**Higher National Unit Specification**

## General information for centres

**Unit title:** Network Design: Security

**Unit code:** DG0E 36

**Unit purpose:** This Unit is designed to introduce candidates to the issues involved designing a secure computer network. It is intended for candidates undertaking an HNC or HND in Computing or a related area who require a detailed knowledge of secure network design. On completion of the Unit candidates should be able to:

1. Create the conceptual design for network infrastructure security.
2. Create the logical design for network infrastructure security.
3. Create the physical design for network infrastructure security.
4. Design an access control strategy for data.
5. Create the physical design for client infrastructure security.

**Credit value:** 1 HN credits at SCQF level 9: (8 SCQF credit points at SCQF level 9)

**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 operating systems and computer networks. This may be demonstrated by the possession of HN Units such as DF9N 34 Network Server Operating System, DF9R 35 Network Infrastructure 1: Implementation and Management and DG00 35 Network Infrastructure 2: Planning and Maintenance.

**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 30 restricted-response questions, based on one or more network design case studies, 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.

## General information for centres (cont)

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 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 Design: Security

## Unit code: DG0E 36

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

Create the conceptual design for network infrastructure security.

**Knowledge and/or skills**

- Analyse business requirements for designing security.
- Design a framework for designing and implementing security.
- Analyse technical constraints when designing security.

**Evidence requirements**

**Restricted response test**

The knowledge and skills component of Outcome 1 must be examined by six questions, based on one or more network design case studies. Two of the questions must be derived from each of the three items listed below. Each question must be derived from a single item.

1. Analyse business requirements for designing security.

   Existing policies and procedures, sensitivity of data, cost, legal requirements, end-user impact, interoperability, maintainability, scalability, risk.

2. Design a framework for designing and implementing security.

   Prevention, detection, isolation, and recovery.

3. Analyse technical constraints when designing security.

   Capabilities of existing infrastructure, technology limitations, interoperability constraints.

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 30 questions.

**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 based on case studies is 3 minutes for each question plus 5 minutes starting-up time and 5 minutes finishing-off time, thus a total of 100 minutes should be allocated for a 30-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 40 minutes.

## Outcome 2

Create the logical design for network infrastructure security.

**Knowledge and/or skills**

- Design a public key infrastructure (PKI) that uses Certificate Services.
- Design a logical authentication strategy.
- Design security for network management.
- Design a security update infrastructure.

**Evidence requirements**

**Restricted response test**

The knowledge and skills component of Outcome 2 must be examined by eight questions, based on one or more network design case studies. Two of the questions must be derived from each of the four items listed below. Each question must be derived from a single item.

1. Design a public key infrastructure (PKI) that uses Certificate Services.

   Certification authority (CA) hierarchy implementation, enrolment, distribution, renewal, revocation and auditing processes, security for CA servers.

2. Design a logical authentication strategy.

   Certificate distribution, forest and domain trust models, interoperability requirements, account and password requirements.

3. Design security for network management.

   Risk management, administration tools, emergency management.

4. Design a security update infrastructure.

   Software update infrastructure, group policy, identifying computers that are not at the current patch level.

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 30 questions.

**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 based on case studies is 3 minutes for each question plus 5 minutes starting-up time and 5 minutes finishing-off time, thus a total of 100 minutes should be allocated for a 30-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 40 minutes.

## Outcome 3

Create the physical design for network infrastructure security.

**Knowledge and/or skills**

- Design network infrastructure security
- Design security for wireless networks
- Design security for a web server
- Design security for communication between networks.
- Design security for different server roles.

## Higher National Unit specification: statement of standards (cont)

## Unit title: Network Design: Security

### Evidence requirements

### Restricted response test

The knowledge and skills component of Outcome 3 must be examined by ten questions, based on one or more network design case studies. Two of the questions must be derived from each of the five items listed below. Each question must be derived from a single item.

1. Design network infrastructure security

   Firewall configuration, IP filtering, IPSec policy, DNS implementation, data transmission.

2. Design security for wireless networks

   Public and private wireless LANs, 802.1x authentication.

3. Design security for a web server

   User authentication, technical requirements / minimum required services, monitoring strategy, baseline, content management strategy.

4. Design security for communication between networks.

   Protocols for VPN access, VPN connectivity, demand-dial routing between internal networks, communication with external organizations, extranet infrastructure, cross-certification of certificate services.

5. Design security for different server roles.

   Domain controller, network infrastructure server, file server, IIS server, terminal server, POP3 mail server, baseline security template.

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 30 questions.

### 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 based on case studies is 3 minutes for each question plus 5 minutes starting-up time and 5 minutes finishing-off time, thus a total of 100 minutes should be allocated for a 30-question end-of-unit test.

## Higher National Unit specification: statement of standards (cont)

## Unit title: Network Design: Security

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 40 minutes.

