Australian Government

Department of Education, Employment and Workplace Relations

ICAS6254A Manage IT security

Release: 1

INDUSTRY SKILLS COUNCILS
Creating Australia's Future

ICAS6254A Manage IT security

Modification History

Not Applicable

Unit Descriptor

Unit descriptor	This unit defines the competency required to manage data security, Enterprise Continuity, Incidents, Networks and telecommunications security, System and Application Security. *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		
	ICAI4249A	Implement and evaluate data security
	ICAI4251A	Implement and evaluate network and telecommunication security
	ICAI5250A	Develop, implement and evaluate system and application security
	ICAI5252A	Develop, implement and evaluate an incident response plan

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. Manage data security	1.1. Ensure that security classification and data management policies and guidance are issued and updated 1.2. Specify policy and coordinate review and approval 1.3. Report compliance of data security policies to management 1.4. Implement appropriate changes and improvement actions as required
2. Manage enterprise continuity	2.1. Coordinate with corporate stakeholders to establish the enterprise continuity of operations program 2.2. Acquire the necessary resources, including financial resources, to conduct an effective enterprise continuity of operations program 2.3. Define the enterprise continuity of operations organizational structure and staffing model 2.4. Define emergency delegations of authority and orders of succession for key positions 2.5. Direct contingency planning, operations, and programs to manage risk 2.6. Define the scope of the enterprise continuity of operations program to address business continuity, business recovery, contingency planning, and disaster recovery and related activities 2.7. Integrate enterprise concept of operations activities with related contingency planning activities 2.8. Establish an enterprise continuity of operations performance measurement program 2.9. Identify and prioritize critical business functions 2.10. Implement appropriate changes and improvement actions as required
3. Manage incidents	3.1. Coordinate with stakeholders to establish the incident management program 3.2. Establish relationships between the incident response team and ***other groups*** 3.3. Acquire and manage the ***resources***, including financial resources, for the incident management functions 3.4. Ensure the coordination between the incident response team and the security administration and technical support teams

ELEMENT	PERFORMANCE CRITERIA
	3.5. Apply lessons learned from information security incidents to improve incident management processes and procedures 3.6. Implement appropriate changes and improvement actions as required
4. Manage networks and telecommunications security	4.1. Establish a network security and telecommunications program in line with enterprise policy and security goals 4.2. Manage the necessary resources, including financial resources, to establish and maintain an effective network security and telecommunications program 4.3. Direct network security and telecommunications personnel 4.4. Establish communications between the network security and telecommunications team and ***related security teams*** 4.5. Integrate network security and telecommunications program activities with technical support, security administration, and incident response activities 4.6. Establish a network security and telecommunications performance measurement program 4.7. Ensure enterprise compliance with ***applicable network-based documents*** 4.8. Ensure that network-based audits and management reviews are conducted to implement process improvement 4.9. Implement appropriate improvement actions, as required
5. Manage system and application security	5.1. Establish the IT system and application security engineering program 5.2. Acquire the necessary resources, including financial resources, to support the integration of security in the SDLC 5.3. Guide IT security personnel through the SDLC phases 5.4. Define the scope of the IT security program as it applies to the application of SDLC 5.5. Plan the IT security program components into the SDLC

Required Skills and Knowledge

REQUIRED SKILLS AND KNOWLEDGE

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

Required skills

- leading and mentoring people to achieve project outcomes
- maintaining commitment of stakeholders and project teams
- negotiating with stakeholders and team members using a range of communication styles to suit different audiences and purposes
- responding to diversity, including gender and disability
- using management tools applicable to complex activities
- applying risk management techniques including risk sharing and transfer
- managing finances
- applying ethical decision making and problem solving
- writing recommendations and preparing reports requiring precision of expression
- applying workplace safety procedures in line with requirements
- accessing/preparing information electronically or in hard copy

Required knowledge

- legislation, organisational/jurisdictional policies and procedures that may impact on management:
  - codes of ethics/conduct
  - occupational health and safety and environment requirements
  - governance requirements
  - quality standards
  - risk management
  - procurement guidelines
  - budgetary framework
  - financial management requirements
  - human resources
  - public relations
  - equal employment opportunity, equity and diversity principles
- management specifications and objectives
- management tools and techniques suited to a range of complex projects activities
- management systems
- organisational and political context
- critical analysis in a management context
- cost schedule control systems to handle potential budget blow-outs

REQUIRED SKILLS AND KNOWLEDGE
• business and commercial issues related to the management

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: • Manage data security • Manage enterprise continuity • Manage incidents • Manage networks and telecommunications security • Manage system and application security
Context of and specific resources for assessment	Assessment must ensure: • Specifying data policy and coordinate review • Direct contingency planning, operations, and programs to manage risk • Manage the necessary resources, including financial resources, to establish and maintain an effective network security and telecommunications program • Establish the IT system and application security engineering program To demonstrate competency in this unit the following resources will be needed: • IT business specifications • Information on the security environment including relevant laws/legislation, existing organisational security policies, organisational expertise and knowledge • Possible security environment also includes the threats to security that are, or are held to be, present in the environment • Risk analysis tools/methodologies • IT security assurance specifications • Management related scenarios
Method of assessment	The following assessment method is appropriate for this unit: • The purpose of this unit is to define the standard of performance to be achieved in the workplace. In

EVIDENCE GUIDE	
	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 to 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. The breadth, depth and complexity involving analysis, design, planning, execution and evaluation across a range of technical and/or management functions including development of new criteria or applications or knowledge or procedures would be characteristic. The demonstration of competency may also require application of a significant range of fundamental principles and complex techniques across a wise and often unpredictable variety of contexts in relation to either varied or highly specific functions. Contribution to the development of a broad plan, budget or strategy may be involved and accountability and responsibility for self and others in achieving the outcomes may also be characteristic.

EVIDENCE GUIDE	
	Applications involve significant judgement in planning, design, technical or leadership/guidance functions related to products, services, operations or procedures would be common. An individual demonstrating this competency would be able to: • Demonstrate understanding of specialised knowledge with depth in some areas • Analyse, diagnose, design and execute judgement across a broad range of technical or management functions • Generate ideas through the analysis of information and concepts at an abstract level • Demonstrate a command of wide-ranging, highly specialised technical, creative or conceptual skills • Demonstrate accountability for personal outputs within broad parameters • Demonstrate accountability for personal and group outcomes within broad parameters • 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.	
Other groups may include:	• internal, e.g. • legal department • HR • procurement • finance

RANGE STATEMENT	
	• external, e.g. • law enforcement agencies • vendors • public relations professionals
Related security teams may include:	• technical support • security administration • incident response
Applicable network-based documents may include:	• standards • procedures • directives • policies • regulations • laws

Unit Sector(s)

Unit sector	Support

Co-requisite units

Co-requisite units		

Competency field

Competency field	