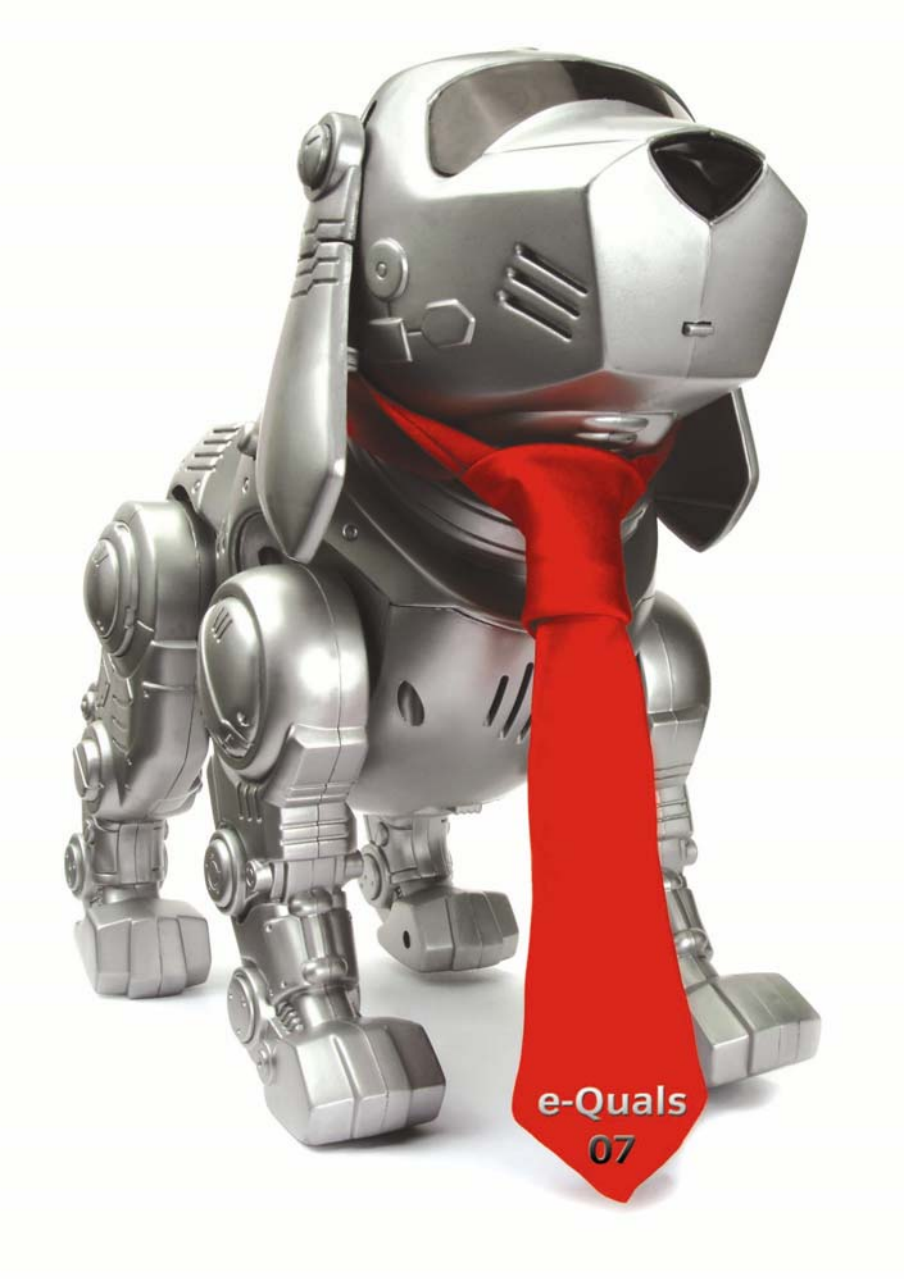
e-Quals Unit Syllabus

Level 3 Implementing an ICT systems security policy (7266/7267-511)

www.cityandguilds.com/e-quals07
November 2008
Version 2.0



About City & Guilds

City & Guilds is the UK's leading provider of vocational qualifications, offering over 500 awards across a wide range of industries, and progressing from entry level to the highest levels of professional achievement. With over 8500 centres in 100 countries, City & Guilds is recognised by employers worldwide for providing qualifications that offer proof of the skills they need to get the job done.

City & Guilds Group

The City & Guilds Group includes City & Guilds, ILM (the Institute of Leadership & Management) which provides management qualifications, learning materials and membership services, NPTC which offers land-based qualifications and membership services, and HAB (the Hospitality Awarding Body). City & Guilds also manages the Engineering Council Examinations on behalf of the Engineering Council.

Equal opportunities

City & Guilds fully supports the principle of equal opportunities and we are committed to satisfying this principle in all our activities and published material. A copy of our equal opportunities policy statement *Access to assessment and qualifications* is available on the City & Guilds website.