## Outcome 4

Design an access control strategy for data

**Knowledge and/or skills**

- Design an access control strategy for directory services.
- Design an access control strategy for files and folders.
- Design an access control strategy for the registry.

**Evidence requirements**

**Restricted response test**

The knowledge and skills component of Outcome 4 must be examined by 3 questions, based on one or more network design case studies. Each of the questions must be derived from one of the three items listed below. Each question must be derived from a single item.

1. Design an access control strategy for directory services.

   Delegation strategy, auditing requirements, group strategy for accessing resources, permission structure for directory service objects

2. Design an access control strategy for files and folders.

   Encryption and decryption, permission structure, backup and recovery strategy, auditing requirements.

3. Design an access control strategy for the registry.

   Permission structure, auditing requirements.

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

Alternatively, the 3 questions for this outcome may contribute towards a single end-of-unit test of 30 questions.

**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 based on case studies is 3 minutes for each question plus 5 minutes starting-up time and 5 minutes finishing-off time, thus a total of 100 minutes should be allocated for a 30-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 40 minutes.

## Outcome 5

Create the physical design for client infrastructure security.

**Knowledge and/or skills**

- Client authentication strategy.
- Security strategy for client remote access.
- Strategy for securing client computers.

**Evidence requirements**

**Restricted response test**

The knowledge and skills component of Outcome 5 must be examined by three questions, based on one or more network design case studies. Each of the questions must be derived from one of the three items listed below. Each question must be derived from a single item.

1. Design a client authentication strategy.

   Authentication requirements, account and password security requirements.

2. Design a security strategy for client remote access.

   Remote access policies, access to internal resources, authentication provider and accounting strategy.

3. Design a strategy for securing client computers.

   Desktop and portable computers, hardening client operating systems, restricting user access to operating system features.

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

Alternatively, the 3 questions for this outcome may contribute towards a single end-of-unit test of 30 questions.

**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 based on case studies is 3 minutes for each question plus 5 minutes starting-up time and 5 minutes finishing-off time, thus a total of 100 minutes should be allocated for a 30-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 40 minutes.

## Administrative Information

**Unit code:** DG0E 36

**Unit title:** Network Design: Security

**Superclass category:** CB

**Date of publication:** May 2004

**Version:** 01

**Source:** SQA

## Higher National Unit specification: support notes

## **Unit title:** Network Design: Security

This part of the Unit specification is offered as guidance.

The support notes are not mandatory.

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

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

Outcome 1: 10 hours
Outcome 2: 10 hours
Outcome 3: 10 hours
Outcome 4: 6 hours
Outcome 5: 4 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 significant changes in terminology.

This Unit may assist candidates in preparing for Microsoft examination 70-298: Designing Security for a Microsoft Windows 2003 Server Network. Vendor certifications can change rapidly and candidates should be encouraged the check the current details at **www.microsoft.com/traincert** to ensure that all objectives have been covered. This examination can contribute towards the Microsoft Certified Systems Engineer (MCSE) award.

The content of this unit may be delivered using 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.

## Higher National Unit specification: support notes (cont)

## Unit title: Network Design: Security

### Outcome 1

This outcome is about creating the conceptual design for network infrastructure security by gathering and analysing business and technical requirements.

### 1 Analyse business requirements for designing security

Candidates should be able to analyse business requirements for designing security. This includes existing policies and procedures, sensitivity of data, cost, legal requirements, end-user impact, interoperability, maintainability, scalability and risk. They should be able to analyse existing security policies and procedures, analyse the organizational requirements for securing data, analyse the security requirements of different types of data and analyse risks to security within the current it administration structure and security practices.

### 2 Design a framework for designing and implementing security

Candidates should also be able to design a framework for designing and implementing security. The framework should include prevention, detection, isolation, and recovery. They should know how to predict threats to a network from internal and external sources, design a process for responding to incidents, design segmented networks and design a process for recovering services.

### 3 Analyse technical constraints when designing security

Candidates should be able to analyse technical constraints when designing security, identify capabilities of the existing infrastructure, identify technology limitations and analyse interoperability constraints.

### Outcome 2

This Outcome is about creating the logical design for network infrastructure security.

### 1 Design a public key infrastructure (PKI) that uses Certificate Services

Candidates should be able to design a public key infrastructure (PKI) that uses Certificate Services and design a certification authority (CA) hierarchy implementation. Types include geographical, organizational, and trusted. They should also know how to design enrolment and distribution processes, establish renewal, revocation and auditing processes and design security for CA servers.

### 2 Design a logical authentication strategy

Candidates should be able to design a logical authentication strategy, including designing certificate distribution, designing forest and domain trust models, designing security that meets interoperability requirements and establishing account and password requirements.

### 3 Design security for network management

Candidates should be able to design security for network management, manage the risk of managing networks and design the administration of servers by using common administration tools such as: Microsoft Management Console (MMC), Terminal Server, Remote Desktop for Administration, Remote Assistance, and Telnet. They should also be able to design security for Emergency Management Services.

