ICAI4249A Implement and evaluate data security

ICAI4249A Implement and evaluate data security

Modification History

Not Applicable

Unit Descriptor

Unit descriptor	This unit defines the competency required for the application of the principles, policies, and procedures necessary to ensure the confidentiality, integrity, availability, and privacy of data in all forms of media (electronic and hardcopy) throughout the data life cycle. *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		
	ICAS3024B	Provide basic system administration
	ICAS4124B	Monitor and administer network 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.

| Innovation and Business Skills Australia

Elements and Performance Criteria

ELEMENT	PERFORMANCE CRITERIA
1. Implement data security	1.1. Perform the data access management process according to established guidelines
	1.2. Apply and maintain *data security* controls and processes in accordance with *documentation*
	1.3. Apply media controls and processes
	1.4. Apply and verify *data security* access controls and privileges
	1.5. Address alleged violations of *data security* and privacy breaches
	1.6. Apply and maintain privacy controls in accordance with *privacy guidance*
2. Evaluate data security	2.1. Assess the effectiveness of the *enterprise data security* and suggest changes where appropriate
	2.2. Evaluate the effectiveness of products and technologies implemented to provide the required protection of data
	2.3. Review alleged violations of *data security* and privacy breaches
	2.4. Identify improvement actions required to maintain appropriate level of data protection

Required Skills and Knowledge

REQUIRED SKILLS AND KNOWLEDGE
This section describes the skills and knowledge required for this unit.
Required skills
- Current industry-accepted hardware and software products, with broad knowledge of general features and capabilities   - Broad knowledge of the client business domain, business function and organisation   - Systems technologies, with broad knowledge of general features and capabilities and substantial depth in some areas   - Risk analysis, with broad knowledge of general features   - Broad knowledge of specific security technology   - Broad knowledge of privacy issues and legislation.
Required knowledge

REQUIRED SKILLS AND KNOWLEDGE

- Problem solving skills for a defined range of unpredictable problems
- Plain English literacy and communication skills in relation to analysis, evaluation and presentation of information
- Research skills for identifying, analysing and evaluating broad features of a particular business domain and best practice in data security methodologies and technologies
- Report writing skills for business requiring depth in some areas, analysis and evaluation of information in a defined range of areas
- Questioning and active listening skills
- Project planning skills in relation to set benchmarks and identified scope.

Innovation and Business Skills Australia

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 knowledge of data security features available in the operating environment. • Assessment must confirm the ability to implement and evaluate data security functions on the system.
Context of and specific resources for assessment	Assessment must ensure: • Appropriate performance of the data access management process • Apply and maintain data security controls and privileges • Assess the effectiveness of the enterprise data security • 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. 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.

Innovation and Business Skills Australia

EVIDENCE GUIDE	
	To demonstrate competency in this unit the learner will require access to: • Security polices • Standards • Case study scenarios
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. The following assessment method is appropriate for this unit: • 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. An individual demonstrating this competency would be able to: • Demonstrate understanding of a broad knowledge

EVIDENCE GUIDE	
	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 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.	
Data security *may include*:	• electronic and physical data, i.e. paper-based • stored and transmitted
Documentation may include:	• data security policy • guidelines • business requirements
Privacy guidance may be in accordance with:	• standards • procedures • directives • policies • regulations • laws
Enterprise data security may include:	• policies • processes • and procedures against established standards • guidelines

|

RANGE STATEMENT	
	• business requirements

Unit Sector(s)

Unit sector	Implement

Co-requisite units

Co-requisite units		

Competency field

Competency field	