



Unit title	Principles of Information Security Testing 2
SQA code	H7D9 04
SCQF level	8
SCQF credit points	17
SSC ref	SECKTEST2

History of changes

Publication date: July 2014

Version: 01

Version number	Date	Description	Authorised by

© Scottish Qualifications Authority 2014

This publication may be reproduced in whole or in part for educational purposes provided that no profit is derived from reproduction and that, if reproduced in part, the source is acknowledged.

Title		Principles of Information Security Testing 2	
Learning Outcomes		Assessment Criteria	
The learner will:		The learner can:	
1	Understand the role of testing in maintaining Information Security.	1.1	Evaluate the impact on organisations and individuals of failures to preserve the confidentiality, integrity and availability of information systems.
		1.2	Critically analyse the role of testing in maintaining the confidentiality, integrity and availability of information systems.
2	Understand the Information Security testing process.	2.1	Evaluate the effectiveness of standard testing techniques for testing Information Security.
		2.2	Evaluate the use of tools in Information Security testing.
		2.3	Explain how to maintain Information Security during testing.
		2.4	Analyse the role and applicability of penetration testing.
		2.5	Evaluate common penetration testing techniques.
3	Be able to plan and carry out Information Security testing.	3.1	Develop outline plans for testing the Information Security of a given system.
		3.2	Develop a detailed plan for the penetration testing of a given system.
		3.3	Carry out penetration testing of a given system according to plan.

Additional information about the Unit
Unit purpose and aim(s)
Security testing determines the level of resilience of an information system to information security threats and vulnerabilities through planning and applying testing methods, including penetration testing, for assessing the robustness of an information system, against a coordinated attack.
Details of the relationship between the Unit and relevant national occupational standards (if appropriate)
This Unit is based on the e-skills UK NOS for Information Security.
Details of the relationship between the Unit and other standards or curricula (if appropriate)
N/A
Assessment requirements specified by a sector or regulatory body (if appropriate)
This Unit may be assessed by any means which provides evidence that the candidate understands the content. Every effort should be made to relate the content to the candidate's organisation wherever possible.

Assessment (evidence) Requirements
The Unit may be assessed using any appropriate methods, or combination of methods, which clearly demonstrate the learning outcomes. Simulation is an allowed assessment method.
Guidance on Instruments of Assessment
Learners must complete real or simulated work activities in order to produce evidence to demonstrate they are occupationally competent. An e-portfolio approach is encouraged.