### 4 Design a security update infrastructure

Candidates should also be able to design a security update infrastructure, design a Software Update Services (SUS) infrastructure, design Group Policy to deploy software updates and design a strategy for identifying computers that are not at the current patch level.

**Outcome 3**

This Outcome covers creating the physical design for network infrastructure security.

### 1 Design network infrastructure security

Candidates should be able to design network infrastructure security, including specifying the required protocols for a firewall configuration, designing IP filtering, designing an IPSec policy. securing a DNS implementation and designing security for data transmission.

### 2 Design security for wireless networks

Candidates should be able to design security for wireless networks, including public and private wireless LANs and design 802.1x authentication.

### 3 Design security for a web server

Candidates should also be able to design user authentication for Internet Information Services (IIS), design user authentication for a Web site by using certificates, by using IIS authentication or by using RADIUS for IIS authentication and be able to design security for Internet Information Services (IIS) and for Web sites that have different technical requirements by enabling only the minimum required services, design a monitoring strategy for IIS, design an IIS baseline that is based on business requirements and design a content management strategy for updating an IIS server.

### 4 Design security for communication between networks

Candidates should also be able to design security for communication between networks, select protocols for VPN access, design VPN connectivity and demand-dial routing between internal networks as well as design security for communication with external organizations, design an extranet infrastructure and design a strategy for cross-certification of Certificate Services.

### 5 Design security for different server roles

Candidates should be able to design security for servers that have specific roles, including s include domain controller, network infrastructure server, file server, IIS server, terminal server, and POP3 mail server, as well as define a baseline security template for all systems and create a plan to modify baseline security templates according to role.

**Outcome 4**

This Outcome is about designing an access control strategy for data.

### 1 Design an access control strategy for directory services

Candidates should be able to design an access control strategy for directory services, create a delegation strategy, analyse auditing requirements, design the appropriate group strategy for accessing resources and design a permission structure for directory service objects.

### 2 Design an access control strategy for files and folders

Candidates should also be able to design an access control strategy for files and folders, design a strategy for the encryption and decryption of files and folders, design a permission structure for files and folders, design security for a backup and recovery strategy and analyse auditing requirements.

### 3 Design an access control strategy for the registry

Candidates should be able to design an access control strategy for the registry, design a permission structure for registry objects and analyse auditing requirements.

**Outcome 5**

This Outcome is about creating the physical design for client infrastructure security.

### 1 Client authentication strategy

Candidates should be able to design a client authentication strategy, analyse authentication requirements and establish account and password security requirements.

### 2 Security strategy for client remote access

Candidates should also be able to design a security strategy for client remote access, design remote access policies, design access to internal resources and design an authentication provider and accounting strategy for remote network access by using Internet Authentication Service (IAS).

### 3 Strategy for securing client computers

Candidates should also be able to design a strategy for securing client computers, including desktop and portable computers, design a strategy for hardening client operating systems and design a strategy for restricting user access to operating system features.

## 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 closed-book restricted-response questions, totalling 30 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. 70% of the questions must be answered correctly.

## 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 Design: Security

## 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 Design: Security

This is a 1-credit Unit at Level 9 intended for candidates undertaking a Computing or IT-related qualification who require a detailed knowledge of secure network design It is designed to develop an understanding of the issues involved designing a secure computer network. On completion of the Unit you should be able to:

- Create the conceptual design for network infrastructure security.
- Create the logical design for network infrastructure security.
- Create the physical design for network infrastructure security.
- Design an access control strategy for data.
- Create the physical design for client infrastructure security.

In the first part of the course, you'll learn how to create the conceptual design for network infrastructure security. This includes analysing business requirements for designing security, designing a framework for designing and implementing security and analysing technical constraints when designing security.

The second section covers creating the logical design for network infrastructure security, including designing a public key infrastructure (PKI) that uses Certificate Services, designing a logical authentication strategy, designing security for network management and designing a security update infrastructure.

The third section is about creating the physical design for network infrastructure security. You'll learn how to design network infrastructure security, design security for wireless networks, design security for a web server, design security for communication between networks and design security for different server roles.

The fourth section covers designing an access control strategy for data. You'll learn how to design an access control strategy for directory services, design an access control strategy for files and folders and design an access control strategy for the registry.

The final section covers creating the physical design for client infrastructure security. You'll learn how to design a client authentication strategy, design a security strategy for client remote access and design a strategy for securing client computers.

There will be a closed-book multiple-choice assessment covering all outcomes. You will be presented with a total of 30 questions and expected to answer 70% of these correctly.

This Unit may assist you in preparing for Microsoft examination 70-298: Designing Security for a Microsoft Windows 2003 Server Network. Vendor certifications can change rapidly, so you should check the current details at **www.microsoft.com/traincert** to ensure that all objectives have been covered. This examination can contribute towards the Microsoft Certified Systems Engineer (MCSE) award.