



Unit title	Carrying Out Information Security Incident Management Activities 2
SQA code	H7D1 04
SCQF level	8
SCQF credit points	15
SSC ref	SECINCM2

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 Incident Management Activities 2	
Learning Outcomes	Assessment Criteria	
The learner will:	The learner can:	
<p>1 Be able to prepare for Information Security Incident Management.</p>	<p>1.1 Interpret given incident management briefs to identify the scope of the incidents to be managed.</p> <p>1.2 Verify the scope of identified incidents with relevant persons.</p> <p>1.3 Evaluate sources of information relating to the impact on information assets and system components of identified incidents.</p> <p>1.4 Record information and data from identified sources following organisational procedures.</p>	
<p>2 Be able to manage Information Security Incidents.</p>	<p>2.1 Follow organisational procedures for the detection and classification of incidents.</p> <p>2.2 Critically review information and data on incidents to assess their impact on information assets and system components.</p> <p>2.3 Determine actions to resolve incidents or mitigate their impact.</p> <p>2.4 Make justified recommendations for actions to be taken to respond to incidents to relevant persons using media, format and structures which meet the needs of the intended audience.</p> <p>2.5 Report any incidents which cannot be resolved or mitigated to the relevant persons following organisational procedures and timelines.</p> <p>2.6 Report on incident management activities using standard documentation following organisational procedures.</p> <p>2.7 Follow organisational procedures for the closure of incidents.</p> <p>2.8 Critically evaluate organisational procedures for Incident Management.</p>	

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.