Australian Government

ICANWK616A Manage security, privacy and compliance of cloud service deployment

Release 1

INDUSTRY SKILLS COUNCILS
Creating Australia's Future

ICANWK616A Manage security, privacy and compliance of cloud service deployment

Modification History

Release	Comments
Release 1	This version first released with ICA11 Information and Communications Technology Version 2.

Unit Descriptor

This unit describes the performance outcomes, skills and knowledge required to manage cloud security controls, and privacy and legal compliance when implementing cloud services for an enterprise.

Application of the Unit

This unit applies to those with managerial responsibility, such as experienced security technical specialists, security analysts and security consultants.

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

ELEMENTS	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. Manage enterprise cloud security controls	1.1. Identify cloud ***security issues*** faced by different ***delivery and deployment models*** relevant to enterprise 1.2. Determine specific enterprise areas of ***security responsibility*** 1.3. Implement most relevant ***security controls and measures*** to protect identified areas of responsibility
2. Manage enterprise cloud privacy and compliance	2.1. Identify relevant ***compliance regulations*** relating to data storage 2.2. Determine most relevant ***business continuity*** and ***data recovery*** plans 2.3. Identify, secure and maintain relevant logs and audit trails 2.4. Investigate and review ***legal, privacy and contractual issues*** to ensure they meet enterprise policy
3. Review, implement and document cloud security, privacy and compliance enhancements	3.1. Implement appropriate changes and integrate into current enterprise's ***continuity of operation program*** (COOP) 3.2. Establish a performance measurement program to evaluate security effectiveness of implemented security controls 3.3. Provide relevant ***documentation*** as part of COOP for audit tracking purposes

Required Skills and Knowledge

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

Required skills

analytical skills to analyse security breaches

- communication skills to:
  - communicate with peers and supervisors in relevant cloud computing technological areas
  - seek assistance and expert advice from relevant people in cloud computing industry area
- literacy skills to interpret technical documentation, equipment manuals and specifications
- research skills to locate appropriate sources of information regarding cloud computing solutions
- technical skills to:
  - identify features of cloud computing solutions
  - test and evaluate cloud computing solutions

Required knowledge

- business and commercial issues relating to the management of cloud security issues
- legislation, organisational and jurisdictional policy and procedures that may impact on management areas:
  - cloud-related privacy issues
  - codes of ethics and conduct
  - equal employment opportunity, equity and diversity principles
  - financial management requirements
  - governance requirements
  - work health and safety (WHS) and environmental requirements
  - quality standards
- management specifications and objectives
- management tools and techniques suited to a range of complex projects activities
- organisational and political context
- systems development life cycle (SDLC)
- techniques for critical analysis in a management context

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: • identify, manage and implement cloud security controls according to legal and privacy requirements • integrate cloud security plans into the enterprise's existing security plans • develop an ongoing performance measurement and evaluation review process.

Context of and specific resources for assessment	Assessment must ensure access to:
	• cloud information and communications technology (ICT) business specifications
	• cloud ICT security assurance specifications
	• management-related scenarios
	• a cloud focused security environment, including the threats to security that are, or are held to be, present in the environment
	• information on the security environment, including:
	  • laws or legislation
	  • existing enterprise security policies
	  • enterprise expertise
	• risk analysis tools and methodologies currently used in industry
	• appropriate learning and assessment support when required
	• modified equipment 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: • direct observation of candidate managing cloud-related networks and telecommunications security • direct observation of candidate managing cloud ICT security incidents • verbal or written questioning to assess candidate's knowledge of enterprise policies and procedures that impact on cloud ICT security • review of documentation prepared by candidate, including programs to manage compliance, privacy and risk.
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.*

Security issues may include:	• applications security • data security • enterprise continuity • infrastructure security • platform security • virtualisation security.
Delivery models may include:	• infrastructure as a service (IaaS) • platform as a service (PaaS) • software as a service (SaaS).
Deployment models may include:	• community cloud • hybrid cloud • private cloud • public cloud.

Security responsibility may include:	• clients:
	  • applications (if not part of licence)
	  • client employee access
	  • data (if not part of licence)
	  • physical client site security
	• enterprise (depending on licensing agreement):
	  • application
	  • data
	  • identity management systems
	  • infrastructure
	  • physical enterprise site security
	  • platform.

Security controls and measures may include:	• security management, including:
	  • corrective controls
	  • detective controls
	  • deterrent controls
	  • preventative controls.

Compliance regulations may include:	• international regulations • internet or web regulations • local regulations

	• regional regulations.

Business continuity may include:	• undertaking analysis of:
	  • business impact analysis
	  • threat and risk analysis
	  • impact scenarios
	• solution design
	• developing solution implementation strategies
	• testing and enterprise acceptance
	• implementing suitable maintenance options.

Data recovery may include:	• logical damage recovery:
	  • corrupt partitions
	  • overwritten data
	• physical damage recovery
	• virus infections.

Legal, privacy and contractual issues may include:	• critical data masked • digital identities protected • end-of-service: return of data and applications • intellectual property: ownership of data • liability of data loss • unauthorised on-selling of information.

Continuity of operations program may include:	• COOP plan execution
	• COOP plan revision and updating
	• COOP program implementation
	• identification of functional requirements:
	  • mission impact analysis
	  • mitigation strategies and plan
	  • plan design and development
	  • project initiation
	  • risk assessment
	  • training, testing and drills.

Documentation may include:	• applicable network-based documents • audits and management reviews • communications protocols • contingency plans and activities • evaluation reports • incident management program, processes and procedures • management reports • network security and telecommunications program • performance measurement program • reviews and improvements records

	• security classification and data management policies • security incident records.

Unit Sector(s)

Networking