Australian Government

Department of Education, Employment and Workplace Relations

# ICAS4124B Monitor and administer network security

Release: 1

ISC INDUSTRY SKILLS COUNCILS

Creating Australia's Future

# ICAS4124B Monitor and administer network security

## Modification History

Not Applicable

## Unit Descriptor

| | |
|---|---|
| **Unit descriptor** | This unit defines the competency required to monitor and administer security functions on a network and wireless access according to organisational policies.<br>The following units are linked and form an appropriate cluster:<br>• ICAD4043B Develop and present a feasibility report<br>• ICAS4119B Monitor and administer systems security<br>• ICAS5202B Ensure privacy for users<br>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** | | |
| | ICAS3032B | Provide network systems administration |

| **Prerequisite units** | | |
|---|---|---|
| | | |

## 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. Review organisation's ***network*** and ***security policy*** to ensure up-to-date knowledge and understanding of policies<br>1.2. Modify default and previously created user settings to ensure that they conform with organisational ***security policy***<br>1.3. Investigate log-on procedures for security and appropriateness and modify log-on ***requirements***, using relevant utilities, where applicable<br>1.4. Review and monitor user wireless access of mobile equipment to the network where applicable<br>1.5. Ensure that appropriate procedures are put in place to deal with user accounts that are no longer required<br>1.6. Access information resources to identify and understand current, documented security gaps and their associated repair procedure<br>1.7. Ascertain the security repairs applicable to the current ***network*** and discuss with ***appropriate person*** to gain approval for repair implementation<br>1.8. Obtain and implement the appropriate ***hardware*** and ***software*** necessary for ***network*** security repair |
| 2. Secure file and resource access | 2.1. Review inbuilt security and access features of the ***operating system*** and document areas for concern<br>2.2. Analyse the file security categorisation scheme and the role of users in setting file security, in relation to organisational ***security policy*** and recommend revision, if necessary<br>2.3. Implement, if necessary, a process for ongoing updates of virus checking ***software***, at ***server*** and workstation levels<br>2.4. Investigate and implement inbuilt or additional ***encryption*** facilities, as appropriate, to meet organisational security needs |
| 3. Monitor threats to the system | 3.1. Investigate the current security of the ***network***, including physical aspects, utilising appropriate third-party testing ***software*** where applicable<br>3.2. Review logs and audit reports to identify and record ***security threats***, intrusions or attempts<br>3.3. Carry out spot checks and other activities to ensure that procedures are not being bypassed<br>3.4. Evaluate the findings of the state of security and |

| ELEMENT | PERFORMANCE CRITERIA |
|---|---|
| | prepare recommendations for improvement<br>3.5. Prepare ***documentation*** in a report for presentation to ***appropriate person*** to gain approval for changes to be made |

## Required Skills and Knowledge

| **REQUIRED SKILLS AND KNOWLEDGE**<br>This section describes the skills and knowledge required for this unit. |
|---|
| **Required skills** |
| • Problem solving skills related to intrusion detection<br>• Analysis and systems evaluation<br>• Research skills for identifying and analysing network security methodologies and technologies<br>• Report writing skills for evaluating system security status in line with organisational security polices<br>• Questioning and active listening skills<br>• Hardware and software installation skills related to improving network security |
| **Required knowledge** |
| • Current industry-accepted hardware and software security products, with broad knowledge of general features and capabilities<br>• Broad knowledge of the client business domain, business function and organisation<br>• Broad knowledge of features and capabilities of networking technologies, with substantial depth in security areas<br>• Broad knowledge of risk analysis<br>• Broad knowledge of privacy issues and privacy legislation<br>• General knowledge of security information sources |

# 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:<br>• Assessment must confirm an understanding of the organisation's network security and access policies.<br>• Assessment must confirm knowledge of the security features available in the operating environment and the ability to monitor and administer security functions on the network. This may include use of third-party diagnostic tools.<br>To demonstrate competency in this unit the following resources will be needed:<br>• A live network with security restrictions<br>• Security and access policies<br>• Security information resources<br>• Hardware and software that will improve security |
| **Context of and specific resources for assessment** | Security planning and monitoring aids in preventing intrusion into a network. With computers containing and manipulating significant data about our finances, purchasing habits and other private information, monitoring and administering network security is an ongoing challenge for organisations which collect and use such information.<br>This unit provides a starting point for monitoring and administering network security. Activities undertaken in this unit should be done in a closed-off LAN/WAN/WLAN and the skills developed not used on live open networks.<br>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 |