Copyright

Publications

City & Guilds publications are available on the City & Guilds website or from our Publications Sales department at the address below or by telephoning +44 (0)20 7294 2850 or faxing +44 (0)20 7294 3387.

City & Guilds
1 Giltspur Street
London EC1A 9DD
T +44 (0)20 7294 2800
F +44 (0)20 7294 2400
www.cityandguilds.com
enquiry@cityandguilds.com

Contents

Unit 511 Implementing an ICT systems security policy

Rationale

This unit will provide the candidate with the basic knowledge and principles to implement a security policy on data networks and computer systems. Candidates will be able to understand the practical steps a network/system administrator can take to mitigate the threats to the network and the consequent effects of any attacks. Additionally candidates will be able to understand the business implications of network and system downtime as a result of attacks on computer systems.

Learning outcomes

There are **four** outcomes to this unit. The candidate will be able to:

- Analyse and identify ICT system security issues
- Implement security on email and instant messaging systems
- Implement and maintain internet and network security
- Maintain data integrity and system security

Guided learning hours

It is recommended that 60 hours should be allocated for this unit. This may be on a full time or part time basis.

Connections with other qualifications

This unit contributes towards the knowledge and understanding required for the following qualifications:

NVQ for IT Professionals (4324) Level 3

Outcome	Unit
4	320 User profile administration
1, 2, 3, 4	310 Security for ICT Systems

Key Skills

Application of number	N/A
Communication	3.2
ICT	2.1
Working with others	N/A
Problem solving	3.1
Improving own learning	2.1

Assessment and grading

Assessment will be by means of a **set assignment** covering both practical activities and underpinning knowledge.

Unit 511 Implementing an ICT systems security policy

Outcome 1 Analyse and identify ICT system security issues

Practical activities

The candidate will be able to:

1 Interpret building, network and system plans and diagrams, and interpret and identify

- a secure areas of buildings
- b internal network topologies
- c external network topologies
- d key networked ICT systems
- e data storage areas/facilities
- f networked and other vulnerable ICT systems and devices

2 identify vulnerable areas within an ICT system and describe the type of security risk in these areas

- a theft of confidential data
- b theft of copyrighted or other intellectual property
- c fraud or other financial risk
- d impact of any damage to company image due to publicity concerning security issues
- e loss of business functions due to system downtime
- f lack of productivity by employees due to system downtime

3 suggest the financial impact to the organisation due to ICT system downtime as a result of security issues

4 collate and record the data from the analysis and assessment.

5 make suggestions for a security policy based upon the conclusions reached, eg

- a physical access control
- b classification of staff roles and levels of access
- c password policies and enforcements
- d virus protection policies
- e acceptable use of ICT resources policy
- f staff education.

Underpinning knowledge

The candidate will be able to:

1 describe the differing type of security risks, eg
   - a physical access to unauthorised areas
   - b theft of data on removable media, disk/tape/CD/paper
   - c security risks and impacts to the business

2 recognise and classify types of security risk, eg
   - a virus attacks
   - b revenge attacks from disgruntled employees
   - c theft of valuable data
   - d 'hacking' attempts from outside the organisation
   - e physical risks – theft of data media

3 determine areas of security risk in an organisation's ICT network

4 describe appropriate data backup and replication procedures to allow the restoration of business-critical data in the event of an attack on ICT systems

5 describe the importance and purpose of a defined security policy

6 describe the roles and responsibilities of key personnel in an Incident Response Team

7 explain the motivations and classifications of those engaged in hacking, information theft and other ICT security issues and attacks, eg
   - a information theft for financial gain
   - b fraud
   - c political
   - d information subversion for black mail etc.
   - e peer group acceptance
   - f ideological

8 outline legal, ethical and human resource issues surrounding information protection and retention, eg
   - a confidentiality
   - b Data Protection Act 1998
   - c The Computer Misuse Act, 1990.

Unit 511 Implementing an ICT systems security policy

Outcome 2 Implement security on email and instant messaging systems

Practical activities

The candidate will be able to:

1 analyse a given network/ICT system in relation to email and messaging privacy and security requirements to identify
   - a risks due to possible information theft/subversion
   - b risks due to system downtime due to virus and other malicious attacks
   - c the current organisations email and messaging security policies and solutions

2 research current types of potential risk, eg
   - a virus attacks from attachments
   - b embedded malicious code in html based email such as Java, Active X and scripts
   - c email address spoofing
   - d alteration of email messages
   - e productivity loss due to spam
   - f offensive email – internal/external sources
   - g hoaxes and propagation of malicious content

3 research current industry solutions to combat the above
   - a virus scanning of incoming emails at network ingress
   - b virus scanning on client machines
   - c encryption techniques:
     - i S/MIME and certificate based technologies
     - ii PGP and like technologies
   - d spam email filtering and protection
   - e internet messaging

