Unit title	Carrying Out Information Security Audits 2
SQA code	H7D5 04
SCQF level	8
SCQF credit points	15
SSC ref	SECAUD2

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	Carrying Out Information Security Audits 2

Learning Outcomes **The learner will:**	**Assessment Criteria** **The learner can:**
1 Be able to prepare for information security audit activities.	1.1 Interpret given information security audit briefs to identify the information assets and system components to be audited. 1.2 Identify sources of information relating to the information assets and system components in scope. 1.3 Develop audit plans, following organisational procedures, which will ensure a thorough assessment of security compliance across the whole scope of the audit. 1.4 Verify audit scope and plans with relevant persons.
2 Be able to carry out information security audit activities.	2.1 Carry out information security audits following organisational procedures. 2.2 Critically review information and data relating to information assets and system components to assess security compliance. 2.3 Report any security non-compliance to the relevant persons in line with organisational procedures and timelines. 2.4 Report on audit activities following organisational procedures. 2.5 Make justified recommendations for actions to be taken to improve security compliance to relevant persons using media, format and structures which meet the needs of the intended audience.

Additional information about the Unit
Unit purpose and aim(s)
This Unit covers the competencies required for assisting with auditing information systems security robustness. This includes checking for, and verifying compliance with, security policies and standards as well as external legal and regulatory requirements. Verifying that information systems meet the security criteria, including policy, standards and procedures. Undertaking security compliance audits in accordance with an appropriate methodology.
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 must be assessed using evidence derived from real work activities.

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.