Australian Government
Department of Education, Employment and Workplace Relations

PSPSEC501A Assess security risks

Release 3

INDUSTRY SKILLS COUNCILS
Creating Australia's Future

PSPSEC501A Assess security risks

Modification History

Release	TP Version	Comments
3	PSP12V1	Unit descriptor edited.
2	PSP04V4.2.	Layout adjusted. No changes to content.
1	PSP04V4.1	Primary release.

.

Unit Descriptor

This unit covers assessment of government security risks. It includes establishing the risk context, gathering and analysing information, identifying and analysing risks, and assessing and prioritising risks to underpin development of a security plan, which is covered in unit *PSPSEC502A Develop security risk management plans*.

In practice, assessment of security risks may overlap with other generalist or specialist public sector work activities such as acting ethically, promoting compliance with legislation, developing client services, undertaking research and analysis.

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

Application of the Unit

Not applicable.

Licensing/Regulatory Information

Not applicable.

Pre-Requisites

Not applicable.

Employability Skills Information

This unit contains employability skills.

Elements and Performance Criteria Pre-Content

Elements are the essential outcomes of the unit of competency.	Together, performance criteria specify the requirements for competent performance. Text in ***bold italics*** is explained in the Range Statement following.

Elements and Performance Criteria

ELEMENT	PERFORMANCE CRITERIA
1. Establish security risk context	1.1 The scope of the risk assessment and its ***strategic*** and ***organisational context*** are identified in accordance with organisational requirements. 1.2 ***Legislation, policies, procedures and guidelines*** related to security risk management are identified and complied with. 1.3 ***Stakeholders*** are identified and their expectations and input are obtained in accordance with organisational policy and procedures. 1.4 ***Security risk criteria*** are identified in accordance with the organisation's security policy, ***jurisdictional policies and legislation***. 1.5 A ***risk assessment plan*** is developed in accordance with organisational priorities, and endorsement is obtained.
2. Gather and analyse information	2.1 Sources of ***information*** are identified and information is gathered in accordance with organisational policy and procedures. 2.2 Internal information including historical information is reviewed. 2.3 New information from internal/external sources is aggregated. 2.4 Information is contextualised to the organisational context. 2.5 Gaps in information are identified and addressed.
3. Identify security risks	3.1 ***Sources of threat*** to the organisation's ***resources*** and functions are identified, and ***threats/potential threats*** are determined in accordance with organisational policy and procedures. 3.2 ***Threat assessment*** is conducted against organisational policies, procedures and guidelines. 3.3 Access to, availability of and procedures relating to resources/areas are analysed to determine ***risk exposure***. 3.4 Risks are assessed using ***risk assessment techniques*** to suit the type and level of risk in accordance with organisational policy and procedures. 3.5 Risk potential is determined and risks are documented in accordance with organisational requirements.
4. Analyse security risks	4.1 Potential ***consequences*** of risks/threats are analysed in light of potential damage to agency, including ***critical lead time for recovery***. 4.2 Analysis techniques are used in accordance with organisational policy and procedures. 4.3 Intent, capability and opportunity for each risk/threat to occur are assessed. 4.4 Using all known information, ***likelihood of risks***/threats occurring is assessed. 4.5 Current security countermeasures/treatment options are

ELEMENT	PERFORMANCE CRITERIA
	analysed to determine areas of vulnerability. 4.6 ***Risk ratings*** are determined and documented in agreed ***format*** using all known information.
5. **Assess and prioritise security risks**	5.1 Stakeholders are consulted about acceptable/unacceptable risk levels. 5.2 ***Acceptable/unacceptable*** levels of risk are documented. 5.3 Identified risks are compared with security risk criteria to determine whether they are acceptable/unacceptable. 5.4 Identified risks are prioritised in accordance with security criteria. 5.5 Risks are documented in priority order in accordance with organisational policies, procedures and guidelines. 5.6 ***Residual risks*** are determined and documented in accordance with organisational policies, procedures and guidelines.

Required Skills and Knowledge

This section describes the essential skills and knowledge and their level, required for this unit.

