



Australian Government

ICTCYS608 Perform cyber security risk assessments

Release: 1

ICTCYS608 Perform cyber security risk assessments

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 conduct a risk assessment and analysis in a business environment. The risk assessment requires the identity and alignment of an organisation's operating environment to their required risk register and the realignment of their operations.

It applies to those who work in risk functions of an organisation, including ICT risk managers, cyber security engineers, network engineers, DevOps engineers and cyber security solutions architects, and are responsible for designing security solutions.

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. Prepare to perform risk assessment	1.1 Analyse organisations risk culture and document findings according to organisational requirements 1.2 Research and document legislative and organisational cyber security risk requirements 1.3 Obtain and analyse organisation's risk register and determine its currency against organisational legislative requirements 1.4 Develop and document risk assessment plan according to organisational requirements 1.5 Communicate risk assessment plan with required personnel and seek and respond to feedback

2. Perform risk assessment	2.1 Initiate risk assessment according to plan 2.2 Document process and outcomes of risk assessment according to organisational policies and procedures
3. Finalise risk assessment	3.1 Analyse and document findings against risk register and determine operations outside of organisation's risk appetite 3.2 Develop and document operational measures to align operations against risk register requirements 3.3 Communicate risk assessment findings to required personnel and highlight areas of non-compliance and solutions 3.4 Lodge documentation according to organisational requirements

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
Reading	Interprets and applies technical, legislative and organisational documentation to determine and confirm compliance and job requirements and compliance
Writing	Develops workplace and legal documentation for a specific audience, using detailed language to convey explicit information, requirements and recommendations
Planning and organising	Develops the operational detail in stages, regularly reviewing priorities and performance during assessment procedure, and identifies and addresses issues of non-compliance
Problem solving	Demonstrates an understanding of context to recognise 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 ICTCYS608 Perform cyber security risk assessments

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:

- conduct a cyber security risk assessment on at least one occasion.

In the course of the above, the candidate must:

- identify and analyse an organisation's risk appetite and risk register against their daily operations
- research cyber security legislation and align organisational risk assessment to require legislation
- document processes and outcomes.

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:

- risk assessment methodologies and processes required in cyber security
- methodologies of identifying and measuring risk culture and risk appetite in the cyber environment
- sources of legislative requirements required in cyber security
- organisational procedures applicable to conducting a cyber security risk assessment including,
- documenting risk assessment processes and findings
- establishing requirements and features of cyber security risk assessment processes.

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:

- software required to conduct a risk assessment
- legislative documentation required to conduct a cyber security risk assessment
- information applicable to organisational environment, culture and operations required to conduct a cyber security risk assessment.

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>