Australian Government

Department of Education, Employment and Workplace Relations

PSPSEC401A Undertake government security risk analysis

Revision Number: 1

PSPSEC401A Undertake government security risk analysis

Modification History

Not applicable.

Unit Descriptor

Unit descriptor

This unit covers work at an operational level, to analyse risk against the organisation's security plan. It includes establishing the security risk context; identifying, analysing and evaluating risk against the organisation's security plan; and compiling of a security risk register. 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.

Implementation of risk treatment options and countermeasures are not included. This is covered in the unit *PSPSEC402A Implement security risk treatments*.

In practice, undertaking government security risk analysis 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, etc.

This is a new unit of competency, added to the *Government Security Management* Competency field of the Training Package in 2004.

Application of the Unit

Not applicable.

Licensing/Regulatory Information

Not applicable.

Pre-Requisites

Not applicable.

Employability Skills Information

Employability skills 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 *Strategic* and *organisational contexts* are confirmed in accordance with the organisation's security plan
	1.2 *Stakeholders* are identified and their expectations and input are gathered in accordance with *legislation, policy and procedures*
	1.3 *Security risk criteria* are identified from the security plan and confirmed as current and relevant
	1.4 Information and resources are obtained to conduct the risk analysis in accordance with organisational policy and procedures
2. Identify security risk	2.1 *Sources* of security risk are identified and recorded in accordance with organisational policy and procedures
	2.2 Risks are identified using a *specified methodology or tools* in accordance with the security plan
	2.3 Sources of risk are identified from the perspective of all stakeholders
	2.4 Stakeholders are consulted during the risk identification process to finalise a list of risks
3. Analyse security risk	3.1 *Threat assessments*, current *exposure* and current security arrangements are identified in accordance with the security plan to estimate the *likelihood* of each risk event occurring
	3.2 Potential *consequences* of each risk are determined in accordance with the security plan, including *critical lead time for recovery*
	3.3 *Risk ratings* are determined, documented and communicated in accordance with the security plan and organisational standards
	3.4 A rationale for each risk rating is included in accordance with organisational requirements
4. Evaluate security risk	4.1 Risks are assessed against the organisation's security risk criteria
	4.2 Risks are prioritised for treatment in accordance with the security plan
	4.3 Risks are monitored in accordance with the security plan until treatment measures have been implemented
5. Compile security risk register	5.1 A *security risk register* is developed that records identified risks, their nature and source
	5.2 The consequences and likelihood of risks, and the adequacy of existing controls are identified in the register
	5.3 Risk ratings are recorded for identified risks in accordance with organisational procedures
	5.4 The security risk register is compiled to meet organisational

ELEMENT	PERFORMANCE CRITERIA
	standards for content, format and presentation and reflects changes in circumstances
	5.5 Risk register is referred to management for decision on which risks will be accepted and which will require treatment

Required Skills and Knowledge

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

researching and critically analysing the operational environment and drawing conclusions

using effective communication with diverse stakeholders involving listening, questioning, paraphrasing, clarifying, oummarizing

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

Security Guidelines for Australian Government IT Systems (ACSI 33)

Commonwealth Protective Security Manual

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 4360:1999

REQUIRED SKILLS AND KNOWLEDGE

public sector legislation such as equal employment opportunity, and equity and diversity principles applied in the context of government security management

Evidence Guide

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* unitsthat must be achieved prior to this unit:*Nil*
- *Co-requisite* unitsthat 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)
- government security risk analysis 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 government security management
- organisational standards and documentation
- tools and methods used in the organisation for security risk analysis
- case studies and workplace scenarios to capture the range of situations likely to be encountered when undertaking government security risk analysis

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 undertaking government security risk

EVIDENCE GUIDE

analysis, including coping with difficulties, irregularities and breakdowns in routine

- government security risk analysis 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
- projects
- questioning
- scenarios
- simulation or role plays
- authenticated evidence from the workplace and/or training courses, such as security risk register

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

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 *italics* in the Performance Criteria is explained here.

Strategic context may include	• the relationship between the organisation and the environment in which it operates • organisational structure • 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
Stakeholders may include	• all those individuals and groups both inside and outside the organisation that have some direct interest in the organisation's behaviour, actions, products and services such as: • employees at all levels of the organisation • community • clients • other public sector organisations • union and association representatives • boards of management • government • Ministers
Legislation, policy and procedures may include	• Commonwealth and State/Territory legislation including equal employment opportunity, occupational health and safety, privacy and anti-discrimination law • national and international codes of practice and standards • the organisation's policies and practices • government policy

RANGE STATEMENT

	• codes of conduct/codes of ethics • Security Guidelines for Australian Government IT Systems (ACSI 33) • Commonwealth Protective Security Manual • Australian and New Zealand standards - Risk management AS/NZS 4360:1999
Security risk criteria may concern	• vital functions and capabilities • 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
Risk may be to	• personnel • information • property • reputation
Sources of security risk may include	• technical • actual events • political circumstances • human behaviour • environmental • conflict • terrorism • internal • external • local • national • international
Specified methodology or tools may be	• qualitative and/or semi-quantitative and/or quantitative • brainstorming • focus groups • expert judgment • strengths, weaknesses, opportunities, 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
Threat assessment	• is used to provide information about people and events that may

RANGE STATEMENT

	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
Threats may be	• criminal • terrorist • from foreign intelligence services • from commercial/industrial competitors • from malicious people • real or perceived
Risk exposure is	• a measure of how open a resource is to harm, or • the potential of a resource to attract harm
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 is	• the period of time a function is compromised • critical if the function is vital to the organisation
Risk ratings may include	• severe • high • major • significant • moderate • low • trivial
Security risk register may include	• source • nature • existing controls • likelihood

RANGE STATEMENT

- consequences
- initial rating
- vulnerability

Unit Sector(s)

Not applicable.

Competency field

Competency field Government Security Management