4 research major cost implications of implementing security solutions including:
   - a initial purchasing costs
   - b installation costs
   - c update and maintenance costs
   - d employee training costs – user and technical

5 select and justify the choice of email and messaging security solution with respect to functionality, business requirements and budget availability

6 identify the issues and considerations surrounding email and messaging privacy with respect to current laws concerning privacy and data protection
   - a employee email/message intercept
   - b e-mail retention
   - c acceptable use policies

Practical activities continued

7 implement basic security protection on an ICT system, i.e.
   a virus scanning
   b spam filtering
8 make recommendations for an organisation wide policy with relation to email and messaging systems and document it.

Underpinning knowledge

The candidate will be able to:

1 explain the importance and relevance of a defined policy relating to the use of email and messaging software
2 describe the vulnerabilities of SMTP (simple mail transfer protocol) eg
   a no encryption as standard
   b mail relaying issues
3 list the security issues relevant to instant messaging applications, eg
   a data is not encrypted and sent in the clear
   b other parties cannot be authenticated as who they say they are
   c stored passwords can be compromised
   d potential 'backdoor' for Trojans, viruses and worms
4 describe the basic features of computer viruses, eg
   a simply computer 'code'
   b usually hidden
   c written with malicious intent
5 list some common types of virus and malicious code, eg
   a Trojan horse
   b logic bomb
   c worms
6 describe common methods of preventing viruses entering and damaging ICT systems, eg
   a intrusion detection
   b virus scanning at the network edge
   c virus scanning on email servers
   d virus scanning on clients
   e user education
   f file filtering techniques – .exe files and other executables, etc.
7 list common limitations of the main virus protection systems available, eg
   a must be configured correctly to scan the correct files
   b must be continually updated
   c effectiveness can be limited if users are not trained and/or do not use the software
8 explain why it is important to keep abreast of emerging technologies, virus threats and other issues and threats relating to email and messaging technologies

Underpinning knowledge continued

9 explain the importance of ensuring that any software or hardware purchased to protect against viruses and other security threats are continually assessed for effectiveness

10 list sources of information relating to email and messaging security issues for IT professionals

11 explain the key financial considerations necessary when constructing a cost proposal for a security solution

12 explain the concepts of the following topics of forensics

- a Chain of Custody
- b Preservation of Evidence
- c Collection of Evidence.

Unit 511 Implementing an ICT systems security policy

Outcome 3 Implement and maintain internet and network security

Practical activities

The candidate will be able to:

1 Interpret diagrams and summaries of installed networking equipment in an organisation in order to

- a analyse risk areas
- b assess potential business risks

2 demonstrate with reference to given network diagrams and topologies potential security threats and risks.

3 Identify security risks associated with different networking media technologies eg

- a fibre based
- b wireless
- c copper based ethernet

4 identify hardware and software solutions to protect the network and client devices from attack

5 install and configure security software as appropriate in the organisation eg

- a hardware/software firewalls
- b virus protection
- c intrusion detection systems
- d proxy servers

6 access security related information and locate sources to enable downloading of software updates or patches

7 take appropriate action to remove unwanted networking protocols on the ICT network that may cause exposure to known security risks eg

- a netBEUI
- b routing protocols

8 select appropriate solutions and technologies to back up important data as part of disaster recovery strategies.

Underpinning knowledge

The candidate will be able to:

1 describe the importance of accurate current network diagrams

2 list some of the well known network protocols that may be unnecessary and that can cause security risks eg

- a SNMP (Simple Network Management Protocol)
- b ICMP (Internet Communication Management Protocol)
- c inappropriate or unauthenticated routing protocols

3 recognise well known network security concepts, potential attacks and vulnerabilities ie

- a spoofing
- b replay
- c dos/ddos (denial of service/distributed denial of service)
- d TCP/IP hijacking
- e man in the middle
- f exploitation of known hardware or software weaknesses
- g back door attacks

4 Recognize and understand the administration of the following Internet security concepts

- a SSL / TLS (Secure Sockets Layer / Transport Layer Security)
- b HTTP/S (Hypertext Transfer Protocol / Hypertext Transfer Protocol over Secure Sockets Layer)

5 explain well known internet security concepts and potential attacks and vulnerabilities that may affect computers and other networked devices ie

- a JavaScript
- b cookies
- c Active X
- d buffer overflows
- e applets
- f CGI scripting

6 describe the security issues inherent with differing networking media

- a coaxial – thinnet, thicknet
- b UTP/STP (Unshielded Twisted Pair/Shielded Twisted Pair)
- c fibre optic
- d wireless technologies (802.11X)

