



Australian Government

PSPSEC011 Assess security risks

Release: 1

PSPSEC011 Assess security risks

Modification History

Release	Comments
1	This unit was released in PSP Public Sector Training Package release 1.0 and meets the Standards for Training Packages. This unit supersedes and is equivalent to PSPSEC501A Assess security risks. • Unit code updated • Content and formatting updated to comply with new standards • All PC transitioned from passive to active voice • PC 2.3 and 2.4; PC 3.2 and 3.3; PC 4.2, 4.3 and 4.4; PC 5.4 and 5.5 merged

Application

This unit describes the skills required to assess government security risks. It includes establishing the risk context, gathering and analysing information and identifying, analysing, assessing and prioritising risks.

This unit applies to those working to develop a security plan or implementing or following an existing plan.

The skills and knowledge described in this unit must be applied within the legislative, regulatory and policy environment in which they are carried out. Organisational policies and procedures must be consulted and adhered to, particularly those related to assessing security risks.

Those undertaking this unit would work independently, initiating support from a range of established and new resources while performing complex tasks in a range of unfamiliar and unfamiliar contexts.

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

Competency Field

Security

Elements and Performance Criteria

ELEMENTS	PERFORMANCE CRITERIA
Elements describe the essential outcomes	Performance criteria describe the performance needed to demonstrate achievement of the element. Where bold italicised text is used, further information is detailed in the range of conditions section.
1. Establish security risk context	1.1 Identify the scope and strategic and organisational contexts of the risk assessment. 1.2 Identify and comply with legislation, policies, procedures and guidelines related to security risk management. 1.3 Identify stakeholders and their expectations and obtain their input. 1.4 Identify security risk criteria. 1.5 Develop and obtain endorsement for a risk assessment plan according to organisational priorities.
2. Gather and analyse information	2.1 Identify sources and gather information. 2.2 Review relevant internal and historical information. 2.3 Aggregate and contextualise new information from internal and external sources. 2.4 Identify and address information gaps.
3. Identify security risks	3.1 Determine sources of threat to the organisation's resources and functions. 3.2 Conduct threat assessment against organisational policies, procedures and guidelines and determine risk exposure. 3.3 Use risk assessment techniques which suit the type and level of risk. 3.4 Determine and document risk potential.
4. Analyse security risks	4.1 Analyse potential consequences of risks or threats in light of potential damage to agency, including critical lead time for recovery. 4.2 Assess intent, capability and opportunity for each risk or threat to occur, using all available information. 4.3 Analyse current security countermeasures and treatment options to determine areas of vulnerability. 4.4 Determine and document risk ratings in agreed format.
5. Assess and prioritise security risks	5.1 Consult stakeholders regarding acceptable and unacceptable risk levels. 5.2 Document acceptable and unacceptable levels of risk. 5.3 Compare identified risks with security risk criteria to determine whether they are acceptable or unacceptable. 5.4 Prioritise and document identified risks in accordance with

	security criteria. 5.5 Document determined residual risks.
--	---

Foundation Skills

The foundation skills demands of this unit have been mapped for alignment with the Australian Core Skills Framework (ACSF). The following tables outline the performance levels indicated for successful attainment of the unit.

ACSF levels indicative of performance:

1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
Learning					Reading					Writing					Oral communication					Numeracy				

Performance variables:

1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
Support					Context					Text complexity					Task complexity				

Further information on ACSF and the foundation skills underpinning this unit can be found in the Foundation Skills Guide on the GSA website.

Unit Mapping Information

This unit supersedes and is equivalent to PSPSEC501A Assess security risks.

Links

Companion Volume implementation guides are found in VETNet -

<https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=bebbece7-ff48-4d2c-8876-405679019623>

Companion Volume implementation guides are found in VETNet -

<https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=bebbece7-ff48-4d2c-8876-405679019623>

Companion Volume implementation guides are found in VETNet -

<https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=bebbece7-ff48-4d2c-8876-405679019623>

Companion Volume implementation guides are found in VETNet -

<https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=bebbece7-ff48-4d2c-8876-405679019623>

Assessment Requirements for PSPSEC011 Assess security risks

Modification History

Release	Comments
1	These Assessment Requirements were released in PSP Public Sector Training Package release 1.0 and meet the Standards for Training Packages. Assessment Requirements created drawing upon specified assessment information from superseded unit

Performance Evidence

Evidence required to demonstrate competence must satisfy all of the requirements of the elements and performance criteria. If not otherwise specified the candidate must demonstrate evidence of performance of the following on at least two occasions.

- applying legislation, regulations and policies relating to security risk management
- undertaking risk assessment
- reading and analysing the complex information in standards and security plans
- researching and analysing the operational environment and drawing accurate conclusions
- applying critical analysis, evaluation and deductive reasoning
- using problem solving and creative thinking in decision making
- communicating with diverse stakeholders: interviewing, listening, questioning, paraphrasing, clarifying, summarising
- writing reports requiring formal language and structure
- using computer technology and modelling to gather and analyse information and prepare reports
- representing numerical, graphical and statistical information in diverse formats

Knowledge Evidence

- Operational knowledge of:
 - public service Acts
 - Crimes Act 1914 and Criminal Code 1985
 - Freedom of Information Act 1982
 - Privacy Act 1988
 - fraud control policy
 - protective security policy
 - Australian Government Information Security Manual (ISM)

- Protective Security Policy Framework
- Australian standards, quality assurance and certification requirements
- Complex knowledge of:
 - risk assessment techniques/processes
 - information handling
 - qualitative and quantitative analysis techniques
 - incident reports and statistics
 - asset holdings and recording mechanisms
 - international treaties and protocols
 - cross-jurisdictional protocols
 - organisation's strategic objectives
 - national strategic objectives
 - requirements of user groups

Assessment Conditions

Assessment of this unit requires evidence gathered over time in a workplace environment or one that closely resembles normal work practice and replicates the diverse conditions likely to be encountered when assessing security risks

Assessors must satisfy the NVR/AQTF mandatory competency requirements for assessors.

Links

Companion Volume implementation guides are found in VETNet -

<https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=bebbece7-ff48-4d2c-8876-405679019623>

Companion Volume implementation guides are found in VETNet -

<https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=bebbece7-ff48-4d2c-8876-405679019623>

Companion Volume implementation guides are found in VETNet -

<https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=bebbece7-ff48-4d2c-8876-405679019623>