



Australian Government

Department of Education, Employment and Workplace Relations

PSPSEC504A Coordinate protective security

Release 3

PSPSEC504A Coordinate protective security

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 the requirements for those with day-to-day responsibility for performance of an organisation's protective security function. It includes providing advice and support to others, monitoring and coordinating security, and liaising with specialist security services. In practice, coordination of protective security may overlap with other generalist or specialist public sector work activities such as acting ethically, promoting compliance with legislation, developing client services, assessing security risk, communicating security awareness. 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. Provide security advice and support

- 1.1 Assistance is provided to management to analyse the security environment and plan to counter potential **threats**.
- 1.2 Advice is provided to management on **physical** and **procedural security measures** in accordance with organisational circumstances.
- 1.3 Assistance is provided in the development of the organisation's security policy and procedures in consultation with management and staff.
- 1.4 Promotion as the first point of contact for security concerns and queries is undertaken within the organisation in accordance with organisational requirements.
- 1.5 Advice is provided on **security matters** in accordance with legislation and **security standards**.

2. Coordinate and monitor security

- 2.1 Protective security arrangements are developed and implemented in conjunction with senior management to create and maintain a secure environment for official information and resources.
- 2.2 Devolved security measures are coordinated/overseen to ensure organisational standards are maintained in a cost-effective and consistent way.
- 2.3 The organisation's security procedures and systems are monitored in an ongoing manner and audited as required in accordance with the organisation's security policy and plan.
- 2.4 Monitoring is undertaken to ensure that employees and contractors are aware of their security responsibilities and obligations, and recommendations are prepared/actions are taken to address any gaps.
- 2.5 **Security incident** reports are reviewed and the implications are assessed for security risk, security procedures and security awareness training.

3. Access security specialists

- 3.1 Contact between the organisation and external **security authorities/organisations** is coordinated in accordance with organisational policy and procedures.
- 3.2 Specialist security organisations are contacted for advice, technical assistance, learning and development to ensure compliance with jurisdictional and organisational security policies, procedures and standards.
- 3.3 Security incidents and **other security issues** are reported/referred to government security authorities in accordance with legislation and security standards.

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 the coordination of protective security
- reading and analysing complex documents such as legislation, regulations and standards in the context of protective security
- researching and critically analysing the operational environment and drawing conclusions
- using communication with diverse stakeholders involving listening, questioning, paraphrasing, clarifying and summarising, to provide advice and support
- responding to diversity, including gender and disability
- writing reports and recommendations requiring formality of language and structure
- using computer technology to gather and analyse information, and prepare reports
- applying procedures relating to occupational health and safety and environment in the context of protective security coordination

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
 - the organisation's functions, assets and security environment
- Australian standards, quality assurance and certification requirements
- AS/NZS ISO31000:2009 Risk management - Principles and Guidelines
- equal employment opportunity, equity and diversity principles
- public sector legislation such as occupational health and safety and environment in the context of coordinating protective security

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
 - PSPLEGN501B Promote compliance with legislation in the public sector
 - PSPSEC501A Assess security risks
 - PSPSEC502A Develop security risk management plans
 - PSPSEC503A Implement and monitor security risk management plans
 - PSPSEC505A Protect security classified information
 - PSPSEC506A Communicate security awareness

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)
- coordination of protective security 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 coordination of protective security
- case studies and workplace scenarios to capture the range of situations likely to be encountered when coordinating protective security

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 coordinating protective security, including coping with difficulties, irregularities and breakdowns in routine

- coordination of protective security 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

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.

Threats may be:

- real or perceived
- criminal
- terrorist
- from foreign intelligence services
- from commercial/industrial competitors
- from malicious people
- to:
 - personnel
 - information
 - property
 - reputation

Physical security measures may include:

- storage arrangements
- access control
- barriers and alarms

Procedural security measures may include:

- use
- classification
- labelling
- handling
- transmission
- restricted access

Security matters may include:

- security incidents
- personnel vetting
- home-based work
- conference security
- classification of information
- security clearances

Protective security standards may include those in:

- fraud control policy
- protective security policy
- public service codes of conduct/ethics
- legislation/regulations, such as:
 - public service Acts
 - Crimes Act 1914 and Criminal Code 1985

- Freedom of Information Act 1982
 - Privacy Act 1988
- Security incidents** may be:
- breaches
 - violations
 - contact
 - approach
 - intentional
 - unintentional
 - deliberate
- Security authorities/organisations** may include:
- organisations contracted to provide security services
 - government authorities/organisations with a security mandate
- Other security issues** may include:
- briefings for people preparing to serve overseas
 - national security clearances
 - security incidents
 - security investigations

Unit Sector(s)

Not applicable.

Competency field

Government Security Management.