Higher National Unit Specification

General information for centres

Unit title: Network Security: Implementation and Administration

Unit code: DG08 35

Unit purpose: This Unit is designed to introduce candidates to the issues involved in implementing and administering network security. It is intended for candidates undertaking an HNC or HND in Computing, Computer Networking or a related area who require a detailed knowledge of network security.

On completion of the Unit candidates should be able to:

1. Implement, manage and troubleshoot security policies.
2. Implement, manage and troubleshoot security updates.
3. Implement, manage and troubleshoot security for network communications.
4. Configure, manage and troubleshoot authentication and remote access security
5. Plan, configure and troubleshoot authorisation and Public Key Infrastructure.

Credit value: 2 HN credits at SCQF level 8: (16 SCQF credit points at SCQF level 8)

**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 DF9P 34 Network Concepts, DF9N 34 Network Server Operating System and DG02 34 Security 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.

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.

General information for centres (cont)

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 administrator must be restricted to matters relating to the administration of the 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.

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.

Higher National Unit specification: statement of standards

Unit title: Network Security: Implementation and Administration

Unit code: DG08 35

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

Implement, manage and troubleshoot security policies.

Knowledge and/or skills

- Configure and deploy security templates.
- Troubleshoot security template problems.
- Configure additional security based on computer roles.

Evidence Requirements

Restricted response test

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

1. Configure and deploy security templates.

   Registry and file system permissions, account policies, audit policies, user rights assignment, security options, system services, restricted groups, event logs, deployment using Group Policy and scripting.

2. Troubleshoot security template problems.

   Group Policy, upgraded operating systems, mixed client-computer operating systems.

3. Configure additional security based on computer roles.

   Database server, mail server, domain controller, authentication server, web server, client computers.

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

Higher National Unit specification: statement of standards (cont)

Unit title: Network Security: Implementation and Administration

Alternatively, the 7 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 **at least two** of the three tasks listed below. The tasks to be completed must be selected by the tutor.

1. Configure and deploy security templates.

   Documentary evidence that the candidate can configure and deploy security templates.

2. Troubleshoot security template problems.

   Documentary evidence that the candidate can troubleshoot at least two security template problems arising from Group Policy, upgraded operating systems or mixed client-computer operating systems.

3. Configure additional security based on computer roles.

   Documentary evidence that the candidate can configure additional security based on computer roles for at least two of the following roles: database server, mail server, domain controller, authentication server, web server, client computers.

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.

Unit title: Network Security: Implementation and Administration

Outcome 2

Implement, manage and troubleshoot security updates

Knowledge and/or skills

- Plan the deployment of security updates.
- Assess the current status of security updates.
- Deploy security updates.

Evidence Requirements

Restricted response test

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

1. Plan the deployment of security updates

   Applicability, compatibility, rollback strategy.

2. Assess the current status of security updates.

   Using system tools.

3. Deploy security updates.

   Slipstreaming, remote installation, custom scripts and isolated networks. Server computers and remote client computers. Using system tools. Troubleshooting.

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

Alternatively, the 8 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 **at least two** of the three tasks listed below. The tasks to be completed must be selected by the tutor.

Unit title: Network Security: Implementation and Administration

1. Plan the deployment of security updates

   Documentary evidence that the candidate can plan the deployment of security updates, taking account of applicability, compatibility and rollback strategy.

2. Assess the current status of security updates.

   Documentary evidence that the candidate can use system tools to assess the current status of security updates.

3. Deploy security updates.

   Documentary evidence that the candidate can use system tools to deploy security updates.

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 3

Implement, manage and troubleshoot security for network communications.

Knowledge and/or skills

- Plan IPSec deployment
- Configure IPSec
- Deploy and manage IPSec policies
- Troubleshoot IPSec
- Plan and implement security for wireless networks
- Deploy, manage and configure SSL certificates

Higher National Unit specification: statement of standards (cont)

Unit title: Network Security: Implementation and Administration

Evidence Requirements

Restricted response test

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

1. Plan IPSec deployment

   Mode, authentication methods, functionality of applications and services.

2. Configure IPSec.

   Domain controllers, web servers, databases, e-mail servers, and client computers; IPSec authentication, encryption levels, IPSec protocol, IPSec certificates

3. Deploy and manage IPSec policies

   Local/Group policies, commands and scripts, IPSec certificates.

