Unit title	Principles of Information Governance and Assurance 1
SQA code	H7CN 04
SCQF level	6
SCQF credit points	15
SSC ref	SECKGA1

History of changes

Publication date: July 2014

Version: 01

Version number	Date	Description	Authorised by

Title	Principles of Information Governance and Assurance 1	
Learning Outcomes **The learner will:**		**Assessment Criteria** **The learner can:**
1	Understand the purpose of Information Governance.	1.1 Explain the importance of confidentiality, integrity and availability for information systems. 1.2 Explain the role of identity in Information Security. 1.3 Explain the importance and use of cryptographic techniques in Information Security. 1.4 Describe the Information Security procedures required by different types of organisations. 1.5 Outline the legal requirements for Information Security for individuals and organisations.
2	Understand Information Security threats and vulnerabilities.	2.1 Describe 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 Describe sources of threats to Information Security in terms of opportunity, ability and motive. 2.4 Describe the types of Information Security vulnerabilities that can arise in hardware and software components. 2.5 Explain how hardware and software vulnerabilities can be identified and resolved.
3	Understand Information Security techniques and technologies.	3.1 Describe common cryptographic techniques including examples of their use in Information Security. 3.2 Explain the limitations of cryptography and their impact on Information Security.

Learning Outcomes The learner will:	Assessment Criteria The learner can:
	3.3 Explain how physical and logical access controls can be used to protect Information Systems. 3.4 Design an access control system incorporating levels of access and the use of identity to protect a given information asset. 3.5 Compare proactive and reactive Information Security techniques. 3.6 Explain the Information Security features of hardware and network components. 3.7 Compare ethical and unethical hacking. 3.8 Describe how ethical hacking can contribute to Information Security testing.
4 Understand Information Security risk assessment and management.	4.1 Describe how to identify information assets which may be at risk. 4.2 Assess the probability and impact of given risks. 4.3 Describe available methods for preserving and restoring the integrity and availability of information assets. 4.4 Explain the responsibilities of system users for information security.

Additional information about the Unit
Unit purpose and aim(s)
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.
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.
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.