Skill requirements
Look for evidence that confirms skills in:

- applying legislation, regulations and policies relating to security risk management
- undertaking risk assessment
- reading and analysing the complex information in standards, legislation and security plans
- researching and analysing the operational environment and drawing conclusions
- applying critical analysis, evaluation and deductive reasoning
- using problem solving and decision making
- using creative thinking
- communicating with diverse stakeholders involving interviewing, listening, questioning, paraphrasing, clarifying, summarising
- responding to diversity, including gender and disability
- writing reports requiring formality of language and structure
- using computer technology to gather and analyse information, and prepare reports
- using computer modelling
- using numerical, graphical and statistical information
- representing mathematical information in a range of formats to suit the information and the purpose
- responding to diversity, including gender and disability
- applying procedures relating to occupational health and safety and environment in the context of security risk management

Knowledge requirements
Look for evidence that confirms knowledge and understanding of:

- legislation, regulations, policies, procedures and guidelines relating to security risk management such as:
  - occupational health and safety
  - 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
- risk assessment techniques/processes
- information handling
- qualitative and quantitative analysis techniques
- incident reports and statistics
- asset holdings and recording mechanisms
- Australian standards, quality assurance and certification requirements
- international treaties and protocols
- cross-jurisdictional protocols
- organisation's strategic objectives
- national strategic objectives
- requirements of user groups
- equal employment opportunity, equity and diversity principles
- public sector legislation such as occupational health and safety and environment in the context of security risk assessment

Evidence Guide

The Evidence Guide specifies the evidence required to demonstrate achievement in the unit of competency as a whole. It must be read in conjunction with the Unit descriptor, Performance Criteria, the Range Statement and the Assessment Guidelines for the Public Sector Training Package.

Units to be assessed together

- *Pre-requisite* units that must be achieved prior to this unit:*Nil*
- *Co-requisite* units that must be assessed with this unit:*Nil*
- *Co-assessed units* that may be assessed with this unit to increase the efficiency and realism of the assessment process include, but are not limited to:
    - PSPETHC501B Promote the values and ethos of public service
    - PSPGOV502B Develop client services
    - PSPGOV504B Undertake research and analysis
    - PSPLEGN501B Promote compliance with legislation in the public sector
    - PSPSEC502A Develop security risk management plans
    - PSPSEC503A Implement and monitor security risk management plans

Overview of evidence requirements

In addition to integrated demonstration of the elements and their related performance criteria, look for evidence that confirms:

- the knowledge requirements of this unit
- the skill requirements of this unit
- application of the Employability Skills as they relate to this unit (see Employability Summaries in Qualifications Framework)
- assessment of security risks in a range of (3 or more) contexts (or occasions, over time)

Resources required to carry out assessment

These resources include:

- legislation, policy, procedures and protocols relating to the assessment of security risk
- Australian Government Information Manual (ISM)
- Protective Security Policy Framework
- case studies and workplace scenarios to capture the range of situations likely to be encountered when assessing security risks

Where and how to assess evidence

Valid assessment of this unit requires:

- a workplace environment or one that closely resembles normal work practice and replicates the range of conditions likely to be encountered when assessing security risks, including coping with difficulties, irregularities and breakdowns in routine

- assessment of security risks in a range of (3 or more) contexts (or occasions, over time)

Assessment methods should reflect workplace demands, such as literacy, and the needs of particular groups, such as:

- people with disabilities
- people from culturally and linguistically diverse backgrounds
- Aboriginal and Torres Strait Islander people
- women
- young people
- older people
- people in rural and remote locations

Assessment methods suitable for valid and reliable assessment of this competency may include, but are not limited to, a combination of 2 or more of:

- case studies
- portfolios
- questioning
- scenarios
- simulation or role plays
- authenticated evidence from the workplace and/or training courses, such as risk assessment plan

For consistency of assessment

Evidence must be gathered over time in a range of contexts to ensure the person can achieve the unit outcome and apply the competency in different situations or environments

Range Statement

The Range Statement provides information about the context in which the unit of competency is carried out. The variables cater for differences between States and Territories and the Commonwealth, and between organisations and workplaces. They allow for different work requirements, work practices and knowledge. The Range Statement also provides a focus for assessment. It relates to the unit as a whole. Text in ***bold italics*** in the Performance Criteria is explained here.

