



<b>Unit title</b>	Carrying Out Information Security Forensic Examinations 2
<b>SQA code</b>	H7D3 04
<b>SCQF level</b>	8
<b>SCQF credit points</b>	9
<b>SSC ref</b>	SECFE4

## 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>	Carrying Out Information Security Forensic Examinations 2	
<b>Learning Outcomes</b>		<b>Assessment Criteria</b>
<b>The learner will:</b>		<b>The learner can:</b>
1	Be able to carry out Information Security forensic examinations.	<p>1.1 Carry out forensic examinations following organisational procedures.</p> <p>1.2 Analyse system information for evidence of actual or attempted breaches of security policy or legislation.</p> <p>1.3 Report any identified actual or attempted breaches of security to the relevant persons following organisational procedures and timelines.</p> <p>1.4 Use security tools to analyse the integrity of software.</p> <p>1.5 Take actions to secure information assets and system components subject to actual or attempted breaches of security in line with organisational timelines.</p> <p>1.6 With the authorisation of relevant persons, seize evidence in accordance with legislation and following organisational procedures.</p> <p>1.7 Seize evidence, minimising disruption to the organisation and maintaining evidential integrity.</p>

<b>Additional information about the Unit</b>
<b>Unit purpose and aim(s)</b>
The conduct of digital forensic examination, following processes to ensure that security incidents are investigated appropriately, in order to investigate who the perpetrators might be and collect evidence.
<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 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.