



Australian Government

Department of Education, Employment and Workplace Relations

ICAI5196B Implement secure encryption technologies

Release: 1

ICAI5196B Implement secure encryption technologies

Modification History

Not Applicable

Unit Descriptor

Unit descriptor	This unit defines the competency required to ensure secure encryption is applied and monitored.
------------------------	---

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 encryption methods	1.1. Review the security plan to determine encryption methods 1.2. Review a range of encryption technologies and rank the most appropriate options 1.3. Assess the costs associated with each encryption option 1.4. Document encryption options and costs and forward to appropriate person for decision
2. Implement encryption	2.1. Purchase encryption technologies according to business procurement procedures 2.2. Apply encryption technologies to the business system 2.3. Analyse the impact of the encryption technologies to user roles and responsibilities 2.4. Inform user of the new encryption technologies and the impact it has on their responsibilities
3. Monitor encryption	3.1. Analyse implementation of the encryption technologies 3.2. Review help desk records for problems concerning implementation and take appropriate action 3.3. Review system logs for user breaches 3.4. Document security breaches and notify appropriate person

Required Skills and Knowledge

REQUIRED SKILLS AND KNOWLEDGE

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

Required skills

- Surveillance analysis
- Implementation of encryption protocols
- Implementing LAN/WLAN, VPN or WAN solutions
- Ability to undertake a network security risk assessment
- Ability to develop enterprise policies and procedures

REQUIRED SKILLS AND KNOWLEDGE**Required knowledge**

- Security threats, including eavesdropping, data interception, data corruption, data falsification, authentication issues
- Organisational issues surrounding security
- Encryption strength
- Encryption types (public key, secret key, hash key)
- The functions and features of symmetric encryption, asymmetric encryption and one-way encryption
- Examples of symmetric key encryption (e.g. DES, Triple DES, Skipjack, IDEA, Blowfish)
- Examples of asymmetric key encryption (e.g. RSA)
- Asymmetric key-based algorithms and public key/private key encryption
- PKI, PGP: pretty good privacy, GnuPG
- Examples of one-way encryption (e.g. message digests [MD5, SHA]), functions and features of timestamps, functions and features of digital signatures, replay security, functions and features of access control permissions, certificate-related infrastructure (certificate authorities, registration authorities, repository services), TCP/IP protocols and applications

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 encryption solutions are implemented and appropriate to the business technology environment and business needs.

To demonstrate competency in this unit the person will require access to:

- Servers
- Encryption software

Context of and specific resources for assessment

The integrity of organisational data and sensitive documents is vital for businesses. Encryption of sensitive data is a way for organisations to protect this data. Confidentiality, integrity and availability of data are the three key goals for securing information.

A number of commercial encryption technologies are available in the market. It is vital that the implementation of these technologies takes place in a methodical and informed manner. Research of available technologies is important including information available through online vendor and newsgroup sources and security forums.

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

EVIDENCE GUIDE	
	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 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.

EVIDENCE GUIDE

	An individual demonstrating this competency would be able to: • Demonstrate understanding of a broad knowledge base incorporating theoretical concepts, with 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.

<i>Encryption</i> may include but is not limited to:	• RSA public key • PGP (Pretty Good Privacy) • symmetric ciphers • asymmetric public-key ciphers • sniffers • PKI • SSH • DESlogin • PKZIP • secure socket layer (SSL) • digital signatures
--	---

RANGE STATEMENT	
<i>Appropriate person</i> may include:	• supervisor • teacher • authorised business representative • client
<i>Encryption technologies</i> may include:	• Authentex DataSafe • GPG (GNU software) • Blowfish Advanced 97 • Crypto ActiveX Tool • Distributed management systems • PGP • Cryptainer LE
<i>User</i> may include:	• a person within a department • a department within the organisation • a third party

Unit Sector(s)

Unit sector	Implement
--------------------	-----------

Co-requisite units

Co-requisite units	

Competency field

Competency field	
-------------------------	--