Australian Government

Department of Education, Employment and Workplace Relations

PSPSEC503A Implement and monitor security risk management plans

Revision Number: 2

PSPSEC503A Implement and monitor security risk management plans

Modification History

PSPSEC503A Release 2: Layout adjusted. Required Knowledge, Range Statement and Evidence Guide updated.
PSPSEC503A Release 1: Primary release.

Unit Descriptor

This unit covers implementation and monitoring of security risk management plans. It includes implementing a security plan, monitoring the risk environment and evaluating the security plan.
In practice, implementation and monitoring of security risk management plans 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, etc.

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. Implement security plan	1.1 ***Security risks*** are treated/***countermeasures*** are implemented in accordance with the security plan.
	1.2 Security plan is implemented to meet timeframe and budgetary requirements.
	1.3 Countermeasures are implemented in compliance with ***legal requirements***, ***government and organisational policy***.
	1.4 ***Residual risks*** are documented and monitored.
2. Monitor the risk environment	2.1 ***Strategies*** to monitor the risk environment are determined and documented.
	2.2 Security risks, and the ***type/s*** and ***source/s*** of threats are monitored to detect changing circumstances that may alter risk management priorities.
	2.3 ***Monitoring*** is conducted on a regular basis in accordance with organisational policy and procedures.
	2.4 Changes to the organisation are monitored to identify circumstances where re-examination of the security environment becomes necessary.
	2.5 Results of monitoring are documented and acted on.
3. Evaluate security plan	3.1 ***Risk treatments*** are monitored to gauge whether they are being implemented properly and fully.
	3.2 Treatments are evaluated against the objectives of the security plan to ensure they remain effective and/or necessary.
	3.3 Feedback is obtained from ***stakeholders*** on the adequacy and need for current security measures affecting their work area.
	3.4 Weaknesses in the security plan are identified and addressed in accordance with organisational policy and procedures.
	3.5 Security plan is reviewed on an on-going basis, as a result of incidents, breaches, and changes in circumstances.
	3.6 Security plan is updated in accordance with organisational policies, procedures and guidelines to reflect current circumstances.

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
- auditing in the context of security risk management
- communicating with diverse stakeholders involving interviewing, negotiating, conflict resolution, 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
- undertaking statistical analysis
- responding to diversity, including gender and disability
- applying procedures relating to occupational health and safety and environment in the context of implementing and monitoring 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
- security plan
- organisation's strategic objectives
- national strategic objectives
- security constraints
- equal employment opportunity, equity and diversity principles
- public sector legislation such as occupational health and safety and environment in the context of implementation and monitoring of security risk management plans

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

PSPSEC502A Develop 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 implemented and monitored 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 Security Manual (ISM)
- Protective Security Policy Framework
- case studies and workplace scenarios to capture the range of situations likely to be encountered when implementing and monitoring 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 implementing and monitoring security risk management plans, including coping with difficulties, irregularities and breakdowns in routine

- security risk management plans implemented and monitored 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
- authenticated evidence from the workplace and/or training courses, such as a reviewed security 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/or 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.

Security risks may include:

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

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 may include:

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

- AS/NZS ISO 31000:2009 Risk management - Principles and Guidelines
- Australian Government Information Security Manual (ISM)
- Protective Security Policy Framework

Residual risks are:
- those that cannot be treated

Strategies may include:
- audits
- incident reporting mechanisms
- technical controls
- systems
- rosters
- access controls
- training

Type of risk may include:
- severe
- high
- major
- significant
- moderate
- low
- trivial

Sources of threats may include:
- technical
- actual events
- political circumstances
- human behaviour
- environmental
- conflict
- terrorism
- internal
- external
- local
- national
- international

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

Risk treatments 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
Stakeholders may include:	• supervisors • managers • other areas within the organisation • other organisations • government • third parties • external contractors

Unit Sector(s)

Not applicable.

Competency field

Government Security Management.