Australian Government

Department of Education, Employment and Workplace Relations

ICAI5197B Install and maintain valid authentication processes

Release: 1

ICAI5197B Install and maintain valid authentication processes

Modification History

Not Applicable

Unit Descriptor

Unit descriptor	This unit defines the competency required to develop, install and maintain an authentication processes. The following unit is linked and forms an appropriate cluster: • ICAI5196B Implement secure encryption technologies

Application of the Unit

Application of the unit	

Licensing/Regulatory Information

Not Applicable

Pre-Requisites

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. Determine authentication requirements	1.1. Determine user and enterprise security requirements with reference to enterprise security plan 1.2. Identify and analyse authentication options according to user and enterprise requirements 1.3. Select the most appropriate authentication and authorisation processes
2. Configure authentication software/tools	2.1. Create an authentication realm and reuse as required to protect different areas of the ***server*** 2.2. Add ***users*** and authorisation rules to the new realm according to business needs 2.3. Describe the ***user*** attributes and the user attribute set-up 2.4. Set up an authentication filter and authorisation parameters on the appropriate ***server*** according to business requirements
3. Apply authentication methods	3.1. Develop and/or obtain authentication protocols as required 3.2. Develop and distribute related policies and procedures to users according to business need 3.3. Brief ***user*** on the authentication system and their responsibilities according to enterprise security plan 3.4. Apply the authentication system to ***network*** and ***user*** according to system/product requirements 3.5. Record and store permission and configuration information in a secure central location
4. Monitor authentication system	4.1. Review the authentication system according to user and enterprise security and quality of service requirements 4.2. Ensure ongoing security monitoring using incident management and reporting processes in accordance with enterprise security plan

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

- Ability to develop enterprise policies and procedures
- Ability to analyse enterprise security requirements and propose solutions
- Scripting
- Ability to liaise with vendors and service providers as required
- Incident management

Required knowledge

- Organisational issues surrounding security
- The function and operation of virtual private networking (VPN) concepts
- Common VPN issues, including quality of service considerations (QOS), bandwidth, dynamic security environment
- The function and operation of authentication
- The features of common password protocols (e.g. password authentication protocol (PAP), challenge handshake authentication protocol (CHAP), challenge phrases, RADIUS authentication)
- Features and function of token cards
- Features and function of authentication adaptors
- Features and function of biometric authentication adaptors
- Features and function of digital certificates (e.g. VeriSign, X.509, SSL)
- Resource accounting through authentication

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 ensure authentications solutions are deployed and appropriate to the business technology environment and business needs. To demonstrate competency in this unit the person will require access to: • Servers
Context of and specific resources for assessment	Security of information and personnel is of increasing importance to all organisations. Authentication is a control or protective measure put into place by an organisation to reduce the vulnerability of the system. Authentication controls include passwords, PINs, smart cards and biometric devices. 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. Assessment must ensure: • 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. • Applications involve participation in development of strategic initiatives as well as personal responsibility and autonomy in performing complex technical

EVIDENCE GUIDE	
	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	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. • 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: • ICAI5196B Implement secure encryption technologies An individual demonstrating this competency would be able to: • Demonstrate understanding of a broad knowledge base incorporating theoretical concepts, with

EVIDENCE GUIDE	
	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.	
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
User may include:	• a person within a department • a department within the organisation • a third party
Network may include but is not limited to:	• large and small LANs • national WANs • the internet

RANGE STATEMENT	
	• VPNs • the use of the PSTN for dial-up modems only • private lines • data • voice

Unit Sector(s)

Unit sector	Implement

Co-requisite units

Co-requisite units		

Competency field

Competency field	