| EVIDENCE GUIDE | |
|---|---|
| | organising activities of self and others as well as contributing to technical solutions of a non-routine or contingency nature.<br>Assessment must ensure:<br>• 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.<br>• Applications may involve responsibility for, and limited organisation of, others. |
| **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.<br>• Competency in this unit should to 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.<br>• Due to the inherent risks involved in activities such as dealing with the security of potentially sensitive information, it is strongly recommend that work and assessment be carried out on a system separate from the organisation's main field of network activity or in a simulated environment. Where a workplace context is used, specific control for security must be adhered to in all circumstances. |

| EVIDENCE GUIDE | |
|---|---|
| | • 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. |
| **Guidance information for assessment** | The interdependence of units for assessment purposes may vary with the particular project or scenario. Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended, for example:<br>• ICAD4043B Develop and present a feasibility report<br>• ICAS4119B Monitor and administer systems security<br>• ICAS5202B Ensure privacy for users<br>An individual demonstrating this competency would be able to:<br>• Use detection tools to detect intrusion<br>• Monitor and administer activities of users<br>• Apply emergency solutions to a variety security problems<br>• Interpret available information and request clarification where needed<br>Additionally, an individual demonstrating this competency would be able to:<br>• Demonstrate understanding of a broad knowledge base incorporating some theoretical concepts<br>• Apply solutions to a defined range of unpredictable problems<br>• Identify and apply skill and knowledge areas to a wide variety of contexts, with depth in some areas<br>• Identify, analyse and evaluate information from a variety of sources<br>• Take responsibility for own outputs in relation to specified quality standards<br>• Take limited responsibility for the quantity and quality of the output of others<br>• Maintain knowledge of industry products and |

| EVIDENCE GUIDE | |
|---|---|
| | 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. | |
| ***Network*** may include: | • large and small LANs<br>• WLANs<br>• VPNs<br>• Intranets<br>• the internet |
| ***Security policy*** may be in relation to: | • theft<br>• viruses<br>• standards (including archival, back-up, network)<br>• privacy<br>• audits and alerts<br>• usually relates directly to the security objectives of the organisation and file access levels |
| ***Appropriate person*** may include: | • supervisor<br>• teacher<br>• authorised business representative<br>• client |
| ***Hardware*** may include but is not limited to: | • mobile equipment<br>• workstations<br>• personal computers<br>• modems or other connectivity devices<br>• networks<br>• DSL modems<br>• remote sites<br>• servers |

| RANGE STATEMENT | |
|---|---|
| ***Software*** may include but is not limited to: | • commercial, in-house, packaged or customised software |
| ***Operating system*** may include but is not limited to: | • Linux 6.0 or above<br>• Windows 98 or above<br>• Apple OS 8 or above |
| ***Documentation*** may follow: | • ISO/IEC/AS standards<br>• audit trails<br>• naming standards<br>• version control<br>• project management templates<br>• report writing principles |
| ***Server*** may include: | • Application/web servers<br>• BEA Weblogic servers<br>• IBM VisualAge and WebSphere<br>• Novell NDS servers<br>• Email servers<br>• Voice servers<br>• File and print servers<br>• FTP servers<br>• Firewall servers<br>• Proxy/cache servers |
| ***Requirements*** may be in reference to: | • business<br>• system<br>• application<br>• network<br>• people in the organisation |
| ***Security threats*** may include: | • eavesdropping<br>• manipulation<br>• impersonation<br>• penetration<br>• denial of service<br>• by-pass<br>• hacking<br>• viruses<br>• spoofing<br>• associations |
| ***Encryption*** may include features or protocols such as: | • RSA public key<br>• PGP (pretty good privacy)<br>• connection orientation |

| RANGE STATEMENT | |
|---|---|
| | • WEP<br>• WPA<br>• AAA<br>• symmetric ciphers<br>• asymmetric public-key ciphers<br>• sniffers<br>• PKI<br>• SSH<br>• Deslogin<br>• PKZIP<br>• secure socket layer (SSL)<br>• digital signatures |

## Unit Sector(s)

| | |
|---|---|
| **Unit sector** | Support |

## Co-requisite units

| | | |
|---|---|---|
| **Co-requisite units** | | |
| | | |
| | | |

## Competency field

| | |
|---|---|
| **Competency field** | |