Unit title:	Network security
Unit number:	28
Level:	5
Credit value:	15
Guided learning hours:	60
Unit reference number:	D/601/1956

UNIT AIM AND PURPOSE

Learners will develop the skills, knowledge and understanding to enable them to design, implement, manage and support an effective, complex network security solution for a business.

LEARNING OUTCOMES AND ASSESSMENT CRITERIA

A pass grade is achieved by meeting **all** the requirements in the assessment criteria.

Learning Outcome (LO) The Learner will:	**Pass** The assessment criteria are the pass requirements for this unit. The Learner can:
LO1 Understand the impact on the social and commercial environment of network security design	1.1 evaluate a current system's network security 1.2 discuss the potential impact of a proposed network design 1.3 discuss current and common threats and their impact
LO2 Be able to design network security solutions	2.1 design a network security solution to meet a given specification 2.2 evaluate design and analyse feedback
LO3 Be able to implement network security solutions	3.1 using a design, implement a complex network security solution 3.2 systematically test the complex network security solution 3.3 document and analyse test results
LO4 Be able to manage network security solutions	4.1 manage a network security solution 4.2 analyse on-going network security policies and practices 4.3 recommend potential change management

GRADING CRITERIA

A merit grade is achieved by meeting **all** the requirements in the pass criteria **and** the merit descriptors.

A distinction grade is achieved by meeting **all** the requirements in the pass criteria **and** the merit descriptors **and** the distinction descriptors.

Merit Criteria (M1, M2, M3) (M1, M2, and M3 are mandatory to achieve a merit grade. Each must be achieved at least once per unit to achieve a merit grade.)	**Distinction Criteria (D1, D2, D3)** (D1, D2, and D3 are mandatory to achieve a distinction grade. Each must be achieved at least once per unit to achieve a distinction grade.) (In order to achieve a distinction grade, all merit criteria must also have been achieved.)
MANDATORY TO ACHIEVE A MERIT GRADE	MANDATORY TO ACHIEVE A DISTINCTION GRADE
M1 Analyse concepts, theories or principles to formulate own responses to situations.	D1 Evaluate approaches to develop strategies in response to actual or anticipated situations.
M2 Analyse own knowledge, understanding and skills to define areas for development.	D2 Evaluate and apply strategies to develop own knowledge, understanding and skills.
M3 Exercise autonomy and judgement when implementing established courses of action.	D3 Determine, direct and communicate new courses of action.

TEACHING CONTENT

The Teaching Content describes what has to be taught to cover **all** Learning Outcomes.

Learners must be able to apply relevant examples to their work although these do not have to be the same as the examples specified.

LO1 Understand the impact on the social and commercial environment of network security design	
Investigation techniques	Selection of appropriate investigation method to enable relevant information to be acquired, e.g. checklists, questionnaires, interviews, observations
Evaluation of network security in terms of	• network security – e.g. policies and procedures, penetration testing, contingency planning, due diligence, internal and external audits, baseline protection process, vetting of contractors, potential partners and staff in sensitive positions; content monitoring and filtering • social impact – financial trust, organisational trust, good will, corporate trust • impact on the individual/customer – e.g. public relations, social networking, social engineering, legal implications, (such as data protection, identity theft) • institutional impact – e.g. loss of production, loss of customer trust, loss of data, system down time, cost of data and system recovery, legal or regulatory investigations and consequences, (such as possible fines)
Current and common threats	e.g. hacking, viruses, time bombs, worms, trap doors, adware, spyware, malware, spam, cybercrime, hacktivism, phishing.
LO2 Be able to design network security solutions	
Security components	e.g. network firewall, email monitoring, intrusion detection and prevention, web monitoring and filtering, virtual private network, network vulnerability scan
Physical Security	Physical access control (e.g. biometrics, keypads, security personnel, lock and key, location), power supply resilience and backup supply, hardware and software built in redundancy, backup of data, configuration, recovery policies and procedures

