



Australian Government

Department of Education, Employment and Workplace Relations

PSPSEC402A Implement security risk treatments

Revision Number: 3

PSPSEC402A Implement security risk treatments

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 identification and implementation of security risk treatments. It includes confirming risk decisions identifying security risk treatment options, implementing countermeasures, and monitoring and reviewing the security risk management process. Depending on the size of the organisation, work may be in a discrete area such as information technology or across all areas within the organisation.

In practice, implementation of security risk treatments may overlap with other generalist or specialist public sector work activities such as working ethically, complying with legislation, applying government processes, gathering and analysing information, exercising regulatory powers.

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. Confirm risk decisions	1.1 Management decisions determining acceptable and unacceptable risks are confirmed in accordance with organisational policy and procedures. 1.2 Low-level risks that the organisation decides to accept are noted and monitored to detect changed circumstances . 1.3 Unacceptable high-level risks are referred for the development of formal management plans. 1.4 Major or significant risks identified as unacceptable are noted for treatment.
2. Identify risk treatments	2.1 Treatments are determined that are consistent with organisational policies, procedures and guidelines and the organisation's security plan. 2.2 Treatments are determined that are cost-effective and match the level and type of risk and the importance of the function or resource. 2.3 Treatments are selected to reduce the likelihood of occurrence or the consequences of the risk, or both. 2.4 Continuity plans are included in treatments, where appropriate, in accordance with the security plan. 2.5 Treatments are documented and submitted for approval in accordance with organisational policy and procedures.
3. Implement countermeasures	3.1 A treatment plan is developed and implemented in accordance with organisational policy and procedures. 3.2 Implementation of countermeasures is undertaken in accordance with the implementation strategy detailed in the security plan. 3.3 Countermeasures are implemented in accordance with timeframe and budgetary requirements. 3.4 Countermeasures are implemented in accordance with legal requirements, government and organisational policy.
4. Monitor and review security risk management process	4.1 Strategies to monitor risk environment are implemented. 4.2 Monitoring is conducted on a regular basis in accordance with organisational policy and procedures. 4.3 Risk treatments are evaluated against the objectives of the security plan to ensure these remain effective and/or necessary. 4.4 Feedback is obtained from stakeholders on the adequacy and need for current security measures affecting their work/area. 4.5 Recommendations for re-examination of security risk or improved risk treatments are conveyed to the appropriate personnel 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 government security management
- reading and analysing the organisation's security plan
- observing and critically analysing the application of security risk treatments in an operational environment
- engaging in communication with diverse stakeholders involving 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
- representing mathematical information in a range of formats to suit the information and the purpose
- applying procedures relating to occupational health and safety and environment in the context of government security management

Knowledge requirements

Look for evidence that confirms knowledge and understanding of:

- legislation, regulations, policies, procedures and guidelines relating to government security 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 analysis terminology and techniques
 - the organisation's security plan
 - the organisation's assets and security environment
 - Australian standards, quality assurance and certification requirements
 - AS/NZS ISO 31000:2009 Risk Management - Principles and Guidelines
- public sector legislation such as equal employment opportunity, and equity and diversity principles applied in the context of government security

management

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:
 - PSPETHC401A Uphold and support the values and principles of public service
 - PSPGOV406B Gather and analyse information
 - PSPGOV422A Apply government processes
 - PSPLEGN401A Encourage compliance with legislation in the public sector
 - PSPREG401C Exercise regulatory powers

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)
- implementation of security risk treatments 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 implementation of security risk treatments
- organisational standards and documentation
- case studies and workplace scenarios to capture the range of situations likely to be encountered when implementing security risk treatments

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 implementing security risk treatments, including coping with difficulties, irregularities and breakdowns in routine

- implementation of security risk treatments 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
- authenticated evidence from the workplace and/or training courses, such as a 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.

Risk may be to:

- personnel
- information
- property
- reputation

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

Sources of security risk may include:

- technical
- actual events
- political circumstances
- human behaviour
- environmental
- conflict
- terrorism
- internal
- external
- local
- national
- international

Level of risk may be:

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

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

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 and intent) of threat source/s

Consequences may include:

- what constitutes harm
- degree of harm
- who would be affected and how
- how much disruption would occur
- levels that are:
 - extreme
 - very high
 - medium
 - low
 - negligible

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

Treatment plans may include:

- responsibilities
- schedules
- expected outcomes
- budget information
- performance measures
- monitoring process

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

Legal requirements, government and organisational policy

- Commonwealth and State/Territory legislation including equal employment opportunity, occupational health and safety, privacy and anti-discrimination law

may include:

- access and equity
- ethics and accountability
- national and international codes of practice and standards
- the organisation's policies and practices
- government policy
- codes of conduct/codes of ethics
- Australian Government Information Security Manual (ISM)
- Protective Security Policy Framework
- AS/NZS ISO 31000:2009 Risk management - Principles and Guidelines

Strategies may include:

- audits
- incident reporting mechanisms
- technical controls
- systems
- rosters
- access controls
- training

Monitoring may include:

- regular checking
- critical observation
- regular recording
- information, such as threat assessments, from senior management
- reports from business units on current security measures
- identification of changes over time such as:
 - notification of major changes to business or corporate goals or plans
 - notification of key projects

Stakeholders may include:

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

Unit Sector(s)

Not applicable.

Competency field

Government Security Management.