



Australian Government

ICTCLD602 Manage information security compliance of cloud service deployment

Release: 1

ICTCLD602 Manage information security compliance of cloud service deployment

Modification History

Release	Comments
Release 1	This version first released with ICT Information and Communications Technology Training Package Version 6.0.

Application

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

It applies to those with managerial responsibility of a business' IT infrastructure, including cloud engineers, systems engineers and experienced security technical specialists, security analysts, security consultants.

No licensing, legislative or certification requirements apply to this unit at the time of publication.

Unit Sector

Cloud computing

Elements and Performance Criteria

ELEMENT	PERFORMANCE CRITERIA
<i>Elements describe the essential outcomes.</i>	<i>Performance criteria describe the performance needed to demonstrate achievement of the element.</i>
1. Identify information security risks for cloud service	1.1 Identify cloud security risks for different cloud delivery and deployment models 1.2 Identify and review legal, privacy and contractual issues, organisational policies, procedures and requirements 1.3 Map responsibilities between organisation and cloud vendor 1.4 Review compliance controls of cloud vendor 1.5 Identify risks and identify risks that are organisation's responsibility
2. Manage cloud security controls	2.1 Identify security controls provided by the cloud vendor for

ELEMENT	PERFORMANCE CRITERIA
	cloud service 2.2 Map security controls to organisation risks 2.3 Configure security controls to mitigate risk according to business needs 2.4 Document configuration of security control and risk mitigation
3. Manage cloud privacy compliance	3.1 Identify required data storage compliance regulations 3.2 Determine data privacy risks associated with cloud service 3.3 Determine and implement business continuity and data recovery plan requirements 3.4 Review user access policies and configuration to data 3.5 Identify, secure and maintain, logs and audit trails according to business requirements 3.6 Document data privacy risk mitigation
4. Implement information security compliance enhancements	4.1 Implement and integrate required changes into organisations risk register and business continuity plans (BCP) 4.2 Establish and document performance measurement program and evaluate security effectiveness of implemented security controls 4.3 Submit documentation changes to required personnel 4.4 Obtain final task sign off from required personnel

Foundation Skills

This section describes language, literacy, numeracy and employment skills incorporated in the performance criteria that are required for competent performance.

SKILL	DESCRIPTION
Learning	Explores and incubates, new and innovative ideas, through unconstrained analysis and critical thinking, to develop and improve the organisation's goals
Oral communication	Articulates requirements and complex concepts using industry standard technical language intended for audience and environment
Reading	Organises, evaluates and critiques ideas, and information, from a wide range of complex texts
Writing	Prepares complex documentation detailing cloud security control and privacy mitigation and recommended enhancements using succinct language and logical structure

SKILL	DESCRIPTION
Planning and organising	- Plans strategic priorities and outcomes within a flexible, efficient and effective context, in a diverse environment, exposed to competing demands - Gathers and analyses data, and seeks feedback to improve plans and processes
Problem solving	- Makes high-impact decisions in a complex and diverse environment, using input from a range of sources - Identifies the key factors that impact on decisions and their outcomes, drawing on experience, competing priorities, and decision-making strategies, where appropriate
Self-management	- Works autonomously making high-level decisions to achieve, and improve, organisational goals - Develops and implements strategies, that confirms that organisational policies, procedures and regulatory requirements are being met
Technology	Demonstrates a sophisticated knowledge of principles, concepts, language and practices associated with the digital world

Unit Mapping Information

Supersedes and is equivalent to ICTNWK616 Manage security, privacy and compliance of cloud service deployment.

Links

Companion Volume Implementation Guide is found on VETNet -

<https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=a53af4e4-b400-484e-b778-71c9e9d6aff2>

Assessment Requirements for ICTCLD602 Manage information security compliance of cloud service deployment

Modification History

Release	Comments
Release 1	This version first released with ICT Information and Communications Technology Training Package Version 6.0.

Performance Evidence

The candidate must demonstrate the ability to complete the tasks outlined in the elements, performance criteria and foundation skills of this unit, including evidence of the ability to:

- identify, manage and implement cloud security controls and document requirements on at least one occasion.

Knowledge Evidence

The candidate must be able to demonstrate knowledge to complete the tasks outlined in the elements, performance criteria and foundation skills of this unit, including knowledge of:

- business and commercial issues relating cloud security management
- cloud shared security responsibility models
- legislation, organisational and jurisdictional policy and procedures that impact management areas including:
 - data privacy and sovereignty issues
 - codes of ethics and conduct
 - equal employment opportunity, equity and diversity principles
 - financial management requirements
 - governance requirements
- industry standard management tools and techniques suited to a range of complex project activities
- key organisational context, policies and procedures and required to manage information security compliance of cloud service deployment
- information security compliance standards, including ISO2700x
- information security compliance constructs, including risk, controls and risk mitigation.

Assessment Conditions

Skills in this unit must be demonstrated in a workplace or simulated environment where the conditions are typical of those in a working environment in this industry.

This includes access to:

- cloud information and communications technology (ICT) business specifications
- cloud ICT security assurance specifications
- cloud-focused security environment, including threats to security that are, or are held to be, present in the environment
- security environment information, including:
 - laws or legislation
 - existing enterprise security policies
 - enterprise expertise
- risk analysis tools and methodologies currently used in industry
- documented organisational work health safety (WHS) requirements.

Assessors of this unit must satisfy the requirements for assessors in applicable vocational education and training legislation, frameworks and/or standards.

Links

Companion Volume Implementation Guide is found on VETNet -

<https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=a53af4e4-b400-484e-b778-71c9e9d6aff2>