook for Outcome 1 must record successful completion by the candidate of the task listed below.

- Authentication methods.

  Documentary evidence that the candidate can use system tools to configure the authentication method for a remote-access connection.

Assessment guidelines

It is suggested that all the above concepts be presented and explained within the context of current real-world practice and applications.

Higher National Unit specification: statement of standards (cont)

Unit title: Security Concepts

The suggested time allocation for a restricted response test is 2 minutes for each question plus 5 minutes starting-up time and 5 minutes finishing-off time, thus a total of 110 minutes should be allocated for a 50-question end-of-unit test.

Although individual outcome tests are permissible, it is suggested that if subtests are to be used, outcomes should be combined to produce tests of no fewer than 10 questions. A 10-question test would therefore have a time allocation of 30 minutes.

Outcome 2

Describe the features of communication security

Knowledge and/or skills

- Describe remote access security.
- Describe email security.
- Describe web security.
- Describe directory security.
- Describe file transfer.
- Describe wireless security.

Evidence requirements

Restricted response test

The knowledge and skills component of Outcome 2 must be examined by ten questions, two being derived from each of four of the six items listed below and one derived from each of the remaining two items. Each question must be derived from a single item.

1. Describe remote access security.

   802.1x, VPN, RADIUS, TACACS/+, L2TP/PPTP, SSH, IPSEC, vulnerabilities

2. Describe email security.

   S/MIME, PGP-like technologies, vulnerabilities

3. Describe web security.

   SSL/TLS, HTTP/S, instant messaging, vulnerabilities

Higher National Unit specification: statement of standards (cont)

Unit title: Security Concepts

4. Describe directory security.

   SSL/TLS, LDAP (recognition rather than administration).

5. Describe file transfer.

   S/FTP, Blind FTP/Anonymous, file sharing, vulnerabilities

6. Describe wireless security.

   WTLS, 802.11x, WEP/WAP, vulnerabilities, site surveys

The test may be administered on its own as a subtest or be combined with other outcome subtests in the Unit.

Alternatively, the 10 questions for this outcome may contribute towards a single end-of-unit test of 50 questions.

Logbook

The logbook for Outcome 2 must record successful completion by the candidate of the task listed below.

- Describe email security.

  Documentary evidence that the candidate can download and install PGP freeware and create PGP keys.

Assessment guidelines

It is suggested that all the above concepts be presented and explained within the context of current real-world practice and applications.

The suggested time allocation for a restricted response test is 2 minutes for each question plus 5 minutes starting-up time and 5 minutes finishing-off time, thus a total of 110 minutes should be allocated for a 50-question end-of-unit test.

Higher National Unit specification: statement of standards (cont)

Unit title: Security Concepts

Although individual outcome tests are permissible, it is suggested that if subtests are to be used, outcomes should be combined to produce tests of no fewer than 10 questions. A 10-question test would therefore have a time allocation of 30 minutes.

Outcome 3

Describe the features of infrastructure security.

Knowledge and/or skills

- Describe network devices.
- Describe media.
- Describe security topologies.
- Describe intrusion detection.
- Describe security baselines.

Evidence requirements

Restricted response test

The knowledge and skills component of Outcome 3 must be examined by ten questions, two being derived from each of the five items listed below. Each question must be derived from a single item.

1. Describe network devices

   Firewalls, Routers, Switches, Wireless, Modems, RAS, Telecom/PBX, VPN, IDS, Network Monitoring/Diagnostics, Workstations, Servers, Mobile Devices

2. Describe media

   Coax, UTP/STP, fibre, removable media (tape, CDR, hard drives, diskettes, flashcards, smartcards)

3. Describe security topologies

   Security Zones (DMZ, Intranet, Extranet, VLANs), NAT, Tunnelling

4. Describe intrusion detection

Network Based (Active Detection, Passive Detection), Host Based (Active Detection, Passive Detection), Honey pots, Incident Response

5. Describe security baselines

   OS/NOS Hardening (Concepts and Processes, File System, Updates), Network Hardening (Updates, Configuration, Enabling and Disabling Services and Protocols, Access control lists); Application Hardening (Updates, Web Servers, Email Servers, FTP Servers, DNS Servers, NNTP Servers, File/Print Servers, DHCP Servers, Data Repositories, Directory Services, Databases)

The test may be administered on its own as a subtest or be combined with other outcome subtests in the Unit.

Alternatively, the 10 questions for this outcome may contribute towards a single end-of-unit test of 50 questions.

Logbook

There are no practical tasks associated with this outcome.

Assessment guidelines

It is suggested that all the above concepts be presented and explained within the context of current real-world practice and applications.