4. Troubleshoot IPSec.

   IPSec rule configurations, firewall configurations, routers, and authentication.

5. Plan and implement security for wireless networks.

   Wireless encryption levels, wireless network connection settings

6. Deploy, manage and configure SSL certificates.

   Renewing certificates; obtaining self-issued certificates versus public-issued certificates; obtain public and private certificates; install certificates for SSL.

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 3 must record successful completion by the candidate of **at least three** of the six tasks listed below. The tasks to be completed must be selected by the tutor.

Higher National Unit specification: statement of standards (cont)

Unit title: Network Security: Implementation and Administration

1. Plan IPSec deployment

   Documentary evidence that the candidate can plan IPSec deployment.

2. Configure IPSec.

   Documentary evidence that the candidate can configure IPSec.

3. Deploy and manage IPSec policies.

   Documentary evidence that the candidate can deploy and manage IPSec policies.

4. Troubleshoot IPSec.

   Documentary evidence that the candidate can troubleshoot IPSec.

5. Plan and implement security for wireless networks.

   Documentary evidence that the candidate can plan and implement security for wireless networks.

6. Deploy, manage and configure SSL certificates.

   Documentary evidence that the candidate can deploy, manage and configure SSL certificates.

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.

In the case of this outcome, the log book must demonstrate the completion of practical tasks relating to at least four of the six areas outlined above.

Unit title: Network Security: Implementation and Administration

Outcome 4

Configure, manage and troubleshoot authentication and remote access security

Knowledge and/or skills

- Configure and troubleshoot authentication.
- Configure and troubleshoot authentication for Web users.
- Configure authentication for security-enhanced remote access.
- Configure and troubleshoot virtual private network (VPN) protocols.
- Manage client-computer configuration for remote access security.

Evidence Requirements

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

1. Configure and troubleshoot authentication.

   Configure authentication protocols to support mixed Windows client-computer environments; interoperability of Kerberos authentication with UNIX computers; authentication for extranet scenarios; trust relationships; authentication for members of non-trusted domain.

2. Configure and troubleshoot authentication for Web users.

   Authentication types include Basic, Integrated Windows, anonymous, digest, and client certificate mapping.

3. Configure authentication for security-enhanced remote access.

   Authentication types include PAP, CHAP, MS-CHAP, MS-CHAP v2, EAP-MD5, EAP-TLS, and multi-factor authentication with smart cards and EAP.

4. Configure and troubleshoot virtual private network (VPN) protocols.

   Internet service provider (ISP), client-computer operating system, Network Address Translation (NAT) devices, remote access server, and firewall server.

5. Manage client-computer configuration for remote access security.

   Using system tools.

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

Alternatively, the 12 questions for this outcome may contribute towards a single end-of-unit test of 50 questions.

Logbook

The logbook for Outcome 4 must record successful completion by the candidate of **at least three** of the five tasks listed below. The tasks to be completed must be selected by the tutor.

1. Configure and troubleshoot authentication.

   Documentary evidence that the candidate can configure authentication protocols to support mixed Windows client-computer environments in at least two of the following scenarios:

   - configure the interoperability of Kerberos authentication with UNIX computers;
   - configure authentication for extranet scenarios;
   - configure trust relationships;
   - configure authentication for members of non-trusted domain.

2. Configure and troubleshoot authentication for Web users.

   Documentary evidence that the candidate can configure and troubleshoot authentication for Web users using at least two of the following authentication types: Basic, Integrated Windows, anonymous, digest and client certificate mapping.

3. Configure authentication for security-enhanced remote access.

   Documentary evidence that the candidate can configure authentication for security-enhanced remote access using at least two of the following authentication types: PAP, CHAP, MS-CHAP, MS-CHAP v2, EAP-MD5 and EAP-TLS.

4. Configure and troubleshoot virtual private network (VPN) protocols.

   Documentary evidence that the candidate can configure and troubleshoot virtual private network (VPN) protocols

5. Manage client-computer configuration for remote access security.

   Documentary evidence that the candidate can use system tools to manage client-computer configuration for remote access security.

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

Plan, configure and troubleshoot authorisation and Public Key Infrastructure.

