



Australian Government

Department of Education, Employment and Workplace Relations

ICAI5098C Install and manage complex networks

Release: 1

ICAI5098C Install and manage complex networks

Modification History

Not Applicable

Unit Descriptor

Unit descriptor	<p>This unit defines the competency required to install and manage networks consisting of multiple components and connectivity options.</p> <p>The following units are linked and form an appropriate cluster:</p> <ul style="list-style-type: none"> • ICAS5122C Identify and resolve network problems • ICAS5123C Manage network security
------------------------	---

Application of the Unit

Application of the unit	
--------------------------------	--

Licensing/Regulatory Information

Not Applicable

Pre-Requisites

Prerequisite units			
	<table border="1"> <tr> <td>ICAI4097C</td> <td>Install and configure a network</td> </tr> </table>	ICAI4097C	Install and configure a network
ICAI4097C	Install and configure a network		

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. Implement multiple servers	<p>1.1. Review <i>client</i> and <i>organisational requirements</i> in order to assess the benefits of employing multiple servers to provide required services</p> <p>1.2. Design <i>network topology</i> that makes use of multiple servers, acting individually or in concert, to meet <i>organisational requirements</i></p> <p>1.3. Develop plans, with prioritised tasks and contingency arrangements, for the implementation of the <i>network</i> design, with minimum disruption to <i>client</i></p> <p>1.4. Liaise with relevant personnel to obtain approval for the plans, and revise plans if necessary</p> <p>1.5. Notify the <i>user</i> of the expected impact of the planned changes</p> <p>1.6. According to plan, implement and configure the multiple <i>servers</i> in accordance with vendor and organisation-specifications</p> <p>1.7. Test network configuration and performance to ensure the expected services are provided to the <i>user</i> and appropriate <i>security</i> is maintained</p>
2. Install and configure devices to extend network reach	<p>2.1. Review <i>user</i> and <i>organisational requirements</i> in order to assess the need for <i>network</i> communication devices and remote access services</p> <p>2.2. Plan, install and configure <i>network</i> communication devices to provide <i>network</i> services to meet user requirements, in accordance with vendor and organisation-specifications</p> <p>2.3. Check and install <i>cabling</i> and associated components in accordance with industry <i>standards</i></p> <p>2.4. Plan, install and configure remote access services to meet <i>user</i> requirements, in accordance with vendor and organisation-specifications</p>
3. Manage different levels of security	<p>3.1. Gather data about <i>user network</i> access needs for work requirements and organisational approval for user access</p> <p>3.2. Evaluate <i>user</i> access data to determine and implement <i>user</i> access levels for network resources</p> <p>3.3. Investigate the need for <i>firewalls</i>, as per <i>security</i> requirements</p> <p>3.4. Plan and implement the required <i>firewalls</i></p> <p>3.5. Undertake ongoing monitoring of the viability and</p>

ELEMENT	PERFORMANCE CRITERIA
	<p>reliability of the <i>network security</i>, through testing and the use of technical <i>tools</i></p> <p>3.6. Continually monitor internal and external <i>network</i> access for security breaches</p> <p>3.7. Develop and maintain appropriate <i>documentation</i> on the security policy for technicians and the user</p>
<p>4. Connect to a host computer</p>	<p>4.1. Review <i>user</i> and <i>organisational requirements</i> for host connection</p> <p>4.2. Evaluate current system <i>hardware</i>, cabling, <i>components</i> and <i>software</i> in terms of requirements necessary to enable host connection to meet <i>user</i> needs</p> <p>4.3. Obtain, install and configure the <i>hardware</i>, cabling and <i>software</i> required to update the system to provide host connectivity</p> <p>4.4. Test the updated system and the host connectivity options, and reconfigure if necessary</p>
<p>5. Integrate and manage network resources with network utilities</p>	<p>5.1. Identify and evaluate appropriate network management tools to assist in the administration of the complex network</p> <p>5.2. Select and install <i>network</i> management tools in accordance with industry and organisational standards</p> <p>5.3. Test <i>tools</i> to ensure they are operational</p> <p>5.4. Gather and analyse <i>user</i> feedback about using the changed system</p> <p>5.5. Prepare and deliver relevant training in a manner appropriate to the audience</p> <p>5.6. Develop and maintain procedures to ensure regular <i>network</i> reporting and administration in accordance with organisational policies and procedures</p> <p>5.7. Complete <i>documentation</i> of complex <i>network</i>, in line with <i>organisational requirements</i></p>

Required Skills and Knowledge

REQUIRED SKILLS AND KNOWLEDGE

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

REQUIRED SKILLS AND KNOWLEDGE**Required skills**

- Plain English literacy and communication skills in relation to dealing with clients and team members (e.g. when asset/inventory recording documentation is completed in line with organisational requirements)
- Report writing skills for business requiring depth in some areas, analysis and evaluation of information in a defined range of areas (e.g. when procedures are developed to ensure regular network reporting and administration in accordance with organisational policies and procedures)
- Questioning and active listening skills in relation to clients and team members (e.g. when impact of the changes being implemented is conveyed to users)
- Project planning skills
- Problem solving skills for a defined range of unpredictable problems

Required knowledge

- Current industry-accepted hardware and software products, with broad knowledge of features and capabilities
- Broad knowledge of the client business domain, business function and organisation (e.g. when implementing multiple servers)
- Broad knowledge of networking technologies, with substantial depth in some areas
- Broad knowledge of OH&S requirements in relation to work safety, environmental factors and ergonomic considerations
- Broad knowledge of supporting documentation systems (e.g. when procedures are developed to ensure regular network reporting and administration in accordance with organisational policies and procedures)
- Knowledge of the Open Systems Interconnection OSI reference model