The suggested time allocation for a restricted response test is 2 minutes for each question plus 5 minutes starting-up time and 5 minutes finishing-off time, thus a total of 110 minutes should be allocated for a 50-question end-of-unit test.

Although individual outcome tests are permissible, it is suggested that if subtests are to be used, outcomes should be combined to produce tests of no fewer than 10 questions. A 10-question test would therefore have a time allocation of 30 minutes.

Higher National Unit specification: statement of standards (cont)

Unit title: Security Concepts

Outcome 4

Describe the basics of cryptography.

Knowledge and/or skills

- Describe cryptographic algorithms
- Describe uses of cryptography
- Describe Public Key Infrastructure (PKI)
- Describe standards and protocols
- Describe key management and certificate lifecycle

Evidence requirements

Restricted response test

The knowledge and skills component of Outcome 4 must be examined by six questions, two being derived from one of the five items listed below and one derived from each of the remaining four items. Each question must be derived from a single item.

1. Describe cryptographic algorithms

   Hashing, Symmetric, Asymmetric

2. Describe uses of cryptography

   Confidentiality**,** Integrity**,** Digital Signatures**,** Authentication**,** Non-Repudiation**,** Access Control

3. Describe Public Key Infrastructure (PKI)

   Certificates (what certificates are used for what purpose), Certificate Policies, Certificate Practice Statements, Revocation, Trust Models

4. Describe standards and protocols

5. Describe key management and certificate lifecycle

Centralized vs. decentralized, storage, escrow, expiration, revocation, status checking, suspension, recovery, M of N control, renewal, destruction, key usage, multiple keys

The test may be administered on its own as a subtest or be combined with other outcome subtests in the Unit.

Alternatively, the 6 questions for this outcome may contribute towards a single end-of-unit test of 50 questions.

Logbook

There are no practical tasks associated with this outcome.

Assessment guidelines

It is suggested that all the above concepts be presented and explained within the context of current real-world practice and applications.

The suggested time allocation for a restricted response test is 2 minutes for each question plus 5 minutes starting-up time and 5 minutes finishing-off time, thus a total of 110 minutes should be allocated for a 50-question end-of-unit test.

Although individual outcome tests are permissible, it is suggested that if subtests are to be used, outcomes should be combined to produce tests of no fewer than 10 questions. A 10-question test would therefore have a time allocation of 30 minutes.

Outcome 5

Describe operational and organisational security.

Knowledge and/or skills

- Describe physical security.
- Describe disaster recovery.
- Describe business continuity.
- Describe policies and procedures.
- Describe privilege management
- Describe forensics.
- Describe risk identification.

Higher National Unit specification: statement of standards (cont)

Unit title: Security Concepts

- Describe education and training.
- Describe documentation.

Evidence requirements

Restricted response test

The knowledge and skills component of Outcome 5 must be examined by nine questions, one being derived from each the nine items listed below. Each question must be derived from a single item.

1. Describe physical security

   Access control**,** physical barriers**,** biometrics**,** social engineering**,** environment**,** wireless cells**,** location**,** shielding**,** fire suppression

2. Describe disaster recovery

   Backups**,** off site storage**,** secure recovery**,** alternate sites**,** disaster recovery plan

3. Describe business continuity

   Utilities, high availability / fault tolerance, backups

4. Describe policies and procedures

   Security policy, acceptable use, due care, privacy, separation of duties, need to know, password management, service level agreements, disposal / destruction, HR policy, hiring and termination - adding / revoking passwords, privileges, etc., code of ethics, incident response policy

5. Describe privilege management

   User/group/role management, single sign-on, centralized vs. decentralized, auditing (privilege, usage, escalation), MAC/DAC/RBAC

6. Describe forensics

   Awareness, role of individual, chain of custody, preservation of evidence, collection of evidence

Higher National Unit specification: statement of standards (cont)

Unit title: Security Concepts

7. Describe risk identification

   Asset identification, risk assessment, threat identification, vulnerabilities

8. Describe education and training

   End users, executives, HR, communication, user awareness, education, online resources

9. Describe documentation

   Standards and guidelines, systems architecture, change documentation, logs and inventories, classification, notification, retention/storage, destruction

The test may be administered on its own as a subtest or be combined with other outcome subtests in the Unit.

Alternatively, the 9 questions for this outcome may contribute towards a single end-of-unit test of 50 questions.

Logbook

The logbook for Outcome 5 must record successful completion by the candidate of the task listed below.

- Describe risk identification

  Documentary evidence that the candidate can use the CERT and ICAT websites to compare vulnerability statistics for 1990, 2000 and the latest year available.