User access	User name, group user membership, group access, personal rights, group rights for specific access to files, server, data, security sensitive workstations, printers, email, storage, regular review and updating of personal and group rights
External access	e.g. firewalls, rules, filters, application and packet monitoring, email monitoring, signature management, traffic filters, certifications and trust, network behavioural norms
Finance	Costs, benefits.
LO3 Be able to implement network security solutions	
Communication methods	e.g. routing protocols, VLANs, MANs, IEEE 802.1Q (dot 1q)
Systems	e.g. switch systems, router systems, firewalls (hardware and/or software), servers
Access Rights	e.g. user, group, network, device VLAN, MAN, address range, file, data, location, time constraints
Malware protection to policy level	Virus definition deployment, server, desktop, router,
Cryptography	e.g. key exchange methodology, encryption such as RSA, IPSEC, IKE, DES
Intrusion detection	e.g. firewall (hardware and/or software), traffic filters, web monitoring, access control
Testing	e.g. vulnerability testing, network mapping, buffer overflow, social engineering, log reviews.
LO4 Be able to manage network security solutions	
Policy review	e.g. IT Security policy and sub policies
System changes	e.g. impact on productivity, group or individual removal or addition, network device addition or removal, change of server, network removal or addition
Environmental testing	e.g. security audits, penetration testing
Systems monitoring	e.g. user access patterns, device behaviour, traffic types, traffic peaks, server activity.

GUIDANCE

Delivery guidance
It will be beneficial to deliver this unit in a way that uses actual events, industry forecasts or sector specific contexts which offer the learner the opportunity to explore, develop and apply the fundamental principles of the sector or subject area. Typical delivery contexts could include individual research into a range of current systems' network security as the basis for a group presentation and discussion on the merits and weaknesses of each network. It would be beneficial if the learners should have access to a network and its security solution in order to monitor and analyse it over a period of time so that analysis of the policies; and actual practices can be considered and recommendations made for change. Several recommendations or requirements for change such as new hardware, software or new groups could be introduced during this period requiring the learner to consider what changes should be made to the security solutions and associated documentation, and how this could be carried out. Learners will benefit from being encouraged to exercise autonomy and judgement to analyse network security and present their findings; research potential threats, design and carryout testing of a particular solution; adapt their thinking and reach considered conclusions when presented with requirements for change to the network or the discovery of new threats based on a foundation of relevant knowledge, understanding and practical skills. Learners would benefit from being presented with subject/sector-relevant problems from a variety of perspectives, and being given the opportunity to explore those using diverse approaches and schools of thought. For example, investigation of different network security solutions, either through individual research, real work or as a result of being provided with a problem by an external organisation or department.

Assessment evidence guidance
Evidence must be produced to show how a learner has met each of the Learning Outcomes. This evidence could take the form of assignments, project portfolios, presentations or, where appropriate, reflective accounts. Where group work/activities contribute to assessment evidence, the individual contribution from each learner must be clearly identified. All evidence must be available for the visiting moderator to review. Where learners are able to use real situations or observations from work placement, care should be taken to ensure that the record of observation accurately reflects the learner's performance. This should be signed, dated, and included in the evidence. It is best practice to record another individual's perspective of how a practical activity was carried out. Centres may wish to use a witness statement as a record of observation. This should be signed and dated and included in the evidence.

RESOURCES

Books

Wu, Chwan-Hwa and Irwin, J. David., *Introduction to Computer Networks and Cybersecurity* CRC Press, 2013.

Williams, Barry, L., *Information Security Policy Development for Compliance: ISO/IEC 27001, NIST SP 800-53, HIPAA Standard, PCI DSS V2.0, and AUP V5.0,* CRC Press, 2013.

Bartlett, Ryan C., *Web Application Defender's Cookbook: Battling Hackers and Protecting Users* John Wiley & Sons, 2012. ISBN-13: 978-1118362181

Kizza, J M., *Guide to Computer Network Security (Computer Communications and Networks)* (2nd Ed), Springer, 2013. ISBN-13: 978-1447145424

Singh, B., *Network Security & Management*

Brotby, K. W., *Information Security Management Metrics: A Definitive Guide to Effective Security Monitoring and Measurement,* Auerbach Publications, 2009. ISBN-13: 978-1420052855

Journals

International Journal of Network Security
International Journal of Computer Science and Network Security (IJCSNS)
ACEEE International Journal of Network Security
Journal of Cryptology
Computers & Security
IEEE Transactions on Information Forensics and Security

Websites

Network Security
www.sciencedirect.com/science/journal/13534858
www.networksecurityjournal.com/
www.sans.org/critical-security-controls/
www.networkworld.com/topics/security.html
http://thesecuritynetwork.org/