Australian Government

Department of Education, Employment and Workplace Relations

ICANWK503A Install and maintain valid authentication processes

Release: 1

INDUSTRY SKILLS COUNCILS
Creating Australia's Future

ICANWK503A Install and maintain valid authentication processes

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 design, develop, install and maintain authentication processes. Security of information and personnel is of increasing importance to 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, personal identification numbers (PINs), smart cards, biometric devices and other Authentication protocols.

Application of the Unit

This unit applies to middle managers, such as information security managers, network engineers or security analysts, responsible for implementing and monitoring the organisational security management system.

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. 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 or tools	2.1 Create an authentication realm and reuse as required to protect different areas of ***server*** 2.2 Add ***users*** and authorisation rules to new realm according to business needs 2.3 Describe user attributes and 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 or obtain authentication ***protocols*** as required 3.2 Develop and distribute related ***methods*** to users according to business need 3.3 Brief user on authentication system and their responsibilities according to enterprise security plan 3.4 Apply 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, according to enterprise security plan 4.3 Adjust authentication system if required

Required Skills and Knowledge

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

Required skills

- analytical skills to:
  - analyse network information
  - plan approaches to technical problems or management requirements
- communication skills to:
  - convey and clarify complex information
  - liaise with clients
- literacy skills to interpret and prepare technical documentation, including recording authentication events related to network security design and incident response
- planning skills to plan control methods for managing authentication processes
- problem-solving skills to:
  - apply solutions in complex networks, including systems processes
  - instigate rapid deployment of solutions to problems involving authentication failure and security incidents
- technical skills to apply best practice to systems authentication methodologies and technologies.

Required knowledge

- overview knowledge of:
  - problems and challenges dealing with organisational authentication issues
  - resource accounting through authentication
  - common virtual private network (VPN) issues, including quality of service (QoS) considerations, bandwidth, dynamic security environment
  - function and operation of VPN concepts
- authentication adaptors
- biometric authentication adaptors
- digital certificates, such as VeriSign, X.509, and SSL
- function and operation of authentication
- network authentication services, such as Kerberos and NT LAN Manager (NTLM)
- features of common password protocols, such as:
  - challenge handshake authentication protocol (CHAP)
  - challenge phrases
  - password authentication protocol (PAP)
  - remote authentication dial-in user service (RADIUS) authentication
- token cards.

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: • design and deploy authentications solutions to the business technology environment and business needs • configure authentication software or tools • monitor and test authentication process after implementation • ensure authentication solutions are current.
Context of and specific resources for assessment	Assessment must ensure access to: • site or prototype where network authentication may be implemented and managed • network support tools currently used in industry • organisational security policies related to authentication, manufacturer recommendations and current authentication standards, including biometric authentication adaptors • appropriate learning and assessment support when required. Where applicable, physical resources should include equipment modified 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: • current and emerging authentication processes • features and limitations in vendor solutions, operating systems and software • direct observation of candidate demonstrating management of authentication processes in a range of complex systems • review of documentation prepared by candidate to manage authentication processes.
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.

Server may include:	• application or web • building environmental assessment (BEA) Weblogic • Certificate authority • email • file and print • firewall • file transfer protocol (FTP) • IAS - RADIUS • IBM VisualAge and WebSphere • Microsoft domain controllers • Novell Directory Services (NDS) • proxy or cache • routing and remote access, e.g. using virtual private network (RRAS-VPN).
Users may include:	• external client • intranet • remote.
Protocols may include:	• CHAP and PAP • Kerberos • lightweight directory access protocol (LDAP) • network level authentication • NTLM • open LDAP • simple and protected GSSAPI negotiation mechanism (SPNEGO) • security support provider interface (SSPI).
Methods may include:	• certificates • challenge response • face, voice and unique bio-electric signals • fingerprint • ID card • other biometric identifier • pass phrase • password

	- PIN - retinal pattern - security token - signature - software token.
Network may include:	- data - internet - large and small local area networks (LANs) - national wide area networks (WANs) - private lines - use of the public switched telephone network (PSTN) for dial-up modems only - voice - VPNs.

Unit Sector(s)

Networking