OCR
Oxford Cambridge and RSA

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

Evidence for this unit can only be achieved through actual work in a work environment. Simulation is not permissible for any competence based unit.

Unit aim

To develop knowledge, understanding and skills to ensure the security of an IT 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)	• 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

Learning Outcomes	Assessment Criteria	Knowledge, understanding and skills
	1.2 Describe specified data protection methods: • system data security facilities • surveillance and monitoring methods • effects of system 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	• methods for protecting data and providing physical security to ICT systems • 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)	• how to select and use a range of security tools to identify and prevent breaches of security

Learning Outcomes	Assessment Criteria	Knowledge, understanding and skills
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	• how to apply security measures to an IT 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 compliance with organisational security procedures egg 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

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.

In addition to the recognition of other qualifications, candidates may claim accreditation of prior achievement for any of the elements assessment criteria or complete units of competence, as long as the evidence fully meets the criteria and the candidate can prove that it is all their own work. It is important also that assessors are convinced that the competence claimed is still current. If the assessors have some doubts, they should take steps to assess the candidate's competence directly. An initial assessment of candidates is recommended.

All the learning outcomes and assessment criteria must be clearly evidenced in the submitted work, which is externally moderated by OCR.

Results will be Pass or Fail.

Guidance on assessment

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' on the OCR website www.ocr.org.uk .