Unit Title:	**Security of ICT Systems**
OCR unit number	38
Level:	3
Credit value:	12
Guided learning hours:	100
Unit reference number:	D/500/7220

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 knowledge, understanding and skills to ensure the security of an ICT system and its data using security tools and assisting in the security auditing process.

Learning Outcomes	Assessment Criteria	Knowledge, understanding and skills
The Learner will: 1 Know the common types of security threat to an organisation, its IT system and its data, with relevant methods and procedures for protecting it	**The Learner can:** 1.1 Describe the common types of security breach that can affect the organisation, such as: • unauthorised use of a system without damage to data; • unauthorised removal or copying of data or code from a system • damage to or destruction of physical system assets and environment • damage to or destruction of data or code inside or outside the system • preventing normal use of a system (eg denial of service attack) 1.2 Describe specified data protection methods: • system data security facilities • surveillance and monitoring methods • effects of system	Candidates must have a good understanding of security threats associated with 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 an

Learning Outcomes	Assessment Criteria	Knowledge, understanding and skills
	configuration on data protection 1.3 Describe specified methods of providing physical security for ICT systems: • access control devices (e.g. locks, biometric controls, CCTV) and their configuration • limiting visibility of data (e.g. by positioning of monitors, using encryption) • shielding (e.g. cable screening, Faraday cages) • types and appropriate uses of access records and authorisations • how to allocate access authority 1.4 Describe relevant organisational security procedures	understanding of methods for protecting data and providing physical security to ICT systems. Candidates must have an understanding of organisational security procedures that should be implemented to secure ICT systems and data.
2 Apply security measures	2.1 Configure and apply specified security tools to identify and prevent breaches of security, such as: • internal system tools (e.g. passwords and permissions, malware scanning, firewall, VPN, authentication and encryption facilities) • external tools (e.g. access control devices)	Candidates must know how to select and use a range of security tools to identify and prevent breaches of security.
3 Monitor security procedures	3.1 Assist in ensuring compliance with organisational security procedures, including: • participating in security audits • gathering and recording information on security • initiating suitable actions to deal with identified breaches of security	Candidates must know how to apply security measures to an ICT system including: • implementing password policy including locking down user accounts; securing administrator's permissions; restricting access to critical services; installing or updating system security software • security tools to prevent breaches of security • assisting in ensuring

Learning Outcomes	Assessment Criteria	Knowledge, understanding and skills
		compliance with organisational security procedures eg participating in security audits, penetration testing, monitoring security procedures, gathering and recording information on security, initiating suitable actions to deal with identified breaches of security

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 objectives have been achieved.

Assessment Criterion 1

Candidates should provide detailed examples of the types of security weaknesses associated with wired and wireless systems and how they can be prevented.

Candidates must describe a range of data protection methods and how they are applied.

Candidates must describe a range of methods used to physically secure ICT systems and how they are implemented.

Candidates must describe the relevant security procedures used by an organisation.

Assessment Criterion 2

Candidates must provide evidence of configuring and applying at least 3 different security tools.

Assessment Criterion 3

Candidates must identify, install and configure security tools to prevent breaches in system security eg:

- Malware scanning
- VPN
- Authentication facilities eg smart card
- External tools eg access control devices

Candidates must provide evidence of assisting with compliance verification of organisational security procedures eg:

- Security audits
- Penetration testing
- Monitoring security procedures
- Gathering and recording information on security
- Initiating suitable actions to deal with identified breaches of security

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.

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 .