Australian Government

Department of Education, Employment and Workplace Relations

ICAT4195B Ensure dynamic website security

Release: 1

ICAT4195B Ensure dynamic website security

Modification History

Not Applicable

Unit Descriptor

Unit descriptor	This unit defines the competency required to ensure and maintain the security of a dynamic, commercial website. The following unit is linked and forms an appropriate cluster: • ICAB5165B Create dynamic pages 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
	ICAT4194B	Ensure basic website security

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. 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***, relevant ***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	2.1. Identify ***operating system*** and cross-platform vulnerabilities
	2.2. Make appropriate scripting/configuration adjustments with reference to functionality of the site and the ***security policy***
	2.3. Identify and rectify weaknesses specific to the ***operating system***
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 relevant 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 where relevant 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 with results recorded, analysed and reported
	5.4. Make security framework changes based on test results

ELEMENT	PERFORMANCE CRITERIA
	5.5. Develop the site security plan with reference to ***security policy*** and ***requirements*** 5.6. Develop and distribute related policies and procedures to ***client***

Required Skills and Knowledge

REQUIRED SKILLS AND KNOWLEDGE

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

Required skills

- Ability to develop enterprise policies and procedures
- Auditing and penetration testing techniques
- Configuring a web server
- Ability to identify key sources of information
- Ability to understand specification sheets
- Ability to accurately summarise and document information
- Ability to see conflicts and integration capabilities between diverse equipment
- Ability to collate, analyse and assess importance and relevance of product information.

Required knowledge

- Security threats, including vandalism, sabotage, breach of privacy or confidentiality, theft and fraud, violations of data integrity, denial of service
- Organisational issues surrounding security
- Functions and features of stored value payment systems (e.g. DigiCash, CyberCoin, Mondex, CAFE, Visa Cash)
- Functions and features of common stored account payment systems (e.g. First Virtual's Internet Payment System, CyberCash secure internet payment system, Secure Electronic Transactions standard (SET), smart cards)
- Functions and features of generic secure protocols (e.g. secure socket layer (SSL), secure hypertext transfer protocol (SHTTP), secure multi-purpose internet mail extensions (S/MIME))
- Functions and features of automated intrusion detection software, functions and features of network address translation (NAT) in relation to securing internal IP addresses, buffer overruns and stack smashing with reference to operating system deficiencies, functions and features of authentication and access control (e.g. single-factor and two-factor authentication, biometric authentication)
- Functions and features of cryptography, including digital signatures and public and

REQUIRED SKILLS AND KNOWLEDGE
private key algorithms, functions and features of CGI scripts, advantages and disadvantages of using the range of security features, protocol stack for internet communications, knowledge of physical web server security, particularly remote hosts • Australian Computer Society Code of Ethics • Copyright and intellectual property • The Commonwealth Privacy Act 2000

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 the ability to identify potential security threats and develop and implement strategies to secure a dynamic website. To demonstrate competency in this unit the person will require access to: • Dynamic website • Security plan
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.
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

EVIDENCE GUIDE	
	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: • ICAB5165B Create dynamic pages 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 • 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

EVIDENCE GUIDE	
	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.	
Client may include but is not limited to:	• internal departments • external organisations • individual people • internal employees
Legislation may include:	• privacy legislation • copyright • liability statements
Standards may include:	• ISO/IEC/AS standards • organisational standards • project standards (for further information refer to the Standards Australia website at: www.standards.com.au)
Security threats may include:	• eavesdropping • manipulation and impersonation • penetration • denial of service and by-pass • hackers • viruses using logging
Equipment may include but is not limited to:	• workstations • personal computers • modems and other connectivity devices • printers • hard drives • monitors

RANGE STATEMENT	
	• switches • DSL modems • Hubs • personal digital assistant (PDA) • other peripheral devices
Security policy may include:	• theft • viruses • standards (including archival, back-up, network) • privacy • audits • alerts and usually relates directly to the security objectives of the organisation
Operating system may include but is not limited to:	• Linux 6.0 or above, Windows 98 or above, Apple OS 8 or above. Note: The use of operating system in this unit is in the context of a pre-existing system and may therefore not be current industry version. Preference is for Linux 7.0 or above, Windows 2000 or above, Apple OS X or above
Firewalls may include:	• hardware appliances • proxy servers • individual PC solution; varying functionality, including network address translation (NAT)/IP masquerading, routing to specific machines
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
Database may include but are not limited to:	• relational databases • object-relational databases • proprietary databases • commercial off-the-shelf (COTS) database

RANGE STATEMENT	
	packages
Requirements may be in reference to:	• business • system • application • network • people in the organisation
Security services may include:	• SSL • S-HTTP • stored account payment systems • stored value payment systems • file access permissions • single stage and dual stage firewalls • encryption • smart cards • digital certificates • authentication and access control • digital signatures • VPN technology • screening routers • packet filters • application proxies • trusted systems with C and B assurance levels • support for generalised security services interfaces • personnel security • servers • trusted hardware and operating systems at selective desktops • network points and mainframes • multi-platform directory services supporting relevant standards

Unit Sector(s)

Unit sector	Test

Co-requisite units

Co-requisite units		

Competency field

Competency field	