



Australian Government

CPPSEC4012 Assess security vulnerabilities of assets

Release: 1

CPPSEC4012 Assess security vulnerabilities of assets

Modification History

Release 1 This version first released with CPP Property Services Training Package Release 9.0.

Supersedes and is equivalent to CPPSEC4012A Identify and assess security of assets. Updated to meet the Standards for Training Packages.

Application

This unit specifies the skills and knowledge required to assess the security vulnerabilities of client assets based on an analysis of asset types, use, ownership and value. It includes auditing security risk control mechanisms and incident reporting measures and testing their operational effectiveness to identify failures and recommend treatment options.

This unit is suitable for those using specialised knowledge to complete routine and non-routine tasks and using their own judgement to deal with predictable and sometimes unpredictable problems.

Legislative, regulatory or certification requirements apply in some states and territories to the provision of advice on security solutions, strategies, protocols and procedures. For further information, check with the relevant regulatory authority.

Pre-requisite Unit

None.

Unit Sector

Security/Risk management

Elements and Performance Criteria

Elements describe the essential outcomes.

Performance criteria describe what needs to be done to demonstrate achievement of the element.

1 List client assets and confirm status.

1.1 Access and interpret key requirements of legislation, regulations and workplace policies and procedures and apply to work instructions to ensure compliance.

1.2 Consult with relevant persons to confirm the location and nature of all assets and clarify client security objectives in relation to each asset.

- 1.3 Source valid and reliable information to confirm the value of all client assets in consultation with relevant persons.
 - 1.4 Document listing of client assets and valuations in a format suitable for analysis.
 - 1.5 Conduct analysis to confirm asset types, use, ownership and value.
 - 1.6 Recognise own limitations in assessing asset security vulnerabilities of client and access specialist resources or advice to meet client requirements.
- 2 Assess security risk control mechanisms to identify asset vulnerabilities.
 - 2.1 Identify and assess methods for accessing client assets.
 - 2.2 Conduct audit of existing and planned security risk control mechanisms and incident reporting measures.
 - 2.3 Obtain and review operating parameters for identified risk control mechanisms to plan testing methods.
 - 2.4 Test operational effectiveness of risk control mechanisms to identify actual and potential failures and report the results to relevant persons.
- 3 Finalise and present asset security vulnerability assessment.
 - 3.1 Finalise asset security vulnerability assessment including recommendations to treat identified security risks, and check to ensure findings and recommendations are supported by verifiable information.
 - 3.2 Use information technologies to document and present asset security vulnerability assessment in a format and style to meet workplace requirements.
 - 3.3 Present final asset security vulnerability assessment to relevant persons for feedback within agreed timeframes.
 - 3.4 Use questioning and active listening to explain identified security vulnerabilities and recommended treatments.
 - 3.5 Complete and secure asset assessment documentation in a manner that facilitates future retrieval and maintains confidentiality according to workplace and regulatory requirements.

Foundation Skills

As well as the foundation skills explicit in the performance criteria of this unit, candidates require:

- oral communication skills to use clear explanations, active listening and questioning skills to convey and clarify information when assessing asset vulnerabilities
- writing skills to document succinct and logically structured client advice.

Unit Mapping Information

Supersedes and equivalent to CPPSEC4012A Identify and assess security of assets.

Links

Companion volumes to this training package are available at the VETNet website - <https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=6f3f9672-30e8-4835-b348-205dfcf13d9b>

Assessment Requirements for CPPSEC4012 Assess security vulnerabilities of assets

Modification History

Release 1 This version first released with CPP Property Services Training Package Release 9.0.

Supersedes and is equivalent to CPPSEC4012A Identify and assess security of assets. Updated to meet the Standards for Training Packages.

Performance Evidence

To demonstrate competency, a candidate must meet the performance criteria of this unit by documenting and presenting comprehensive assessments of the security vulnerabilities of assets for three different clients involving at least three of the following types of assets:

- buildings
- critical infrastructure
- equipment
- information systems
- people.

Knowledge Evidence

To be competent in this unit, a candidate must demonstrate knowledge of:

- workplace policies and procedures that ensure compliance with legislative and regulatory requirements when assessing the security vulnerabilities of assets:
 - client service standards
 - licensing requirements in the security industry
 - regulatory requirements in the jurisdiction of operation
- application of *ISO 31000:2018 Risk management – Guidelines* when assessing security vulnerabilities of assets
- audit techniques used when assessing existing and planned security risk control and reporting mechanisms for client assets
- difference between crowded places and critical infrastructure
- factors that may influence value of client assets
- methods for testing operational effectiveness of assets and risk control mechanisms
- methods for validating the reliability of information used to assess security vulnerabilities of assets
- risk assessment techniques
- sources and types of information used to confirm asset status and values

- type and nature of a range of security risks to client assets and control measures for each
- types of client assets that may require protection from security risks
- understanding of ways that assets are valued:
 - criticality to operations
 - depreciated value
 - formal valuation
 - personal value to client
 - purchase price
 - replace cost
- ways that social and cultural differences may be expressed during client consultations.

Assessment Conditions

Assessors must meet the requirements for assessors contained in the Standards for Registered Training Organisations.

All individuals engaged by a licensed RTO for security licensing purposes must hold both a security trainers licence (where such a licence exists within the relevant jurisdiction) and the licence for performing the security activities for which the individual is providing training or assessment. Regulators may impose other assessor conditions to meet jurisdictional assessment requirements.

Assessment must be conducted in the workplace or in a simulated workplace environment. Candidates must have access to:

- legislation, regulations, policies and procedures that apply to assessing the security vulnerabilities of client assets in the jurisdiction of operation
- client information and specifications, information technologies and resources required to achieve the performance evidence
- *ISO 31000:2018 Risk management – Guidelines.*

Links

Companion volumes to this training package are available at the VETNet website - <https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=6f3f9672-30e8-4835-b348-205dfcf13d9b>