Evidence Guide

EVIDENCE GUIDE	
<p>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.</p>	
Overview of assessment	
Critical aspects for assessment and evidence required to demonstrate competency in this unit	<p>Evidence of the following is essential:</p> <ul style="list-style-type: none"> • Assessment must confirm the ability to install, configure and test components in a complex network. • Assessment must confirm the ability to manage a complex network that consists of multiple components and connectivity options. <p>To demonstrate competency in this unit the following resources will be needed:</p> <ul style="list-style-type: none"> • Network design documentation • Equipment specifications • Live network • Hardware and software components for complex networks
Context of and specific resources for assessment	<p>The installation and management of complex networks is a critical business function. As organisations rely more heavily on electronic internal communications, commercial e-business transactions with customers and virtual supplier partnerships, complex networks which enable and support such relationships are critical. The uninterrupted, efficient and secure operation of ICT networks is a primary objective of network specialists working to support business objectives. The breadth, depth and complexity covering planning and initiation of alternative approaches to skills or knowledge applications across a broad range of technical and/or management requirements, evaluation and coordination would be characteristic.</p> <p>The demonstration of competency may also require self-directed application of knowledge and skills, with substantial depth in some areas where judgement is required in planning and selecting appropriate equipment, services and techniques for self and others.</p>

EVIDENCE GUIDE	
	<p>Assessment must ensure:</p> <ul style="list-style-type: none"> • Applications involve participation in development of strategic initiatives as well as personal responsibility and autonomy in performing complex technical operations or organising others. It may include participation in teams including teams concerned with planning and evaluation functions. Group or team coordination may also be involved.
Method of assessment	<p>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.</p> <ul style="list-style-type: none"> • 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. • 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	<p>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:</p> <ul style="list-style-type: none"> • ICAS5122C Identify and resolve network problems • ICAS5123C Manage network security

EVIDENCE GUIDE

	<p>An individual demonstrating this competency would be able to:</p> <ul style="list-style-type: none"> • Demonstrate understanding of a broad knowledge base incorporating theoretical concepts, with substantial depth in some areas • Analyse and plan approaches to technical problems or management requirements • Transfer and apply theoretical concepts and/or technical or creative skills to a range of situations • Evaluate information, using it to forecast for planning or research purposes • Take responsibility for own outputs in relation to broad quantity and quality parameters • Take some responsibility for the achievement of group outcomes • 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.

Servers may include:

- Application/web servers
- BEA Weblogic servers
- IBM VisualAge and WebSphere
- Novell NDS servers
- Email servers
- File and print servers
- Voice servers
- FTP servers
- Firewall servers
- Proxy/cache servers

RANGE STATEMENT	
Client may include but is not limited to:	<ul style="list-style-type: none"> • internal departments • external organisations • clubs • individual people • internal employees
Organisational requirements may include but is not limited to:	<ul style="list-style-type: none"> • how and what the organisation wants in regard to work environment • problem solution processes • preventative maintenance and diagnostic policy • roles and technical responsibilities in network management • vendor and product service-level support agreements
Documentation may follow:	<ul style="list-style-type: none"> • ISO/IEC/AS standards • audit trails • naming standards • version control • project management templates and report writing • maintaining equipment inventory • client training • satisfaction reports
User may include:	<ul style="list-style-type: none"> • a person within a department • a department within the organisation • a third party
Cabling may include but is not limited to:	<ul style="list-style-type: none"> • UTP • STP • Category 5e, 6, 7 • fibre
Network may include but is not limited to:	<ul style="list-style-type: none"> • large and small LANs • national WANs • VPNs • the internet • the use of the PSTN for dial-up modems only • private lines • data • voice
Network topology may include:	<ul style="list-style-type: none"> • cabled ring • star • bus

RANGE STATEMENT	
	<ul style="list-style-type: none"> • hierarchical and hybrid or wireless networks
Firewalls may include:	<ul style="list-style-type: none"> • hardware appliances • proxy servers • individual PC solution • also: varying functionality, including network address translation (NAT)/IP Masquerading, routing to specific machines as well as Stateful Packet Inspection (SPI), Denial of Service (DOS) detection and blocking, spoofing, unauthorised associations
Components may include:	<ul style="list-style-type: none"> • motherboards • CMOS battery • central processing unit (CPU) • CD and DVD drives • interface cards • drives • fax/modem cards • RAM upgrades • CPU upgrades
Hardware may include but is not limited to:	<ul style="list-style-type: none"> • mobile equipment • workstations • personal computers • modems • wireless access points and other connectivity devices • networks • DSL modems • remote sites • servers
Tools may include but are not limited to:	<ul style="list-style-type: none"> • network performance software • data and voice integration measurements • policing and shaping tools • frequency analysers • cable testing • equipment testing • carrier connection tests
Security may include but is not limited to:	<ul style="list-style-type: none"> • IPSec • LEAP • WEP • WPA

RANGE STATEMENT	
	<ul style="list-style-type: none"> • AAA • Diameter • tokens • smart cards
<i>Standards</i> may include:	<ul style="list-style-type: none"> • ISO/IEC/IEEE/IETF/ITU/AS standards, • organisational standards • project standards
<i>Software</i> may include but is not limited to:	<ul style="list-style-type: none"> • commercial software applications • organisation-specific software, packaged software, in-house or customised software

Unit Sector(s)

Unit sector	Implement
--------------------	-----------

Co-requisite units

Co-requisite units	

Competency field

Competency field	
-------------------------	--