Australian Government

Department of Education, Employment and Workplace Relations

ICAWEB423A Ensure dynamic website security

Release: 1

ICAWEB423A Ensure dynamic website security

Modification History

Release	Comments
Release 1	This Unit first released with *ICA11 Information and Communications Technology Training Package version 1.0*

Unit Descriptor

This unit describes the performance outcomes, skills and knowledge required to ensure and maintain the security of a dynamic, commercial website.

Application of the Unit

This unit applies to web developers who are required to confirm the security of dynamic websites.

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
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

1. Undertake risk assessment	1.1 Identify functionality and features of the website and confirm with ***client***
	1.2 Identify ***security threats*** with reference to functionality of the site and organisational ***security policy***, ***legislation*** and ***standards***
	1.3 Complete a risk analysis to prioritise security threats and identify system vulnerabilities
	1.4 Identify resource and budget constraints and validate with client as required
	1.5 Source appropriate products, ***security services*** and ***equipment*** according to enterprise purchasing policies
2. Secure operating systems (OS)	2.1 Identify ***OS*** and cross-platform vulnerabilities
	2.2 Make appropriate scripting or configuration adjustments with reference to functionality of the site and the security policy
	2.3 Identify and rectify weaknesses specific to the OS
3. Secure site server	3.1 Configure the web server securely with reference to required functionality and the security policy
	3.2 Review and analyse server-side scripting with reference to required functionality and the security policy
	3.3 Install ***firewalls*** as required
	3.4 Establish access control permissions to ***server*** and ***database***
4. Secure data transactions	4.1 Identify data transactions with reference to functionality and features of website
	4.2 Identify and apply channel protocols related to requirements
	4.3 Install and configure payment systems
5. Monitor and document security framework	5.1 Develop a program of selective independent audits and penetration tests
	5.2 Determine performance benchmarks
	5.3 Implement audit and test programs, and record, analyse and report results
	5.4 Make security framework changes based on test results
	5.5 Develop the site-security plan with reference to security policy and requirements
	5.6 Develop and distribute related policy and procedures to client

Required Skills and Knowledge

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

Required skills

- communication skills to liaise with internal and external personnel on technical, operational and business-related matters
- literacy skills to:
  - collate, analyse and assess importance and relevance of product information
  - summarise and document information
  - write procedures
- numeracy skills to take test measurements, interpret results and evaluate performance
- planning and organisational skills to:
  - develop enterprise policy and procedures
  - plan, prioritise and monitor own work
- research skills to interrogate vendor databases and websites
- technical skills to:
  - configure a web server
  - identify key sources of information
  - see conflicts and integration capabilities between diverse equipment
  - understand specification sheets
  - use auditing and penetration testing techniques.

Required knowledge

- Australian Computer Society Code of Ethics
- client business domain, structure, function and organisation, including organisational issues surrounding security
- copyright and intellectual property as related to website information
- commonwealth Privacy Act 2000
- current industry-accepted hardware and software products
- desktop applications and OS as required
- technical knowledge of functions and features of:
  - automated intrusion detection software
  - network address translation (NAT) related to securing internal IP addresses, buffer overruns and stack smashing with reference to operating system deficiencies
  - authentication and access control
  - common stored account payment systems
  - cryptography
  - CGI scripts
  - generic secure protocols
  - stored value payment systems
  - advantages and disadvantages of using the range of security features
  - protocol stack for internet communications
  - physical web server security, particularly remote host security threats.

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: • identify potential security threats to a website • develop strategies to secure a dynamic website • implement such strategies.
Context of and specific resources for assessment	Assessment must ensure access to: • dynamic website • security plan • user requirements • relevant legislation, standards and organisational requirements • 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:
	• verbal or written questioning to assess candidate's knowledge of:
	  • client domain
	  • website security techniques
	  • current website security threats
	• review of candidate's documented:
	  • risk assessment
	  • performance benchmarks
	• evaluation of candidate's security framework.

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.

Client may include:	• external organisation • individual • internal department • internal employee.
Security threats may include:	• denial of service and by-pass • eavesdropping • hackers • manipulation and impersonation • penetration • viruses using logging.
Security policy may include:	• audits and alerts • privacy • standards, including archival, backup and network • theft • viruses.
Legislation may include:	• copyright • liability statements • privacy legislation.
Standards may include:	• International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) and Australian Standards (AS) standards • organisational standards • project standards.
Security services may include:	• application proxies • authentication and access control • digital certificates • digital signatures • encryption • file access permissions • multi-platform directory services supporting relevant standards • network points and mainframes • packet filters • personnel security • screening routers

	• servers • secure hypertext transfer protocol (SHTTP) • single stage and dual stage firewalls • smart cards • secure socket layer (SSL) • stored account payment systems • stored value payment systems • support for generalised security services interfaces • trusted hardware and operating systems at selective desktops • trusted systems with C and B assurance levels • virtual private network (VPN) technology.
Equipment may include:	• hard drives • hubs • modems and other connectivity devices, including digital subscriber line (DSL) modems • monitors • other peripheral devices • personal computers (PCs) • personal digital assistants (PDAs) • printers • switches • workstations.
OS may include:	• Mac OS 8 or above • Linux 6.0 or above • Windows XP or above.
Firewalls may include:	• hardware appliances • individual PC solution; varying functionality, including network address translator (NAT) and IP masquerading, routing to specific machines • proxy servers.
Server may include:	• application or web servers • BEA Weblogic servers • email servers • file and print servers • file transfer protocol (FTP) servers • firewall servers • IBM VisualAge and WebSphere • Novell Directory Services (NDS) servers • proxy or cache servers.
Database may include:	• commercial off-the-shelf (COTS) database packages • object-relational databases • proprietary databases

	• relational databases.
Requirements may refer to:	• application • business • network • people in the organisation • system.

Unit Sector(s)

Web