Assessment guidelines

It is suggested that all the above concepts be presented and explained within the context of current real-world practice and applications.

The suggested time allocation for a restricted response test is 2 minutes for each question plus 5 minutes starting-up time and 5 minutes finishing-off time, thus a total of 110 minutes should be allocated for a 50-question end-of-unit test.

Higher National Unit specification: statement of standards (cont)

Unit title: Security Concepts

Although individual outcome tests are permissible, it is suggested that if subtests are to be used, outcomes should be combined to produce tests of no fewer than 10 questions. A 10-question test would therefore have a time allocation of 30 minutes.

Administrative Information

Unit code: DG02 34

Unit title: Security Concepts

Superclass category: CB

Date of publication: May 2004

Version: 01

Source: SQA

Higher National Unit specification: support notes

Unit title: Security Concepts

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 80 hours.

The suggested time allocation for each outcome (including assessment) is as follows:

Outcome 1: 24 hours
Outcome 2: 16 hours
Outcome 3: 16 hours
Outcome 4: 12 hours
Outcome 5: 12 hours

Guidance on the content and context for this Unit

As it is likely that the bulk of the material in this Unit will be delivered through lecturer exposition, 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 groupwork.

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. Candidates should be strongly encouraged to undertake further reading, and opportunities for individual or group research should be provided.

The most important overall emphasis should be on the relevance and currency of content in such a rapidly-evolving field.

This Unit may assist candidates in preparing for CompTIA examination SY0-101: Security+. Vendor certifications can change rapidly and candidates should be encouraged the check the current details at **www.comptia.org** to ensure that all objectives have been covered. This examination can also contribute towards the Microsoft Certified Systems Administrator (MCSA) award.

Higher National Unit specification: support notes (cont)

Unit title: Security Concepts

Outcome 1

Outcome 1 is about the general concepts of Network Security.

1 Recognise access control models.

Candidates should be able to differentiate and explain the following access control models: MAC (Mandatory Access Control), DAC (Discretionary Access Control), RBAC (Role Based Access Control).

2 Authentication methods.

Candidates should be able to differentiate and explain the following authentication methods: Kerberos, CHAP (Challenge Handshake Authentication Protocol), certificates, username / password, tokens, multi-factor, mutual, biometrics.

3 Disable non-essential services and protocols.

Candidates should be able to identify non-essential services and protocols and know what actions to take to reduce the risks of those services and protocols.

4 Combat attacks.

Candidates should also be able to recognize the following attacks and specify the appropriate actions to take to mitigate vulnerability and risk: DOS / DDOS (Denial of Service / Distributed Denial of Service), back door, spoofing, man in the middle, replay, TCP/IP hijacking, weak keys, mathematical, social engineering, birthday, password guessing (brute force and dictionary) and software exploitation.

5 Recognise malicious code.

Candidates should be able to recognise the following types of malicious code and specify the appropriate actions to take to mitigate vulnerability and risk: viruses, trojan horses, logic bombs and worms.

6 Describe auditing techniques.

Candidates should understand the concept and significance of auditing, logging and system scanning.

Higher National Unit specification: support notes (cont)

Unit title: Security Concepts

Outcome 2

Outcome 2 covers Communication Security.

1 Describe remote access security.

Candidates should be able to recognize and understand the administration of the following types of remote access technologies: 802.1x, VPN (Virtual Private Network), RADIUS (Remote Authentication Dial-In User Service, TACACS (Terminal Access Controller Access Control System), L2TP / PPTP (Layer Two Tunnelling Protocol / Point to Point Tunnelling Protocol), SSH (Secure Shell), IPSEC (Internet Protocol Security).

2 Describe email security.

Candidates should also be able to recognise and understand the administration of the following email security concepts: S/MIME (Secure Multipurpose Internet Mail Extensions), PGP (Pretty Good Privacy) like technologies, vulnerabilities (SPAM, hoaxes). PGP freeware can be downloaded from **www.pgpi.com** or numerous other sources that can be located via a search engine.

3 Describe web security.

Candidates should be able to recognise and understand the administration of the following Internet security concepts: SSL / TLS (Secure Sockets Layer / Transport Layer Security), HTTP/S (Hypertext Transfer Protocol / Hypertext Transfer Protocol over Secure Sockets Layer), Instant Messaging (vulnerabilities, packet sniffing, privacy, vulnerabilities (JavaScript, ActiveX, buffer overflows, cookies, signed applets, CGI (Common Gateway Interface) scripts, SMTP (Simple Mail Transfer Protocol) relay.

