



Australian Government

ICTCYS606 Evaluate an organisation's compliance with cyber security standards and law

Release: 1

ICTCYS606 Evaluate an organisation's compliance with cyber security standards and law

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 identify cyber security standards and laws and evaluate an organisation's working practices and compliance to these standards and laws as well as determine changes required to continue compliance.

It applies to those who work in an internal audit function, including those who specialise in cyber security and compliance and are responsible for implementing and monitoring an organisation's compliance to cyber security standards and laws both locally and internationally.

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

Unit Sector

Cyber security

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. Research existing security standards and laws	1.1 Identify standards and laws required for organisations cyber security operations and summarise findings 1.2 Analyse and align required laws and standards to organisational cyber operations 1.3 Obtain and analyse organisation's existing cyber security compliance strategies and document outcomes according to organisational policies and procedures 1.4 Determine time periods and benchmarking of compliance evaluation requirements

2. Analyse compliance activities	2.1 Conduct compliance assessment according to organisational and legislative requirements 2.2 Document assessment findings according to organisational policies and procedures 2.3 Identify and document areas of non-compliance and near misses
3. Align organisation's activities to required standards	3.1 Develop and document all compliance requirements 3.2 Distribute requirements to required personnel in preparation to realign business activities to requirements 3.3 Develop an evaluation strategy according to organisational policies and procedures 3.4 Submit all documents to required personnel and seek and respond to feedback

Foundation Skills

This section describes those language, literacy, numeracy and employment skills that are essential to performance but not explicit in the performance criteria.

SKILL	DESCRIPTION
Learning	- Obtains information applicable to legislative requirements and organisational procedures and identity management standards and principles - Monitors outcomes of decisions, considering results and identifying key concepts and principles that may be adaptable in the future
Reading	Interprets information from different sources in a range of formats when identifying best practices and interpreting how these standards apply to the organisation
Writing	Uses industry specific terminology in documenting research findings, recommendations and best practice implementation
Planning and organising	Uses problem solving skills to identify anomalies and subtle deviations to normal expectations, focusing attention and remedying problems as they arise

Unit Mapping Information

No equivalent unit. New unit.

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 ICTCYS606 Evaluate an organisation's compliance with cyber security standards and law

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 cyber security standards and laws and analyse an organisation's operations and compliance to required laws and standards on at least one occasion.

In the course of the above, the candidate must:

- document processes and summarise findings.

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:

- security risks, and tolerance of risk in an organisation
- cyber security standards, regulations and laws applicable to the organisation
- organisational business processes and applicable cyber security requirements in each area
- principles of cyber security
- methods of identifying cyber security incidents
- different types of cyber security incidents including security vulnerabilities and malware.

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:

- standards outlining cyber security standards and laws applicable to the organisation
- software required to implement cyber security standards and laws.

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>