Underpinning knowledge continued

7 describe the particular security issues and solutions with wireless networking technologies
   a 802.11X
   b SSID (Service Set Identifier)
   c WEP (wireless encryption protocol)
   d EAP/LEAP (Extensible Authentication Protocol/LAN based Extensible Authentication Protocol)
   e TKIP (Temporal Key Integrity Protocol)
   f WPA (WiFi Protected Access)
   g 802.11i (IEEE proposed standard for wireless security)
8 describe the purpose and functions of network based security devices and solutions, eg
   a firewalls
   b network based intrusion detection systems
   c host based intrusion detection systems
   d honey pots
   e NAT and NAT-T
   f PAT
   g proxy servers
9 explain the purpose and concepts behind the following security topologies
   a DMZs (demilitarised zones)
   b intranets
   c extranets
   d VLAN (virtual local area network)
   e VPN (virtual private network)
10 describe the features of X.509 Certificates, Certification Authorities and Certification hierarchies
11 describe sources of security related information for IT professionals, eg
   a Cert
   b Infosec
   c Sans
   d FBI and other government related sites
   e vendor internet websites
12 explain the importance of ensuring that any software or hardware purchased to protect against viruses and other security threats is continually assessed for effectiveness
13 explain why it is important to keep abreast of emerging security related technologies, virus threats and other issues and threats relating to email and messaging technologies.

Practical activities

The candidate will be able to:

1 make appropriate recommendations for hardware and software to implement secure access to an organisations networks, eg

- a VPN
- b VLANs
- c encryption
- d authentication methods

2 Make recommendations to implement an organisation wide password policy, eg

- a password length
- b enforced change
- c choice of characters

3 Configure basic networking protocols in a secure manner on a dial up modem connection to an internet service provider (ISP) or other remote network, eg

- a CHAP
- b PAP.

Underpinning knowledge

The candidate will be able to:

1 describe the purpose and functions of authentication, authorisation and accounting principles in ICT security, eg
   - a TACACS
   - b RADIUS
   - c proxy server technology

2 describe and differentiate between access control models
   - a MAC (Mandatory Access Control)
   - b DAC (Discretionary Access Control)
   - c RBAC (Role Based Access Control)

3 understand the concepts of common encryption techniques
   - a shared key
   - b public key

4 outline the features of encryption techniques
   - a Diffe Helman
   - b RSA
   - c DES
   - d Triple DES
   - e Md5 Hashing
   - f non repudiation of messages

5 describe some of the relative strengths and weaknesses of encryption methods, eg
   - a ease of 'cracking' the encryption relative to bit length
   - b computation power required to encrypt data relative to the length of keys

6 explain some of the considerations when selecting the most appropriate encryption technique, eg
   - a consequences of data compromise
   - b cost of purchasing encryption software/hardware
   - c computing power available

7 explain common password weakness and attacks, eg
   - a brute force cracking
   - b dictionary cracking
   - c implications of the use of personal details for passwords

8 explain good password security practices, eg
   - a regular change of password
   - b enforced change of password
   - c enforced character length
   - d enforced mixing of characters/letters/numbers

Underpinning knowledge continued

9 recognise and explain the principles behind common methods of authentication
   a Kerberos
   b CHAP (Challenge Handshake Authentication Protocol)
   c PAP (Password Authentication Protocol)
   d certificates
   e tokens
   f multi-factor
   g mutual
   h biometrics

10 Recognize and understand the administration of the following directory security concepts
   a SSL / TLS (Secure Sockets Layer / Transport Layer Security)
   b LDAP (Lightweight Directory Access Protocol)
   c TACACS (Terminal Access Controller Access Control System)
   d L2TP / PPTP (Layer Two Tunnelling Protocol / Point to Point Tunnelling Protocol)
   e SSH (Secure Shell)
   f IPSEC (Internet Protocol Security)
   g vulnerabilities

11 recognise the role that 'social engineering' can play in compromising security, eg
   a third parties claiming to have been given permission to access systems
   b telephone calls asking for information from people masquerading as trusted parties
   c blackmail.

Unit record sheet

Use this form to track your progress through this unit.

Tick the boxes when you have covered each outcome. When they are all ticked, you are ready to be assessed.

Outcome	✓	Date
1 **Analyse and identify ICT system security issues**	☐	
2 **Implement security on email and instant messaging systems**	☐	
3 **Implement and maintain internet and network security**	☐	
4 **Maintain data integrity and system security**	☐	

Candidate Signature ..... **Date** .....

City & Guilds Registration Number .....

Quality nominee (if sampled) ..... **Date** .....

Assessor Signature ..... **Date** .....

External Verifier Signature (if sampled) ..... **Date** .....

Centre Name ..... **Centre Number** .....

Published by City & Guilds
1 Giltspur Street
London
EC1A 9DD
T +44 (0)20 7294 2468
F +44 (0)20 7294 2400
www.cityandguilds.com
www.cityandguilds.com/e-quals07