Australian Government

Department of Education, Employment and Workplace Relations

PSPSEC502A Develop security risk management plans

Release 3

INDUSTRY SKILLS COUNCILS
Creating Australia's Future

PSPSEC502A Develop security risk management plans

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 planning to treat security risks through the development of a security risk management plan. It includes identifying security countermeasures and developing a formal security plan.

In practice, development of a security risk management plan 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. Identify countermeasures	1.1 Documented ***risks/threats are reviewed*** and management decisions on ***acceptable*** and ***unacceptable*** risks are confirmed. 1.2 ***Treatment options/countermeasures*** are determined that are consistent with organisational policies, procedures and guidelines to reduce the ***likelihood*** of occurrence or the ***consequences*** of the risk, or both. 1.3 Treatments include ***continuity plans***, where appropriate, in accordance with organisational policy and procedures. 1.4 Treatments match the ***level*** and type of risk and the importance of the function or resource. 1.5 A ***cost-benefit analysis*** is conducted to determine cost-effective countermeasures. 1.6 ***Stakeholders*** are consulted on the cost-benefit analysis, and countermeasures are determined and submitted for decision/prioritising in accordance with organisational policy and procedures.
2. Develop security plan	2.1 Security plan is prepared in accordance with organisational policy and procedures. 2.2 The plan contains explanatory information on the importance of security and the organisation's security objectives in achieving corporate and business objectives. 2.3 The plan summarises ***threat assessments*** undertaken, current ***exposure*** and current protective security arrangements. 2.4 The plan outlines security strategies for implementation of countermeasures, monitoring and evaluation. 2.5 The plan includes a timetable and security budget for implementation of countermeasures including how they will be implemented and by whom. 2.6 Security plan is submitted for approval and communicated to stakeholders in accordance with organisational policy and procedures.

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 plans
- using evaluation and deductive reasoning
- undertaking problem solving and decision making
- using communication with diverse stakeholders involving presentation, listening, questioning, paraphrasing, clarifying, summarising
- reading and analysing the complex information in standards, legislation and security plans
- writing reports requiring formality of language and structure
- using computer technology to gather and analyse information, and prepare reports
- 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 developing security risk management plans

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
- Australian standards, quality assurance and certification requirements
- international treaties and protocols
- cross-jurisdictional protocols
- organisation's strategic objectives

- national strategic objectives
- formats for different types of reports
- cost-benefit analysis techniques
- 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
  - PSPSEC501A Assess security risks
  - 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)
- security risk management plans developed in a range of (2 or more) contexts (or occasions, over time)

Resources required to carry out assessment

These resources include:

- legislation, policy, procedures and protocols relating to security risk management plans
- 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 developing security risk management plans

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 developing security risk management plans, including coping with difficulties, irregularities and breakdowns in routine

- security risk management plans developed in a range of (2 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 security risk management 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.

Risks/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

Risk review includes:

- consideration of current and historical information

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

Treatment options may include:

- addition of security measures
- reduction of security measures
- avoiding the risk through change of practice
- acceptance of residual risk
- minimisation of harm through response mechanisms
- accepting the risk

Countermeasures may include:

- revision of agency security plan
- upgrade of existing security
- installation of new security measures
- technical controls

- training
- personnel-oriented
- information-oriented
- property-oriented
- reputation-oriented

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

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

Continuity plans:

- may lessen the adverse consequences of risk
- provide a set of planned procedures that enable organisations to continue or recover services to the government and the public with minimal disruption over a given period, irrespective of the source of the disruption

Level of risk may be:

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

Cost-benefit analysis may be against:

- existing requirements
- future requirements
- forecast requirements

Stakeholders may include:

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

- workgroup

Threat assessment:

- is used to provide information about people and events that may pose a threat 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

Unit Sector(s)

Not applicable.

Competency field

Government Security Management.