Knowledge and/or skills

- Plan group structure
- Plan and configure authorisation
- Install, manage and configure certificate services

Evidence Requirements

Restricted response test

The knowledge and skills component of Outcome 5 must be examined by eight questions, three being derived from two of the three items listed below and two being derived from the remaining item. Each question must be derived from a single item.

1. Plan group structure

   Type of groups, security group scope, nested group structure.

2. Plan and configure authorisation

   Access control lists, user rights, digital signatures.

Higher National Unit specification: statement of standards (cont)

Unit title: Network Security: Implementation and Administration

3. Install, manage and configure certificate services

   Certification authorities, certificate templates, certificate revocation lists, key recovery

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

Alternatively, the 8 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 **at least two** of the three tasks listed below. The tasks to be completed must be selected by the tutor.

1. Plan group structure

   Documentary evidence that the candidate can plan group structure, taking account of type of groups, security group scope and nested group structure.

2. Plan and configure authorisation

   Documentary evidence that the candidate can plan and configure authorisation, taking account of access control lists, user rights and digital signatures.

3. Install, manage and configure certificate services.

   Documentary evidence that the candidate can install, manage and configure certificate services, taking account of certification authorities, certificate templates, certificate revocation lists and key recovery.

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.

Administrative Information

Unit code:	DG08 35
Unit title:	Network Security: Implementation and Administration
Superclass category:	CB
Date of publication:	May 2004
Version:	01
Source:	SQA

Additional copies of this Unit specification can be purchased from the Scottish Qualifications Authority. The cost for each Unit specification is £2.50. (A handling charge of £1.95 will apply to all orders for priced items.)

Higher National Unit specification: support notes

Unit title: Network Security 2: Implementation and Administration

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:	12 hours
Outcome 2:	12 hours
Outcome 3:	24 hours
Outcome 4:	20 hours
Outcome 5:	12 hours

Guidance on the content and context for this Unit

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.

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.

The following notes assume that the unit will be delivered using a Microsoft operating system, such as Windows 2000/2003 Server. However, no restriction is placed on the operating system to be used and centres are free to choose alternative operating systems such as Linux/Unix, although this may require changes in terminology.

This Unit may assist candidates in preparing for Microsoft examinations 70-214: Implementing and Administering Network Security or 70-299: Implementing and Administering Network Security in a Microsoft Windows 2003 Server Network. Vendor certifications can change rapidly and candidates should check the current details at **www.microsoft.com/traincert** to ensure that all objectives have been covered. These examinations can contribute towards the Microsoft Certified Systems Administrator (MCSA) or Microsoft Certified Systems Engineer (MCSE) awards.

Unit title: Network Security 2: Implementation and Administration

The content of this unit may be delivered using relevant vendor-supplied materials, such as Microsoft Official Curriculum (MOC). As these materials are under continuous development, centres should check carefully to ensure that such materials meet all the requirements for the unit. If MOC materials are used, some of the practical tasks involved may contribute towards the practical assessments required for the unit.

Outcome 1: Implement, manage and troubleshoot security policies.

1 Configure and deploy security templates.

Candidates should be able to configure security templates. This includes configuring registry and file system permissions, account policies, .pol files, audit policies, user rights assignment, security options, system services, restricted groups and event logs. They should also be able to plan the deployment of security templates, and use a variety of deployment methods including Active Directory-based Group Policy Objects (GPOs), command-line tools and scripting.

2 Troubleshoot security template problems.

Candidates should also be able to diagnose and troubleshoot security template problems in a mixed operating systems environment and troubleshoot security policy inheritance and removal of security template settings.

3 Configure additional security based on computer roles.

Candidates should also be able to configure additional security based on computer roles including server roles such as SQL Server, Exchange Server, domain controller, Internet Authentication Service (IAS) server and Internet Information Services (IIS) server and client computer roles, such as desktop, portable and kiosk. They should be able to plan and configure security settings and software restriction policies, plan network zones for computer roles and plan security for infrastructure services such as DHCP and DNS.

They should be able to plan and configure auditing and logging for a computer role, taking account of Windows Events, Internet Information Services (IIS), firewall log files, Netlog and RAS log files and analyse security configuration using tools such as the Microsoft Baseline Security Analyser (MBSA), the MBSA command-line tool and Security Configuration and Analysis. They should be able to use Group Policy to tailor the user experience for different classes of workers and restrict access to management tools and web browser configuration.

