



Australian Government

Department of Education, Employment and Workplace Relations

ICAWEB512A Administer business websites and servers

Release: 1

ICAWEB512A Administer business websites and servers

Modification History

Release	Comments
Release 1	This Unit first released with <i>ICAI1 Information and Communications Technology Training Package version 1.0</i>

Unit Descriptor

This unit describes the performance outcomes, skills and knowledge required to maintain and manage business websites and associated servers.

Application of the Unit

This unit applies to middle managers, such as multimedia developers, web strategists or project managers, responsible for managing business websites and associated servers.

They provide technical advice, guidance and leadership in resolution of specified problems and their role may involve responsibility for others.

The role involves leading development of strategic reviews, and preparing a security plan, as well as preparing for future growth and requirements. Related tasks include evaluating and testing security website metrics and performance indicators.

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

<p>1. Maintain business website and contents</p>	<p>1.1 Establish personnel policy and procedures for managing access and changes to aspects of the business website</p> <p>1.2 Design and start a training program for teaching staff how to use procedures and policies as well as making changes to the business website</p> <p>1.3 Evaluate and test site-analysis software on a non-live <i>server</i> to verify features and functions are safe for use on a live server</p> <p>1.4 Generate site summary reports in line with the organisational quality management program or guidelines</p> <p>1.5 Review reports found to have generated security flaws</p> <p>1.6 Check links for functionality and ongoing relevance</p> <p>1.7 Modify web pages according to changing business requirements and analysis of site summary report</p> <p>1.8 Maintain and debug <i>database</i> information according to site and information requirements</p>
<p>2. Maintain business security of the website</p>	<p>2.1 Establish a security response procedure to control information placed on the business website by developers, designers and end users</p> <p>2.2 Develop a <i>security plan</i></p> <p>2.3 Test site security according to organisational requirements of the security plan</p> <p>2.4 Maintain site security using information from security vendors and technical media outlets</p>
<p>3. Monitor business website performance</p>	<p>3.1 Select <i>server analysis tools</i> with reference to organisational requirements and the range of functionalities requiring monitoring</p> <p>3.2 Determine business website load metrics and performance indicators in line with organisational requirements</p> <p>3.3 Measure business website server performance with server analysis tools</p> <p>3.4 Identify and document business options for performance improvement</p> <p>3.5 Submit website server performance reports to <i>client</i></p>
<p>4. Undertake capacity planning</p>	<p>4.1 Determine future peak volumes by measuring page usage and volume access</p> <p>4.2 Develop an upgrade program to deal with increasing load and performance issues</p>

	<p>4.3 Set performance benchmarks to take into consideration possible future scenarios for each load metric</p> <p>4.4 Determine options for upgrade path for <i>equipment</i> needs based on research and business website performance growth forecasting</p>
--	--

Required Skills and Knowledge

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

Required skills

- analytical skills to:
 - evaluate site-analysis software
 - select server analysis tools according to organisational requirements
- communication skills to:
 - facilitate training programs for staff
 - liaise with vendors
- literacy skills to write reports and planning documentation
- planning skills to forecast business website-performance growth
- technical skills to:
 - use:
 - current forecasting methodology for identifying traffic peaks
 - current site server
 - integrity-checking software
 - intrusion-detection software
 - traffic-tracking software
 - web server log-file analysis
 - maintain:
 - firewalls
 - virtual private network (VPN) gateways
 - respond to request for proposals (RFPs).

Required knowledge

- bottlenecks and methods of correction
- electronic commerce modelling language (ECML)
- queuing systems
- standard generalised markup language (SGML) and associated standards
- user request classes
- website architecture
- website security issues
- workload metrics.

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	<p>Evidence of the ability to:</p> <ul style="list-style-type: none"> • evaluate and test site-analysis software • maintain site security • monitor website performance • develop upgrade program to cater for business website performance growth.
Context of and specific resources for assessment	<p>Assessment must ensure access to:</p> <ul style="list-style-type: none"> • site servers and web servers where tasks may be performed • business website • site server and analysis software currently used in industry • requirements and business-planning documentation • appropriate learning and assessment support when required • modified equipment for people with special needs.
Method of assessment	<p>A range of assessment methods should be used to assess practical skills and knowledge. The following examples are appropriate for this unit:</p> <ul style="list-style-type: none"> • direct observation of candidate testing site security according to security plan • verbal or written questioning to assess candidate's knowledge of features of website architecture and security issues • review of documentation prepared by candidate, including security plan, training program, website server performance reports and upgrade program.
Guidance information for assessment	<p>Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended, where appropriate.</p> <p>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.</p> <p>Indigenous people and other people from a non-English speaking background may need additional support.</p> <p>In cases where practical assessment is used it should be combined with targeted questioning to assess required knowledge.</p>

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.

<i>Server</i> may include:	<ul style="list-style-type: none"> • Apache HTTP server • email servers • file and print servers • file transfer protocol (FTP) servers • IBM VisualAge and WebSphere • iPlanet-Enterprise • Lotus Domino • Microsoft Internet Information Server (Microsoft IIS) • NetDynamics • Netscape Enterprise server, Netscape FastTrack, Netscape eBusiness • proxy servers • Sun Microsystems iPlanet web server • Sun Microsystems Java web server • Zope.
<i>Database</i> may include:	<ul style="list-style-type: none"> • DB2 • Informix • Ingres • Microsoft SQL (MS SQL) server • Mini SQL (mSQL) • MySQL • Oracle • Sybase.
<i>Security plan</i> may include:	<ul style="list-style-type: none"> • alerts relating to the security objectives of the organisation • audits • privacy • standards: <ul style="list-style-type: none"> • archival • backup • network • theft • viruses.
<i>Server analysis tools</i>	<ul style="list-style-type: none"> • Apache Jmeter • Apache JSSI.

may include:	
<i>Client</i> may include:	<ul style="list-style-type: none">• employee• external organisation• individual• internal department.
<i>Equipment</i> may include:	<ul style="list-style-type: none">• hard drives• hubs• modems or other connectivity devices, including digital subscriber line (DSL) modems• monitors• other peripheral devices• personal computers• personal digital assistants (PDAs)• printers• switches• workstations.

Unit Sector(s)

Web