Unit title	Carrying Out Information Security Risk Assessment 2
SQA code	H7CW 04
SCQF level	8
SCQF credit points	12
SSC ref	SECRA2

History of changes

Publication date: July 2014

Version: 01

Version number	Date	Description	Authorised by

Title	Carrying Out Information Security Risk Assessments 2

Learning Outcomes **The learner will:**	**Assessment Criteria** **The learner can:**
1 Be able to prepare for Information Security Risk Assessments.	1.1 Interpret given risk assessment briefs to identify the information assets and system components to be assessed. 1.2 Verify the scope of identified information assets and system components with relevant persons. 1.3 Evaluate sources of information relating to potential risks that may impact on the security of identified information assets and system components.
2 Be able to carry out Information Security Risk Assessments.	2.1 Use a range of investigative methods to gather information relating to potential risks that may impact on the security of identified information assets and system components. 2.2 Record all gathered information in line with organisational requirements. 2.3 Analyse gathered information to identify risks to the security of identified information assets and system components. 2.4 Assess identified risks to determine their probability of occurrence and potential impact. 2.5 Evaluate risks against organisational risk tolerance levels. 2.6 Report any risks which exceed organisational risk tolerance levels to the relevant persons following organisational procedures and timelines. 2.7 Formulate actions to mitigate risks. 2.8 Report the results of risk assessment in line with organisational procedures. 2.9 Communicate the results and implications of risk assessments to relevant persons using media, format and structures which meet the needs of the intended audience.

Learning Outcomes The learner will:	Assessment Criteria The learner can:
	2.10 Evaluate organisational procedures for Risk Assessment.

Additional information about the Unit
Unit purpose and aim(s)
Conducting risk assessments on information assets, information systems and digital process control systems. It includes following the processes for assessing, communicating and responding to risks to security.
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.