Australian Government

Department of Education, Employment and Workplace Relations

ICAS4119B Monitor and administer system security

Release: 1

ICAS4119B Monitor and administer system security

Modification History

Not Applicable

Unit Descriptor

Unit descriptor	This unit defines the competency required to monitor and administer security functions of a system. The following units are linked and form an appropriate cluster: • ICAS4124B Monitor and administer network security • ICAT4194B Ensure basic website security • ICAT4195B Ensure dynamic website security No licensing, legislative, regulatory or certification requirements apply to this unit at the time of publication.

Application of the Unit

Application of the unit	

Licensing/Regulatory Information

Refer to Unit Descriptor

Pre-Requisites

Prerequisite units		
	ICAI3020B	Install and optimise operating system software
	ICAS3024B	Provide basic system administration

Employability Skills Information

Employability skills	This unit contains employability skills.

Elements and Performance Criteria Pre-Content

Elements describe the essential outcomes of a unit of competency.	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.

Elements and Performance Criteria

ELEMENT	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. Use the appropriate utilities to check strength of passwords 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

REQUIRED SKILLS AND KNOWLEDGE

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

Required skills

- Problem solving skills for a defined range of unpredictable problems
- Plain English literacy and communication skills in relation to analysis, evaluation and presentation of information
- Research skills for identifying, analysing and evaluating broad features of a particular business domain and best practice in system security methodologies and technologies
- Report writing skills for business requiring depth in some areas, analysis and evaluation of information in a defined range of areas
- Questioning and active listening skills
- Project planning skills in relation to set benchmarks and identified scope

Required knowledge

- Current industry-accepted hardware and software products, with broad knowledge of general features and capabilities
- Broad knowledge of the client business domain, business function and organisation
- Systems technologies, with broad knowledge of general features and capabilities and substantial depth in some areas
- Risk analysis, with broad knowledge of general features
- Broad knowledge of specific security technology
- Broad knowledge of privacy issues and legislation

Evidence Guide

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 following is essential: • Assessment must confirm knowledge of security features available in the operating environment. • Assessment must confirm the ability to monitor and administer security functions on the system. This may include use of third-party diagnostic tools. To demonstrate competency in this unit the learner will require access to: • Security policy • Standards • Live system
Context of and specific resources for assessment	The breadth, depth and complexity of knowledge and skills in this competency would cover a broad range of varied activities or application in a wider variety of contexts most of which are complex and non-routine. Leadership and guidance would be involved when organising activities of self and others as well as contributing to technical solutions of a non-routine or contingency nature. Assessment must ensure: • Performance of a broad range of skilled applications including the requirement to evaluate and analyse current practices, develop new criteria and procedures for performing current practices and provision of some leadership and guidance to others in the application and planning of the skills would be characteristic. • Applications may involve responsibility for, and limited organisation of, others.

EVIDENCE GUIDE	
Method of assessment	The purpose of this unit is to define the standard of performance to be achieved in the workplace. In undertaking training and assessment activities related to this unit, consideration should be given to the implementation of appropriate diversity and accessibility practices in order to accommodate people who may have special needs. Additional guidance on these and related matters is provided in ICA05 Section 1. • Competency in this unit should be assessed using summative assessment to ensure consistency of performance in a range of contexts. This unit can be assessed either in the workplace or in a simulated environment. However, simulated activities must closely reflect the workplace to enable full demonstration of competency. • Assessment will usually include observation of real or simulated work processes and procedures and/or performance in a project context as well as questioning on underpinning knowledge and skills. The questioning of team members, supervisors, subordinates, peers and clients where appropriate may provide valuable input to the assessment process. The interdependence of units for assessment purposes may vary with the particular project or scenario.
Guidance information for assessment	Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended, for example: • ICAS4124B Monitor and administer network security • ICAT4194B Ensure basic website security • ICAT4195B Ensure dynamic website security An individual demonstrating this competency would be able to: • Demonstrate understanding of a broad knowledge base incorporating some theoretical concepts • Apply solutions to a defined range of unpredictable problems

EVIDENCE GUIDE	
	• Identify and apply skill and knowledge areas to a wide variety of contexts, with depth in some areas • Identify, analyse and evaluate information from a variety of sources • Take responsibility for own outputs in relation to specified quality standards • Take limited responsibility for the quantity and quality of the output of others • Maintain knowledge of industry products and services

Range Statement

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:	• a person within a department • a department within the organisation • a third party
Security policy may be in relation to:	• theft • viruses • standards (including archival, back-up, network) • privacy • audits and alerts, usually relates directly to the security objectives of the organisation
Legislation may include:	• privacy legislation • copyright • liability statements
Hardware may include but is not limited to:	• workstations • personal computers • modems or other connectivity devices • networks • DSL modems

RANGE STATEMENT	
	• remote sites • servers
Software may include but is not limited to:	• commercial, in-house, packaged or customised software
Appropriate person may include:	• supervisor • teacher • authorised business representative • client
Operating system may include but is not limited to:	• Linux 6.0 or above • Windows 98 or above • Apple OS 8 or above
Server may include:	• Application/web servers • BEA Weblogic servers • IBM VisualAge and WebSphere • Novell NDS servers • Email servers • File and print servers • FTP servers • Firewall servers • Proxy/cache servers
System may include but is not limited to:	• hardware and software components that run a computer
Computer may include:	• laptops • workstations • servers • other devices
Encryption may include:	• features or protocols such as RSA public key • PGP (pretty good privacy) • symmetric ciphers • asymmetric public-key ciphers • sniffers • PKI • SSH • Deslogin • PKZIP • secure socket layer (SSL) • digital signatures
Security threats may include:	• eavesdropping

RANGE STATEMENT	
	• manipulation • impersonation • penetration • denial of service • by-pass • hacking • viruses
Security strategies may include:	• privacy • authentication • authorisation and integrity • usually relates directly to the security objectives of the organisation

Unit Sector(s)

Unit sector	Support

Co-requisite units

Co-requisite units		

Competency field

Competency field	