



Australian Government

Department of Education, Employment and Workplace Relations

PSPSEC304A Undertake information technology security audits

Release 3

PSPSEC304A Undertake information technology security audits

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 security audits of information systems and architecture in accordance with the organisation's security plan and jurisdictional standards for government information security. It includes planning and conducting the information technology security audit and reporting on security findings.

In practice, undertaking information technology security audits may overlap with other generalist or specialist public sector work activities such as acting ethically, complying with legislation, working effectively, organising information.

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. Plan security audit	1.1 The scope and objectives of the audit are identified. 1.2 An audit plan is prepared that meets organisational requirements and the objectives of the audit. 1.3 The organisation's information systems to be included in the audit are identified in the audit plan. 1.4 Appropriate personnel are advised of the audit plan and its requirements. 1.5 Possible sources of security risk are identified and prioritised. 1.6 Audit checklist is prepared in accordance with organisational policy and procedures.
2. Conduct security audit	2.1 Systems, procedures, records and documents are identified and analysed. 2.2 Audit is conducted in accordance with the audit plan. 2.3 Audit activities are recorded in accordance with the checklist and organisational requirements. 2.4 Situations requiring specialist input are identified and referred for action. 2.5 Situations requiring referral to other areas are identified and referred in a timely manner.
3. Report on security findings	3.1 Audit records are maintained in accordance with legislation, policy and procedures. 3.2 Audit report is prepared in accordance with organisational requirements and audit objectives. 3.3 Background and scope of the audit, outcomes and recommendations are included in the report. 3.4 Report is written in a language and style to suit the audience and meets organisational requirements for accuracy and timeliness. 3.5 Recommendations are supported by evidence, and written as actions with responsible person/s identified for implementation.

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 information technology security audits and government security management
- gathering, analysing and recording data
- using computer technology to undertake security audits
- managing risk in the context of government security management
- engaging in discussion involving complex exchanges of oral information
- responding to diversity, including gender and disability
- using written communication, including ongoing and final reporting
- reading complex and formal documents such as legislation and other documents
- using information technology for preparing written recommendations and reports requiring formality of language and style
- applying procedures relating to occupational health and safety and environment in the context of information technology security audits

Knowledge requirements

Look for evidence that confirms knowledge and understanding of:

- legislation, regulations, policies, procedures and guidelines relating to information technology security audits
- operational knowledge of policies and procedures in regard to use of information technology systems
- organisation's security plan
- information technology systems and architecture
- use and maintenance of hardware and software systems
- solutions to problems/breakdowns
- operation of equipment
- Australian Audit Standards
- aspects of criminal law and administrative law relating to the outcomes of compliance audits
- protocols for reporting fraud, corruption, maladministration and security breaches
- fundamental ethical principles in the handling of documents and information, natural justice, procedural fairness, respect for persons and responsible care
- equal employment opportunity, equity and diversity principles
- public sector legislation such as occupational health and safety and environment in the context of security audits

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:
 - PSPETHC301B Uphold the values and principles of public service
 - PSPGOV301B Work effectively in the organisation
 - PSPGOV302B Contribute to workgroup activities
 - PSPGOV307B Organise workplace information
 - PSPLEGN301B Comply with legislation in the public sector
 - PSPOHS301A Contribute to workplace safety
 - PSPSEC301A Secure government assets
 - PSPSEC302A Respond to government security incidents
 - PSPSEC303A Conduct security awareness sessions

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)
- information technology security audits undertaken 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 information technology security audits
- 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 undertaking information technology security audits

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 information technology security audits, including coping with difficulties, irregularities and breakdowns in routine
- information technology security audits undertaken 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
- questioning
- scenarios
- simulation or role plays
- 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.

Information systems may include:

- architecture
- audio-visual systems
- communications equipment
- hardware
- Internet
- intranet
- laptops
- pagers
- personal computers
- scanning equipment
- software
- systems

Information systems may be:

- centrally based
- location based
- stand-alone
- networked

Appropriate personnel may include:

- supervisors
- managers
- employees
- contractors

Security risk may include:

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

Specialist input may include:

- agency security adviser/s
- specialist agencies such as:
 - Australian Security Intelligence Organisation
 - Department of Foreign Affairs and Trade
 - Australian Public Service Commission
 - Defence Signals Directorate
 - Australian Federal Police
 - Attorney-General's Department
 - Australian National Audit Office
 - Office of the Australian Information Commissioner (OAIC)

Other areas may include:

- fraud investigation area
- compliance area
- other organisations such as police, other law enforcement or investigation agencies
- senior management

Report may be:

- written
- oral
- electronic

Unit Sector(s)

Not applicable.

Competency field

Government Security Management.