Higher National Unit specification: support notes (cont)

Unit title: Network Security 2: Implementation and Administration

Outcome 2: Implement, manage and troubleshoot security updates

1 Plan the deployment of security updates.

Candidates should be able to plan the deployment of service packs and hotfixes, including evaluating applicability, testing compatibility with existing applications, planning deployment environments for both pilot and production phases, planning batch deployment of multiple hotfixes and planning rollback strategy.

2 Assess the current status of security updates.

They should be able to assess the current status of service packs and security updates, including assessing current patch levels by using the MBSA GUI tool and using the MBSA command-line tool with scripted solutions.

3 Deploy security updates.

Candidates should also be able to install service packs and security updates on new and existing client computers and servers, taking account of slipstreaming, using Remote Installation Services (RIS), custom scripts, and isolated networks. They should be able to manage service packs and security updates, using system tools such as Microsoft Software Update Service, Automatic Updates, and SMS, and diagnose and resolve problems relating to the deployment of service packs and security updates, including third-party application compatibility, permissions and version conflicts.

Outcome 3: Implement, manage and troubleshoot security for network communications.

1 Plan IPSec deployment

Candidates should be able to plan IPSec deployment, including deciding which IPSec mode to use, planning authentication methods and testing the functionality of existing applications and services.

2 Configure IPSec

Candidates should be able to configure IPSec policies to secure communication between networks and hosts, including domain controllers, Internet Web servers, databases, e-mail servers, and client computers. They should also be able to configure IPSec authentication, configure appropriate encryption levels, taking account of perfect forward secrecy (PFS) and key lifetimes, configure the appropriate IPSec protocol, including Authentication Header (AH) and Encapsulating Security Payload (ESP) and configure IPSec inbound and outbound filters and filter actions.

3 Deploy and manage IPSec policies

Candidates should be able to deploy and manage IPSec policies by using Local policy objects or Group Policy objects (GPOs) and by using commands and scripts. Tools include IPSecPol and NetSh. They should also be able to deploy and renew IPSec certificates on managed and unmanaged client computers.

4 Troubleshoot IPSec

Candidates should be able to troubleshoot IPSec, including monitoring IPSec policies by using IP Security Monitor, configuring IPSec logging, including Oakley logs and IPSec driver logging, troubleshoot IPSec across networks, including network address translation, port filters, protocol filters, firewalls and routers and troubleshoot IPSec certificates including enterprise trust policies and certificate revocation list (CRL) checking.

5 Plan and implement security for wireless networks

Candidates should be able to plan and implement security for wireless networks, including planning authentication and encryption methods and access policies, configuring wireless encryption and installing and configuring wireless support for client computers.

6 Deploy, manage and configure SSL certificates

Candidates should be able to deploy and manage SSL certificates, including obtaining and renewing public and private certificates. They should be aware of the distinction between self-issued certificates and public-issued certificates. They should also be able to configure SSL to help protect communication channels including client computer to web server, web server to SQL server, client computer to Active Directory domain controller, and e-mail server to client computer.

Outcome 4: Configure, manage and troubleshoot authentication and remote access security

1 Configure and troubleshoot authentication.

Candidates should be able to configure authentication protocols to support mixed Windows client-computer environments and configure the interoperability of Kerberos authentication with UNIX computers. They should also be able to configure authentication for extranet scenarios, plan, configure and troubleshoot trust relationships and configure authentication for members of non-trusted domains.

Unit title: Network Security 2: Implementation and Administration

2 Configure and troubleshoot authentication for Web users.

Candidates should be able to configure and troubleshoot authentication for Web users and be aware that authentication types include Basic, Integrated Windows, anonymous, digest, and client certificate mapping.

3 Configure authentication for security-enhanced remote access.

Candidates should also be able to configure authentication for security-enhanced remote access and be aware that authentication types include PAP, CHAP, MS-CHAP, MS-CHAP v2, EAP-MD5, EAP-TLS, and Multi-factor authentication with smart cards and EAP.

4 Configure and troubleshoot virtual private network (VPN) protocols.

Candidates should be able to configure and troubleshoot virtual private network (VPN) protocols and identify and resolve problems relating to Internet service provider (ISP), client-computer operating system, Network Address Translation (NAT) devices, Routing and Remote Access server and firewall server.