Strategic context may include:

- the relationship between the organisation and the environment in which it operates
- the organisation's functions:
  - political
  - operational
  - financial
  - social
  - legal
  - commercial
  - the various stakeholders and clients

Organisational context may include:

- the organisation, how it is organised, and its capabilities
- any official resources, including physical areas and assets, that are vital to the operation of the organisation
- key operational elements of the organisation
- any major projects

Legislation, policies procedures and guidelines may include:

- Commonwealth and State/Territory legislation relating to security
- national and international codes of practice and standards
- the organisation's policies and practices
- jurisdictional policies
- codes of conduct/codes of ethics
- AS/NZS ISO 31000:2009 Risk management - Principles and guidelines
- Australian Government Information Security Manual (ISM)
- Protective Security Policy Framework

Stakeholders may include:

- supervisors
- managers
- other areas within the organisation
- other organisations
- government
- third parties

Security risk criteria may

- vital functions and capabilities

concern:	• the expectations of stakeholders and clients • the personal security of employees and clients • general expectations about confidentiality • the availability of the organisation's official resources

Jurisdictional policies and legislation relating to risk criteria cover:

- expectations about the care and confidentiality of official information reflected in legislation such as Public Service Act 1999, Crimes Act 1914 and Criminal Code 1985
- the availability of official information to the public (Freedom of Information Act 1982)
- expectations about the collection, use and care of personal information (the Privacy Act 1988)
- expectations about the well-being and personal security of staff (Occupational Health and Safety [Commonwealth Employment] Act 1991)
- the measures and procedures agencies must adopt to protect official resources from fraud (Commonwealth fraud control policy)
- the expectation that there will be a Commonwealth-wide system for providing appropriate protection to security classified information (Commonwealth protective security policy)

Risk assessment plan will include:

- the strategic and organisational context of the agency (or organisation, area or project under review)
- the scope and objectives of the review
- information and resources required to complete the review
- the security risk criteria

Information may be:

- hardcopy
- audio-visual
- electronic

Sources of threat may include:

- people
- systems
- environmental
- financial
- natural
- conflict
- terrorism
- political circumstances
- internal
- external
- local
- national
- international

Resources may be:

- agency owned
- contractor owned
- hired

- leased
- owned by third parties

Threats/potential threats may be:

- internal
- external
- national
- international
- real
- perceived
- to:
  - people
  - property
  - information
  - reputation
  - criminal
  - terrorist
- from foreign intelligence services
- from commercial/industrial competitors
- from malicious people

Threat assessment:

- is used to provide information about people and events that may pose a risk to a particular resource or function
- evaluates and discusses the likelihood of a threat being realised
- determines the potential of a threat to actually cause harm

Risk exposure is:

- a measure of how open a resource is to harm, or
- the potential of a resource to attract harm

Risk assessment techniques may include:

- qualitative and/or semi-quantitative and/or quantitative
- brainstorming
- focus groups
- expert judgment
- strengths, weaknesses, opportunities and threats (SWOT) analysis
- analysis of risk registers
- examination of available data such as audit results, incident reports
- nomogram
- risk matrix
- scenario analysis
- business continuity planning

Consequences may include:

- degree of harm
- who would be affected and how
- how much disruption would occur

- damage to:
  - the organisation
  - other organisations
  - government
  - third parties
- critical lead time for recovery

Critical lead time for recovery is

- the period of time a function is compromised
- critical if the function is vital to the organisation

Likelihood of risk may be determined through analysis of:

- current controls to deter, detect or prevent harm
- effectiveness of current controls
- level of exposure
- threat assessment
- determination of threat source/s
- competence/capability of threat source/s
- opportunity for threat to occur

Risk ratings may include:

- severe
- high
- major
- significant
- moderate
- low
- trivial

Format for risk documentation may include:

- matrix
- table
- graphs
- graphics
- computer modelling

Acceptable risks are:

- those which an organisation has determined have the least potential for harm

Unacceptable risks are:

- those which an organisation has determined have the most potential for harm

Residual risks are:

- those which cannot be treated but still need to be documented

Unit Sector(s)

Not applicable.

Competency field

Government Security Management.