Unit title	Carrying Out Information Security Incident Management Activities 1
SQA code	H7E4 04
SCQF level	6
SCQF credit points	9
SSC ref	SECINM1

History of changes

Publication date: July 2014

Version: 01

Version number	Date	Description	Authorised by

Title	Carrying Out Information Security Incident Management Activities 1

Learning Outcomes **The learner will:**	**Assessment Criteria** **The learner can:**
1 Be able to gather information to manage Information Security incidents.	1.1 Follow organisational procedures for the detection and classification of incidents. 1.2 Identify the information assets and system components that may be impacted by detected incidents. 1.3 Verify the scope of detected incidents with relevant persons. 1.4 Obtain information and data on incidents to assess their impact on information assets and system components.
2 Be able to carry out Information Security Incident Management activities.	2.1 Identify types of actions required to resolve incidents or mitigate their impact. 2.2 Report any incidents which cannot be resolved or mitigated to the relevant persons following organisational procedures. 2.3 Make recommendations for specific actions to be taken to respond to incidents. 2.4 Report on incident management activities using standard documentation following organisational procedures. 2.5 Follow organisational procedures for the closure of incidents.

Additional information about the Unit
Unit purpose and aim(s)
The conduct of information security incident management. This includes implementing incident management processes to ensure that security incidents are handled appropriately.
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.