Australian Government

Department of Education, Employment and Workplace Relations

PSPSEC404A Conduct personnel security assessments

Release 3

INDUSTRY SKILLS COUNCILS
Creating Australia's Future

PSPSEC404A Conduct personnel security assessments

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 conduct of personnel security assessments to ensure that government staff and contractors who have access to security classified information meet general suitability indicators. It includes collecting, analysing and evaluating personal information, making recommendations on security assessment outcomes, and recording and reporting on personnel security assessments.

In practice, the conduct of personnel security assessments may overlap with other generalist or specialist public sector work activities such as acting ethically, complying with legislation, applying government processes, gathering and analysing information, using resources.

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.

        Government Skills Australia

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. **Collect**, **analyse and evaluate personal information**	1.1 *Information* is collected from the subject to be assessed in accordance with the purpose of the *security assessment*.
	1.2 Where gaps, anomalies, deficiencies or discrepancies exist in the information provided, additional information is obtained in accordance with organisational policy and procedures.
	1.3 Information is *corroborated* in accordance with organisational policy and procedures and *assessed* for its validity and reliability.
	1.4 Analysis is conducted in accordance with general suitability indicators in accordance with *legislation and security standards*.
	1.5 Data is extracted and interpreted and outcomes are recorded in accordance with organisational policy and procedures.
	1.6 Assessment process is conducted with care and sensitivity to assist subjects to deal with its discriminatory and intrusive nature.
2. **Make recommendations on security assessment outcomes**	2.1 *Recommendations* are formulated consistent with the information obtained.
	2.2 Recommendations are consistent with organisational guidelines and security standards.
	2.3 Recommendations are conveyed in accordance with organisational guidelines.
	2.4 Where recommendations are negative, the right to seek a review of the decision is confirmed with the requester of the security assessment and the subject, where appropriate, in accordance with organisational policy and procedures.
	2.5 Improvements to procedures are recommended as required as part of the cycle of continuous improvement.
3. **Record and report on personnel security assessments**	3.1 Accurate, *complete*, up-to-date records are presented in the required format.
	3.2 *Reports* are prepared that are clear, fair and objective and use language suited to the purpose of the report and organisational requirements.
	3.3 Reports are presented in the required format.
	3.4 Urgency and levels of risk are addressed in reports.
	3.5 Procedures for storage and management of confidential and sensitive information are adhered to.

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 personnel security assessments
- undertaking critical analysis, evaluation and deductive reasoning
- applying problem solving and decision making
- corroborating information
- organising information in a logical manner
- writing reports and recommendations
- using computer technology
- managing files
- responding to diversity, including gender and disability
- applying procedures relating to occupational health and safety and environment in the context of personnel security assessments

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
    - Protective Security Policy Framework
    - general suitability indicators
    - international treaties and protocols
    - formats for different types of reports
    - risk assessment
    - management of secure information
    - equal employment opportunity, equity and diversity principles
    - public sector legislation such as occupational health and safety and environment in the context of personnel security assessments

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
	• PSPGOV402B Deliver and monitor service to clients
	• PSPGOV406B Gather and analyse information
	• PSPLEGN401A Encourage compliance with legislation in the public sector
	• PSPSEC401A Undertake government security risk analysis
	• PSPSEC402A Implement security risk treatments
	• PSPSEC403A Develop and advise on government security procedures
	• PSPSEC405A Handle security classified information
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)
	• conduct of personnel security assessments 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 conduct of personnel security assessments
	• Commonwealth Protective Security Manual
	• case studies and workplace scenarios to capture the range of situations likely to be encountered when conducting personnel security assessments
Where and how to	Valid assessment of this unit requires:

assess evidence	• a workplace environment or one that closely resembles normal work practice and replicates the range of conditions likely to be encountered when conducting personnel security assessments, including coping with difficulties, irregularities and breakdowns in routine
	• conduct of personnel security assessments 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
- demonstration
- observation
- portfolios
- projects
- questioning
- scenarios
- simulation or role plays
- authenticated evidence from the workplace and/or training courses, such as reports

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.

Information may include:	- birth certificate - marriage certificate - decree nisi/decree absolute - deed poll - academic qualifications/academic transcripts - employment histories - citizenship - passport - defence forces discharge certificate
Security assessment may be for:	- initial evaluation - re-evaluation - temporary access - emergency access - provisional access - limited higher access
Corroboration of information may be with:	- official records - referee reports - employer records - third party reports
Assessment of information may relate to:	- character - attributes - background - actions - anything in a person's background or lifestyle likely to pose a security threat
Legislation and security standards may include those referred to in:	- public service Acts - protective security policy - fraud control policy - Crimes Act 1914 and Criminal Code 1985 - Freedom of Information Act 1982 - Privacy Act 1988 - occupational health and safety

	• AS/NZS ISO 31000:2009 Risk management - Principles and Guidelines
	• Australian Government Information Security Manual (ISM)
	• Protective Security Policy Framework
Recommendations may relate to:	• assessment of suitability
	• action required
Completeness of records includes:	• request from someone other than the subject, such as a supervisor
	• despatch of information pack/forms
	• all enquiries and responses
	• receipt of incoming documents
	• consent to collect/corroborate information
	• personal security file
Reports may include:	• interview reports
	• assessment reports
	• case notes
	• incidents
	• records of interview
	• notes for file

Unit Sector(s)

Not applicable.

Competency field

Government Security Management.