Australian Government

Department of Education, Employment and Workplace Relations

ICASAS507A Implement and evaluate systems for regulatory and standards compliance

Release: 1

ICASAS507A Implement and evaluate systems for regulatory and standards compliance

Modification History

Release	Comments
Release 1	This Unit first released with *ICA11 Information and Communications Technology Training Package version 1.0*

Unit Descriptor

This unit describes the performance outcomes, skills and knowledge required to implement and evaluate the application of the principles, policies and procedures that enable an enterprise to meet applicable information security laws, regulations and standards to satisfy statutory requirements, perform industry-wide best practices, and achieve its information security program goals.

Application of the Unit

This unit applies to staff in a range of IT areas responsible for ensuring that systems, networks and websites comply with laws, conform to best practices and organisational standards, and meet security requirements.

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

Element	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. Implement compliance systems	1.1 Monitor and assess the information security compliance practices of personnel according to enterprise policy and procedures 1.2 Maintain ongoing and effective communications with ***key compliance stakeholders*** 1.3 Conduct internal audits to determine if information security control objectives, controls, processes, and procedures are effectively applied and maintained, and perform as expected
2. Evaluate compliance systems	2.1 Assess the effectiveness of enterprise compliance program controls against ***appropriate benchmarks*** 2.2 Assess the effectiveness of information security compliance process and procedures for process improvement and implement changes where appropriate 2.3 Compile, analyse and report performance measures

Required Skills and Knowledge

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

Required skills

- communication skills to articulate complex security scenarios in a clear and concise manner, relevant to all levels of the organisation
- literacy skills to interpret current security standards
- planning and organisational skills to schedule internal audits
- research skills to monitor the latest security standards as well as industry best practice.

Required knowledge

- client business domain
- current industry-accepted hardware and software products, including security features and capabilities
- legislation relating to IT security
- operating system, including strengths and weaknesses over lifetime of product
- privacy issues and legislation relating to integrating legal requirements with IT security.

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: • monitor and assess information security compliance • conduct internal audits • assess the effectiveness of enterprise compliance • compile, analyse and report performance measures.
Context of and specific resources for assessment	Assessment must ensure access to: • IT business specifications • information on the security environment, including laws or legislation, existing organisational security policies, organisational expertise and knowledge • possible security environment, which includes threats to security that are, or are held to be, present in the environment • risk analysis tools and methodologies • IT security assurance specifications • 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:
	• verbal or written questioning to assess candidate's knowledge of:
	  • enterprise policies
	  • information security aims
	  • IT audits
	• review of candidate's documented performance measures
	• observation of candidate conducting an IT audit.

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.

Key compliance stakeholders may include:	• employees • external organisations • individuals • internal departments.
Appropriate benchmarks may include:	• applicable laws • policies • procedures • regulations • standards.

Unit Sector(s)

Systems administration and support