Unit title:	IT security management
Unit number:	29
Level:	5
Credit value:	15
Guided learning hours:	60
Unit reference number:	A/601/1995

UNIT AIM AND PURPOSE

This unit provides the opportunity for learners to explore the IT security risks for organisations and the approaches that are necessary to minimise such risks.

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 risks to IT security	1.1 identify and evaluate types of security risks to organisations 1.2 evaluate organisational security procedures
LO2 Understand mechanisms to control organisational IT security	2.1 discuss risk assessment procedures 2.2 evaluate data protection processes and regulations as applicable to an organisation 2.3 analyse physical security issues for an organisation
LO3 Be able to manage organisational security	3.1 design and implement a security policy for an organisation 3.2 evaluate the suitability of the tools used in an organisational policy 3.3 discuss the human resource issues that have to be considered when carrying out security audits

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 risks to IT security	
Security risks	Poorly protected passwords, weak external security on LAN, unauthorised use of a system, file permissions, hackers damage or destruction of data both internal and external to the system, physical damage/theft of assets
Security procedures	IT policy, impact of security risks, Computer Misuse Act, Data Protection Act.
LO2 Understand mechanisms to control organisational IT security	
Risk assessment	Hardware, software, loss of data, likelihood of a security breach, virus, Trojan, worm, spyware, responsible use policy
Data Protection	Legislation, e.g. Data Protection Act, Computer Misuse Act, antivirus software, firewalls, backup procedures, user access rights
Physical security issues	Passwords, biometric, mandatory, discretionary, anti-theft devices.
LO3 Be able to manage organisational security	
Policy	Policy owner, responsibilities of users, standards, logs, risks, business continuity, code of practice for IT
Tools	Logon profiles, logs, audits, training, monitor user activity
Human resource issues	Staff rights and responsibilities, security policy, discipline procedures for staff found breaching policies.

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 the use of guest speakers as well as staff within the centre who have responsibility for IT security management. Learners will benefit from being encouraged to exercise autonomy and judgement to evaluate existing policies and/or case studies, consider to what extent these are effective, and to adapt their thinking and reach considered conclusions when designing a policy for an organisation. Learners would benefit from being presented with subject/sector-relevant problems from a variety of perspectives and being given the opportunity to explore them using a variety of approaches and schools of thought. For example, in LO2, learners have to evaluate processes and regulations for an organisation; this may be through a case study or the use of a guest speaker.

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

Roebuck, Kevin., *IT Security Assessment: High-impact Strategies – What You Need to Know: Definitions, Adoptions, Impact, Benefits, Maturity, Vendors,* Emereo Pty Limited, 2011, ISBN 9781743045763

Batten, Lance., *IT Security Management 100 Success Secrets – 100 Most Asked Questions: The Missing IT Security Management Control, Plan, Implementation, Evaluation and Maintenance Guide* - Second Edition, Emereo Pty Limited, 2010, ISBN 9781742442525

Vielhauer, Claus., *Biometric User Authentication for IT Security: From Fundamentals to Handwriting – Advances in Information Security* v.18, Springer-Verlag New York Inc, 2005, ISBN 9780387261942

Saito, William Hiroyuki., *The Future of Privacy and IT Security,* John Wiley & Sons Inc, 2013. ISBN 9781118063057

Ackermann, Tobias., *IT Security Risk Management in the Context of Cloud Computing,* Springer Gabler, 2013, ISBN 9783658011147

Journals

Journal of Computer Security ISSN 0926-227X

Computers & Security ISSN 0167-4048

International Journal of Information Security ISSN: 1615-5262 (print version) ISSN: 1615-5270 (electronic version)

Websites

Understanding Recent Trends in IT Security Management : The State of Security
www.tripwire.com/state-of-security/it-security-data-protection/connecting-security-to-the-business/understanding-recent-trends-in-it-security-management/