4 Describe directory security.

Candidates should be able to recognise and understand the administration of the following directory security concepts: SSL/TLS (Secure Sockets Layer / Transport Layer Security), LDAP (Lightweight Directory Access Protocol).

5 Describe file transfer.

Candidates should be able to recognise and understand the administration of the following file transfer protocols and concepts: S/FTP (File Transfer Protocol), Blind FTP (File Transfer Protocol) / Anonymous, File Sharing, vulnerabilities (packet sniffing, 8.3 naming conventions).

Higher National Unit specification: support notes (cont)

Unit title: Security Concepts

6 Describe wireless security.

Candidates also should recognize and understand the administration of the following wireless technologies and concepts: WTLS (Wireless Transport Layer Security), 802.11 and 802.11x, WEP/WAP (Wired Equivalent Privacy / Wireless Application Protocol), vulnerabilities, site surveys.

Outcome 3

Outcome 3 is about Infrastructure Security.

1 Describe network devices.

Candidates should be able to understand security concerns and the concepts of the following types of devices: firewalls, routers, switches, wireless, modems, RAS (Remote Access Server), Telecom / PBX (Private Branch Exchange), VPN (Virtual Private Network), IDS (Intrusion Detection System), network monitoring / diagnostics, workstations, servers and mobile devices.

2 Describe media.

Candidates should also be able to understand the security concerns for the following types of media: coaxial cable, UTP / STP (Unshielded Twisted Pair / Shielded Twisted Pair), fibre optic cable, removable media (tape, CD-R (Recordable Compact Disks), hard drives, diskettes, flashcards, smartcards).

3 Describe security topologies.

Candidates should be able to understand the concepts behind the following kinds of security topologies: security zones (DMZ (Demilitarized Zone), Intranet, Extranet), VLANs (Virtual Local Area Network), NAT (Network Address Translation) and tunnelling.

4 Describe intrusion detection.

Candidates should be able to describe implementation and configuration of the following types of intrusion detection system: network based (active detection, passive detection), host based (active detection, passive detection), honey pots, incident response.

Higher National Unit specification: support notes (cont)

Unit title: Security Concepts

5 Describe security baselines.

Candidates should be able to explain what a security baseline is and describe the implementation and configuration of each kind of intrusion detection system: OS / NOS

(Operating System / Network Operating System) hardening (file system, updates (hot fixes, service packs, patches)), network hardening (updates (firmware), configuration (enabling and disabling services and protocols, access control lists)), application hardening (updates (hot fixes, service packs, patches), web servers, e-mail servers, FTP (File Transfer Protocol) servers, DNS (Domain Name Service) servers, NNTP (Network News Transfer Protocol) servers, file / print servers, DHCP (Dynamic Host Configuration Protocol) servers, data repositories (directory services, databases).

Outcome 4

Outcome 4 covers the basics of Cryptography.

1 Describe cryptographic algorithms

On completion, candidates should be able to identify and explain the of the following different kinds of cryptographic algorithms: hashing, symmetric, asymmetric.

2 Describe uses of cryptography

Candidates should understand how cryptography addresses the following security concepts: confidentiality, integrity (digital signatures), authentication, non-repudiation (digital signatures), access control

3 Describe Public Key Infrastructure (PKI)

Candidates should understand and be able to explain the following concepts of PKI (Public Key Infrastructure): certificates (policies, practice statements), revocation, trust models.

4 Describe standards and protocols

Candidates should be able to identify and differentiate different cryptographic standards and protocols.

5 Describe key management and certificate lifecycle

Candidates should also be able to explain: key management and certificate lifecycles, centralized vs. decentralized, storage (hardware vs. software, private key protection), escrow, expiration, revocation (status checking), suspension (status checking), recovery (m-of-n control (of m appropriate individuals, n must be present to authorize recovery), renewal, destruction, key usage (multiple key pairs (single, dual)).

Outcome 5

Outcome 5 covers operational and organisational security.

1 Describe physical security.

On completion, candidates should understand the application of physical security including access control (physical barriers, biometrics), social engineering and environment (wireless cells, location, shielding and fire suppression).

2 Describe disaster recovery.

Candidates should understand the security implications of disaster recovery, including backups (off site storage), secure recovery (alternate sites), disaster recovery plan.

3 Describe business continuity.

Candidates should be aware of the security implications of business continuity, including utilities, high availability, fault tolerance and backups.

4 Describe policies and procedures.

Candidates should also understand the concepts and uses of the following types of policies and procedures: security policy, acceptable use, due care, privacy, separation of duties, need to know, password management, SLAs (Service Level Agreements), disposal / destruction, human resources policy (hiring and termination (adding and revoking passwords and privileges, etc.), code of ethics and incident response policy.

