



Australian Government

Department of Education, Employment and Workplace Relations

ICASAS418A Monitor and administer security of an IT system

Release: 1

ICASAS418A Monitor and administer security of an IT system

Modification History

Release	Comments
Release 1	This Unit first released with <i>ICA11 Information and Communications Technology Training Package version 1.0</i>

Unit Descriptor

This unit describes the performance outcomes, skills and knowledge required to monitor and administer security functions of an IT system.

Application of the Unit

This unit applies to experienced technical support personnel, such as help-desk supervisors, IT support technicians, and user support specialists responsible for maintaining the security of a system.

Licensing/Regulatory Information

No licensing, legislative, regulatory or certification requirements apply to this unit at the time of endorsement but users should confirm requirements with the relevant federal, state or territory authority.

Pre-Requisites

Not applicable.

Employability Skills Information

This unit contains employability skills.

Elements and Performance Criteria Pre-Content

Element	Performance Criteria
<i>Elements describe the essential outcomes of a unit of competency.</i>	<i>Performance criteria describe the performance needed to demonstrate achievement of the element. Where bold italicised text is used, further information is detailed in the required skills and knowledge section and the range statement. Assessment of performance is to be consistent with the evidence guide.</i>

Elements and Performance Criteria

1. Ensure user accounts are controlled	1.1 Modify default user settings to ensure that they conform to security policy 1.2 Modify previously created user settings to ensure they conform to updated security policy 1.3 Ensure legal notices displayed at logon are appropriate 1.4 Check strength of passwords using the appropriate utilities and consider tightening rules for password complexity 1.5 Take action to ensure password procedures are reviewed with appropriate other internal departments 1.6 Monitor email to uncover breaches in compliance with legislation 1.7 Access information services to identify security gaps and take appropriate action using hardware and software or patches
2. Secure file and resource access	2.1 Review inbuilt security and access features of the operating system and consider need for further action 2.2 Develop or review the file security categorisation scheme, and develop an understanding of the role of users in setting security 2.3 Monitor and record security threats to the system 2.4 Implement a virus checking process and schedule for the server, computer and other system components 2.5 Investigate and implement inbuilt or additional encryption facilities
3. Monitor threats to the network	3.1 Use third-party software or utilities to evaluate and report on system security 3.2 Review logs and audit reports to identify security threats 3.3 Carry out spot checks and other security strategies to ensure that procedures are being followed 3.4 Prepare and present an audit report and recommendations to appropriate person 3.5 Obtain approval for recommended changes to be made

Required Skills and Knowledge

This section describes the skills and knowledge required for this unit.

Required skills

- communication skills to:
 - liaise with technical team members
 - present information
 - provide assistance with organisational guidelines
 - review logs and audit reports to identify security threats
- problem-solving skills to:
 - identify security threats
 - use third-party software or utilities to evaluate system security
- project planning skills to:
 - identify scope
 - implement a virus checking process and schedule
 - set benchmarks
- report writing skills to:
 - present audit reports and recommendations
 - report on system security
- research skills to identify, analyse and evaluate broad features of a particular business domain and best practice in system security methodologies and technologies
- technical skills to:
 - check strength of passwords
 - implement virus checking processes and schedules
 - modify user settings
 - monitor and record security threats to the system.

Required knowledge

- current industry-accepted hardware and software products
- privacy issues and legislation with regard to IT security
- key components of risk analysis process for system security
- specific security technology
- systems technologies
- client business domain, including client organisation structure and business functionality.

Evidence Guide

The evidence guide provides advice on assessment and must be read in conjunction with the performance criteria, required skills and knowledge, range statement and the Assessment Guidelines for the Training Package.

Overview of assessment	
Critical aspects for assessment and evidence required to demonstrate competency in this unit	Evidence of the ability to: • monitor and administer security functions on the system, which may include use of third-party diagnostic tools • confirm knowledge of security features available in the operating environment.
Context of and specific resources for assessment	Assessment must ensure access to: • security policy • industry and organisational standards • live system • appropriate learning and assessment support when required • modified equipment for people with special needs.
Method of assessment	A range of assessment methods should be used to assess practical skills and knowledge. The following examples are appropriate for this unit: • direct observation: • ensuring security policy compliance • using security strategies to evaluate and report on system security and threats • review of: • audit report and recommendations prepared • virus checking process and schedule implemented • verbal or written questioning to assess candidate's knowledge of security features within the operating environment.
Guidance information for assessment	Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended, where appropriate. Assessment processes and techniques must be culturally appropriate, and suitable to the communication skill level, language, literacy and numeracy capacity of the candidate and the work being performed. Indigenous people and other people from a non-English speaking background may need additional support. In cases where practical assessment is used it should be combined with targeted questioning to assess required knowledge.

Range Statement

The range statement relates to the unit of competency as a whole. It allows for different work environments and situations that may affect performance. Bold italicised wording, if used in the performance criteria, is detailed below. Essential operating conditions that may be present with training and assessment (depending on the work situation, needs of the candidate, accessibility of the item, and local industry and regional contexts) may also be included.

User may include:	• department within the organisation • person within a department • third party.
Security policy may relate to:	• audits and alerts • file access levels • privacy • security objectives of the organisation • standards: • archival • backup • network • theft • viruses.
Legislation may include:	• copyright • liability statements • privacy legislation.
Hardware may include:	• modems or other connectivity devices • networks • personal computers • remote sites • servers • workstations.
Software may include:	• application: • spreadsheet • database • word-processing • internet browser • commercial • customised • in-house • programming: • assembler • compiler

	• development tools • system: • computer security software • device drivers • operating system.
Operating system may include:	• Linux • GNU and Linux • Mac OS X • Microsoft Windows • Unix-like operating systems: • HP-UX • IBM AIX • Silicon Graphics IRIX • Sun Solaris.
Security threats may include:	• by-pass • denial of service • eavesdropping • hacking • impersonation • manipulation • penetration • viruses.
Server may include:	• application or web servers • BEA Weblogic servers • email servers • file and print servers • firewall servers • FTP servers • IBM VisualAge and WebSphere • Novell Directory Services (NDS) servers • proxy or cache servers • voice servers.
Computer may include:	• laptops • other devices: • hand-held and mobile devices • personal digital assistant (PDA) • servers • workstations.
Encryption may include:	• asymmetric public-key ciphers • Deslogin

	• digital signatures • public key infrastructure (PKI) • PKZIP • pretty good privacy (PGP) • RSA public key • secure socket layer (SSL) • sniffers • SSH • symmetric ciphers.
Security strategies may include:	• authentication • authorisation and integrity • privacy • security objectives of the organisation.
Appropriate person may include:	• authorised business representative • client • project manager • security consultant • supervisor.

Unit Sector(s)

Systems administration and support