



Australian Government

PSPSEC004 Undertake information technology security audits

Release: 1

PSPSEC004 Undertake information technology security audits

Modification History

Release	Comments
1	This unit was released in PSP Public Sector Training Package release 1.0 and meets the Standards for Training Packages. This unit supersedes and is equivalent to PSPSEC304A Undertake information technology security audits. • Unit code updated • Content and formatting updated to comply with new standards • All PC transitioned from passive to active voice • PC 1.1 and 1.2, PC 1.5 and 1.6, PC 2.4 and 2.5, PC 3.1 and 3.2 merged

Application

This unit describes the skills required to plan and conduct an information technology security audit and report on security findings.

This unit applies to those working in a role where they have responsibilities under the organisation's security plan.

The skills and knowledge described in this unit must be applied within the legislative, regulatory and policy environment in which they are carried out. Organisational policies and procedures must be consulted and adhered to.

Those undertaking this unit would generally work independently and as part of a team using support resources as required. They would perform complex tasks in a range of familiar and unfamiliar contexts.

No licensing, legislative or certification requirements apply to unit at the time of publication.

Competency Field

Security

Elements and Performance Criteria

ELEMENTS	PERFORMANCE CRITERIA
Elements describe	Performance criteria describe the performance needed to demonstrate

the essential outcomes	achievement of the element. Where bold italicised text is used, further information is detailed in the range of conditions section.
1. Plan security audit	1.1 Identify the scope and objectives of the audit and prepare an audit plan to meet the objectives. 1.2 Identify the organisation's information systems to be included in the audit plan. 1.3 Advise appropriate personnel of the audit plan and its requirements. 1.4 Identify and prioritise possible sources of security risk and prepare an audit checklist.
2. Conduct security audit	2.1 Identify and analyse systems, procedures, records and documents. 2.2 Conduct audit in accordance with the audit plan. 2.3 Record audit activities. 2.4 Identify situations requiring specialist input or referral to other areas and act on referral.
3. Report on security findings	3.1 Maintain audit records and prepare audit reports. 3.2 Produce report including background, scope, outcomes and recommendations. 3.3 Use language and style to suit the audience and in line with organisational requirements for accuracy and timeliness. 3.4 Support recommendations with evidence and highlight actions identifying person/s responsible for implementation.

Foundation Skills

The foundation skills demands of this unit have been mapped for alignment with the Australian Core Skills Framework (ACSF). The following tables outline the performance levels indicated for successful attainment of the unit.

ACSF levels indicative of performance:

1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
Learning					Reading					Writing					Oral communication					Numeracy NA				

Performance variables:

1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
Support					Context					Text complexity					Task complexity				

Further information on ACSF and the foundation skills underpinning this unit can be found in the Foundation Skills Guide on the GSA website.

Unit Mapping Information

This unit supersedes and is equivalent to PSPSEC304A Undertake information technology security audits.

Links

Companion Volume implementation guides are found in VETNet -

<https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=bebbece7-ff48-4d2c-8876-405679019623>

Companion Volume implementation guides are found in VETNet -

<https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=bebbece7-ff48-4d2c-8876-405679019623>

Companion Volume implementation guides are found in VETNet -

<https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=bebbece7-ff48-4d2c-8876-405679019623>

Companion Volume implementation guides are found in VETNet -

<https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=bebbece7-ff48-4d2c-8876-405679019623>

Assessment Requirements for PSPSEC004 Undertake information technology security audits

Modification History

Release	Comments
1	These Assessment Requirements were released in PSP Public Sector Training Package release 1.0 and meet the Standards for Training Packages. • Assessment Requirements created drawing upon specified assessment information from superseded unit

Performance Evidence

Evidence required to demonstrate competence must satisfy all of the requirements of the elements and performance criteria. If not otherwise specified the candidate must demonstrate evidence of performance of the following on at least two occasions.

- applying legislation, regulations and policies relating to information technology security audits and government security management
- gathering, analysing and recording data
- using computer applications to undertake security audits
- managing risk in the context of government security management
- engaging in discussion involving exchanges of complex information
- responding to diversity

Knowledge Evidence

Evidence required to demonstrate competence must satisfy all of the requirements of the elements and performance criteria. If not otherwise specified the depth of knowledge demonstrated must be appropriate to the job context of the candidate.

- 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
- 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

Assessment Conditions

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 IT security audits.

Assessors must satisfy the NVR/AQTF mandatory competency requirements for assessors.

Links

Companion Volume implementation guides are found in VETNet -

<https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=bebbece7-ff48-4d2c-8876-405679019623>

Companion Volume implementation guides are found in VETNet -

<https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=bebbece7-ff48-4d2c-8876-405679019623>

Companion Volume implementation guides are found in VETNet -

<https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=bebbece7-ff48-4d2c-8876-405679019623>