Higher National Unit specification: support notes (cont)

Unit title: Security Concepts

5 Describe privilege management

Candidates should be able to explain the concepts of privilege management: user / group / role management, single sign-on, centralized vs. decentralized, auditing (privilege, usage, escalation), MAC / DAC / RBAC (Mandatory Access Control / Discretionary Access Control / Role Based Access Control)

6 Describe forensics.

Candidates should also understand the concepts of the following topics of forensics: chain of custody, preservation of evidence and collection of evidence.

7 Describe risk identification.

Candidates should be able to explain the following concepts of risk identification: asset identification, risk assessment, threat identification, vulnerabilities. Statistical information can be obtained from **www.cert.org/stats** or **icat.nist.gov**

8 Describe education and training.

Candidates should understand the security relevance of the education and training of end users, executives and human resources: communication, user awareness, education, on-line resources.

9 Describe documentation.

Candidates should be able to explain the following documentation concepts: standards and guidelines, systems architecture, change documentation, logs and inventories, classification, notification, retention / storage, destruction

Guidance on the delivery and assessment of this Unit

This Unit is likely to form part of a group award which is primarily designed to provide candidates with technical or professional knowledge and skills related to a specific occupational area. It is highly technical in content and should not be adopted by group awards in other areas or delivered as a stand-alone Unit without careful consideration of its appropriateness. It is not a Unit which candidates are likely to find accessible at an introductory level; it is suggested that it be delivered only as part of a second-year HND program in Computing or a related area, after candidates have experience of basic background topics involved in the hardware and software aspects of computer networks. It should be delivered in tandem with other networking Units rather than prior to them, and opportunities for teaching and assessment integration explored.

Higher National Unit specification: support notes (cont)

Unit title: Security Concepts

To minimise assessment overhead, sets of restricted-response questions are used to provide evidence of candidates' knowledge for all Outcomes. It is suggested that multiple-choice questions can be used as the preferred assessment method – as well as reducing the time required for assessment and marking, these reduce the need for candidates to memorise details and encourage understanding. The numbers of questions which must be answered correctly in each assessment correspond to 70% of those set in each case.

Open learning

If this Unit is delivered by open or distance learning methods, additional planning and resources may be required for candidate support, assessment and quality assurance.

A combination of new and traditional authentication tools may have to be devised for assessment and re-assessment purposes.

For further information and advice, please see *Assessment and Quality Assurance for Open and Distance Learning* (SQA, February 2001 — publication code A1030).

Special needs

This Unit specification is intended to ensure that there are no artificial barriers to learning or assessment. Special needs of individual candidates should be taken into account when planning learning experiences, selecting assessment instruments or considering special alternative Outcomes for Units. For information on these, please refer to the SQA document *Guidance on Special Assessment Arrangements* (SQA, 2001).

General information for candidates

Unit title: Security Concepts

This is a 2-credit Unit at Level 7 intended for candidates undertaking a Computing or IT-related qualification who require an understanding of Network Security. It is designed to develop a detailed knowledge of the issues involved in designing and constructing secure computer networks. On completion of the Unit you should be able to:

- Describe the general concepts of network security.
- Describe the features of communication security.
- Describe the features of infrastructure security.
- Describe the basics of cryptography.
- Describe operational and organisational security.

In the first part of the course, you will study the general concepts of network security, including access control models, authentication methods, non-essential services and protocols, combating attacks, malicious code and auditing techniques.

The second section covers the features of communication security including remote access security, email security, web security, directory security, file transfer security and wireless security.

The third section covers the features of infrastructure security including devices, media, security topologies, intrusion detection and security baselines.

The fourth section covers the basics of cryptography, including cryptographic algorithms, uses of cryptography, public key infrastructure, standards and protocols, key management and certificate lifecycle

The final section covers operational and organisational security, including physical security, disaster recovery, business continuity, policies and procedures, privilege management, forensics, risk identification, education and training and documentation

There will be a closed-book multiple-choice assessment covering all outcomes. You will be presented with 50 questions and expected to answer 70% of these correctly. You will also be expected to keep a log book recording the practical tasks you have carried out during the Unit. You must satisfy the requirements for these assessments in order to achieve the Unit.

This Unit may assist you in preparing for CompTIA examination SY0-101: Security+. Vendor certifications can change rapidly, so you should check the current details at **www.comptia.org** to ensure that all objectives have been covered. This examination can also contribute towards the Microsoft Certified Systems Administrator (MCSA) or Microsoft Certified Systems Engineer (MCSE) awards.