



<b>Unit title</b>	Principles of Information Governance and Assurance 2
<b>SQA code</b>	H7CP 04
<b>SCQF level</b>	8
<b>SCQF credit points</b>	18
<b>SSC ref</b>	SECKGA2

## History of changes

**Publication date:** July 2014

**Version:** 01

<b>Version number</b>	<b>Date</b>	<b>Description</b>	<b>Authorised by</b>

© 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.

<b>Title</b>		Principles of Information Governance and Assurance 2	
<b>Learning Outcomes</b>		<b>Assessment Criteria</b>	
<b>The learner will:</b>		<b>The learner can:</b>	
1	Understand the purpose of Information Governance.	1.1	Evaluate the importance of confidentiality, integrity and availability for information systems.
		1.2	Evaluate the role of identity in Information Security.
		1.3	Evaluate the role of cryptography in Information Security.
		1.4	Explain the Information Security procedures required by different types of organisations.
		1.5	Describe the legal requirements for Information Security for individuals and organisations.
2	Understand Information Security threats and vulnerabilities.	2.1	Evaluate the types of threats facing the Information Security of individuals and organisations.
		2.2	Explain the development of threats to the Information Security of individuals and organisations.
		2.3	Evaluate sources of threats to Information Security in terms of opportunity, ability and motive.
		2.4	Evaluate the types of Information Security vulnerabilities associated with hardware and software components.
		2.5	Describe how hardware and software vulnerabilities can be identified and resolved.
3	Understand Information Security techniques and technologies.	3.1	Evaluate common cryptographic techniques used in Information Security.
		3.2	Evaluate physical and logical access controls used to protect Information Systems.
		3.3	Design an access control system incorporating levels of access and the use of identity to protect a given information system.

<b>Learning Outcomes</b>	<b>Assessment Criteria</b>
<b>The learner will:</b>	<b>The learner can:</b>
	<p>3.4 Critically compare proactive and reactive Information Security techniques.</p> <p>3.5 Evaluate the Information Security features of hardware and network components.</p> <p>3.6 Explain how ethical hacking can contribute to Information Security testing.</p>
<p>4 Understand Information Security risk assessment and management.</p>	<p>4.1 Explain how to identify information assets which may be at risk.</p> <p>4.2 Assess the probability and impact of given risks.</p> <p>4.3 Explain available methods for preserving and restoring the integrity and availability of information assets.</p> <p>4.4 Evaluate the impact of the actions of system users on information security.</p>

<b>Additional information about the Unit</b>
<b>Unit purpose and aim(s)</b>
The determination, establishment and maintenance of appropriate governance and assurance of information systems security. This relates to information contained within information assets, and that are integrated into information systems, and also the wide range of digital process control systems. The scope is the entire domain including hardware, software, people, processes and technology.
<b>Details of the relationship between the Unit and relevant national occupational standards (if appropriate)</b>
This Unit is based on the e-skills UK NOS for Information Security.
<b>Details of the relationship between the Unit and other standards or curricula (if appropriate)</b>
N/A
<b>Assessment requirements specified by a sector or regulatory body (if appropriate)</b>
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.

**Guidance on Instruments of Assessment**

Learners must complete real work activities in order to produce evidence to demonstrate they are occupationally competent. An e-portfolio approach is encouraged.

Simulation is allowed for aspects of the Unit specified when:

- a learner is required to complete a work activity that does not occur on a regular basis and therefore opportunities to complete a particular work activity do not easily arise
- a learner is required to respond to a situation that rarely occurs, such as responding to an emergency situation
- the safety of a learner, other individuals and/or resources will be put at risk.

Simulation must replicate the workplace to such an extent that learners will be able to fully transfer their occupational competence to the workplace and real situations.