Unit Title:	**Security of ICT Systems**
OCR unit number	201
Level:	4
Credit value:	15
Guided learning hours:	90
Unit reference number:	H/500/7221

Candidates undertaking this unit must complete real work activities in a work environment. Simulation is only allowed in exceptional circumstances (please refer to the centre handbook for further details).

Unit purpose and aim

To develop the knowledge, understanding and skills needed to implement and maintain IT security systems.

Learning Outcomes	Assessment Criteria	Knowledge, understanding and skills
The Learner will: 1 Understand the security threats to an IT system, their operational impact and the methods available to combat them	**The Learner can:** 1.1 Describe the data protection methods that are relevant to the organisation 1.2 Describe physical security methods in use 1.3 Describe organisational security procedures 1.4 Describe types of possible security breaches and their operational impacts	Candidates must have a detailed understanding of a wide range of security threats and their operation impact to include the following: • weak external security on LAN • unauthorised use of a system without damage to data • poorly protected passwords • unauthorised removal or copying of data or code from a system • damage to or destruction of data or code inside or outside the system • hardware and media loss or theft • unauthorised access through internet connections • risks from disasters or other unforeseen events • file permissions • hackers, both external and internal inside and out Candidates must have a detailed understanding of methods for protecting data and providing physical security to ICT systems. Candidates must have a detailed understanding of organisational security procedures that should be implemented to secure ICT systems and data.

Learning Outcomes	Assessment Criteria	Knowledge, understanding and skills
2 Maintain and improve ICT security procedures	2.1 Review and update security procedures 2.2 Ensure compliance with security procedures by scheduling security audits 2.3 Initiate suitable actions to deal with identified breaches of security 2.4 Inform colleagues of their security responsibilities and confirm their understanding at suitable intervals	Candidates must be able to carry out security audits to include • a critical review of results • identification of action requirements • Informing colleagues of changes and responsibilities
3 Implement security procedures	3.1 Schedule and carry out security risk assessments 3.2 Select appropriate security tools for the organisation or department to use	Candidates must be able to • carry out security risk assessments • select appropriate security measures

Assessment

Candidates undertaking this unit must complete real work activities in order to produce evidence to demonstrate they are occupationally competent. Real work is where the candidate is engaged in activities that contribute to the aims of the organisation by whom they are employed, for example in paid employment or working in a voluntary capacity.

Simulation is only allowed for aspects of units when a candidate 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. When simulation is used, assessors must be confident that the simulation replicates the workplace to such an extent that candidates will be able to fully transfer their occupational competence to the workplace and real situations.

Internal quality assurance personnel must agree the use of simulated activities before they take place and must sample all evidence produced through simulated activities.

It is the assessor’s role to satisfy themselves that evidence is available for all performance, knowledge and evidence requirements before they can decide that a candidate has finished a unit. Where performance and knowledge requirements allow evidence to be generated by other methods, for example by questioning the candidate, assessors must be satisfied that the candidate will be competent under these conditions or in these types of situations in the workplace in the future. Evidence of questions must include a written account of the question and the candidate’s response. Observations and/or witness testimonies must be detailed and put the evidence into context ie the purpose of the work etc.

All of the assessment criteria in the unit must be achieved and clearly evidenced in the submitted work, which is externally assessed by OCR.

Evidence for the knowledge must be explicitly presented and not implied through other forms of evidence.

Evidence requirements

All aspects of the assessment criteria must be covered and evidence must be available that shows where and how the assessment criteria have been achieved.

Assessment Criterion 1

Candidates should provide a detailed report including

- protection methods that are relevant to the organisation
- physical security methods in use
- organisational security procedures
- security breaches and their operational impacts

Assessment Criterion 2

Candidates should provide evidence of

- reviewing and updating security procedures
- compliance with security procedures through scheduled security audits
- actions dealing with identified breaches of security
- informing colleagues of their security responsibilities and confirmation of their understanding

Assessment Criterion 3

Candidates should provide evidence of

- carrying out security risk assessments
- selecting appropriate security measures

This may include copies of risk assessments, correspondence to colleagues etc.

Candidates are encouraged to choose activities which will allow them to cover all or a majority of the criteria at one time. It is not necessary to use different activities for each element of the criterion.

Guidance on assessment and evidence requirements

Evidence can reflect how the candidate carried out the process or it can be the product of a candidate's work or a product relating to the candidate's competence.

For example: The process that the candidate carries out could be recorded in a detailed personal statement or witness testimony. It is the assessor's responsibility to make sure that the evidence a candidate submits for assessment meets the requirements of the unit.

Questioning the candidate is normally an ongoing part of the assessment process, and is necessary to:

- test a candidate's knowledge of facts and procedures
- check if a candidate understands principles and theories *and*
- collect information on the type and purpose of the processes a candidate has gone through.
- candidate responses must be recorded

It is difficult to give a detailed answer to how much evidence is required as it depends on the type of evidence collected and the judgement of assessors. The main principles, however, are as follows: for a candidate to be judged competent in a unit, the evidence presented must satisfy:

- all the items listed, in the section ‘Learning Outcomes’
- all the areas in the section ‘Assessment Criteria’

The quality and breadth of evidence provided should determine whether an assessor is confident that a candidate is competent or not. Assessors must be convinced that candidates working on their own can work independently to the required standard.

You should refer to the ‘*Admin Guide: Vocational Qualifications* (A850)’ for *Notes on Preventing Computer-Assisted Malpractice*.

Additional information

For further information regarding administration for this qualification, please refer to the OCR document ‘*Admin Guide: Vocational Qualifications’ (A850)* on the OCR website www.ocr.org.uk .