5 Manage client-computer configuration for remote access security.

Candidates should also be able to manage client-computer configuration for remote access security by using system tools such as Remote Access Policy and Connection Manager Administration Kit.

Outcome 5: Plan, configure and troubleshoot authorisation and Public Key Infrastructure.

1 Plan group structure

Candidates should be able to plan group structure, including deciding which types of groups to use, planning security group scope and planning nested group structure.

2 Plan and configure authorisation

Candidates should be able to plan and configure authorisation, including configuring access control lists (ACLs), planning and troubleshooting the assignment of user rights and planning requirements for digital signatures.

Unit title: Network Security 2: Implementation and Administration

3 Install, manage and configure certificate services

Candidates should also be able to install, manage and configure Certificate Services, including installing and configuring Certificate Authority (CA) hierarchies (enterprise, standalone, and third-party CAs). They should be able to install and configure the root, intermediate and issuing CA, taking account of renewals and hierarchy. They should also be able to configure certificate templates, configure archival and recovery of keys, and deal with LDAP queries, HTTP queries, and third-party CAs. They should be able to configure the publication of Certificate Revocation Lists (CRLs), configure public key Group Policy; configure certificate renewal and enrolment and deploy certificates to users, computers and CAs and backup and restore the CA.

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 a Unit which candidates are unlikely to find accessible at an introductory level; it is suggested that it be delivered only as part of an HNC/HND program in Computing or a related area. It should be delivered in tandem with other Computing Units and opportunities for teaching and assessment integration explored.

To minimise assessment overhead, one or more sets of restricted-response questions, totalling 50 questions in all, should be used to provide evidence of candidates' knowledge for all Outcomes. It is suggested that multiple-choice questions should 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. 75% of the questions must be answered correctly to pass each assessment. Candidates must also complete a log book or checklist recording the practical work undertaken for each outcome.

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).

Higher National Unit specification: support notes (cont)

Unit title: Network Security 2: Implementation and Administration

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: Network Security: Implementation and Administration

This is a 2-credit Unit at Level 8 intended for candidates undertaking a Computing or IT-related qualification who require a detailed knowledge of network security. It is designed to develop an understanding of the issues involved in implementing and administering network security. On completion of the Unit you should be able to:

- Implement, manage and troubleshoot security policies.
- Implement, manage and troubleshoot security updates.
- Implement, manage and troubleshoot security for network communications.
- Configure, manage and troubleshoot authentication and remote access security
- Plan, configure and troubleshoot authorisation and Public Key Infrastructure.

In the first part of the course, you will study implementing, managing and troubleshooting security policies, including configuring security templates, deploying security templates, troubleshooting security template problems, configuring additional security based on computer roles and configuring additional security for client-computer operating systems by using Group Policy.

The second section covers implementing, managing and troubleshooting service packs and security updates, including determining the current status of service packs and security updates, installing service packs and security updates on new and existing client computers and servers, managing service packs and security updates and troubleshooting the deployment of service packs and security updates.

The third section covers implementing, managing and troubleshooting security for network communications. This includes planning IPSec deployment, configuring and troubleshooting IPSec, planning and implement security for wireless networks, deploying, managing and configuring SSL certificates and configuring security for remote access users.

The fourth section covers configuring, managing and troubleshooting authentication and remote access security, including authentication for Web users and authentication for security-enhanced remote access and configuring and troubleshooting virtual private network (VPN) protocols and managing client-computer configuration for remote access security.

The final section covers planning, configuring and troubleshooting authorisation and Public Key Infrastructure. This includes planning group structure, planning and configuring authorisation and installing, managing and configuring certificate services

There will be one or more closed-book restricted-response assessments covering all outcomes. You will be presented with a total of 50 questions and expected to answer 75% 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.

General information for candidates (cont)

This Unit may assist you in preparing for Microsoft examinations 70-214: Implementing and Administering Network Security or 70-299: Implementing and Administering Security in a Microsoft Windows Server 2003 Network. Vendor certifications can change rapidly and you should check the current details at **www.microsoft.com/traincert** to ensure that all objectives have been covered. These examinations can contribute towards the Microsoft Certified Systems Administrator (MCSA) or Microsoft Certified Systems Engineer (MCSE) awards.