



Australian Government

CPPSEC5005 Implement security risk management plans

Release: 1

CPPSEC5005 Implement security risk management plans

Modification History

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

Supersedes and is equivalent to CPSEC5005A Implement security risk assessment plan. Updated to meet the Standards for Training Packages.

Application

This unit specifies the skills and knowledge required to implement security risk management plans. It includes organising, costing and allocating resources, monitoring emerging security risks and changes in the operating environment against activities and targets in action plans, and reviewing treatment options to update security risk management plans. Risk management plans are implemented based on the principles of *ISO 31000:2018 Risk management – Guidelines* (ISO 31000).

This unit is suitable for those using a broad range of cognitive, technical and communication skills to select and apply methods and technologies to analyse information and provide solutions to sometimes complex 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 Organise and allocate resources to support security risk management plan. | 1.1 Access and interpret key requirements of legislation, regulations and Australian standard ISO 31000 to understand and comply with requirements for implementing security risk management plans. |
|---|---|

- 1.2 Review security risk management plan to clarify and cost resource requirements.
 - 1.3 Plan and schedule activities and targets to meet requirements of risk management action plans.
 - 1.4 Define roles, responsibilities and work schedules for implementing security risk management plan and communicate to relevant persons.
 - 1.5 Organise efficient allocations of resources, equipment and materials required to implement risk management action plans.
 - 1.6 Disseminate information to support security risk management plan information according to workplace and regulatory requirements.
- 2 Monitor emerging security risks and operating environment.
 - 2.1 Monitor emerging risks and assess ongoing suitability of implemented security risk treatment options based on ISO 31000 principles.
 - 2.2 Monitor changes to operating environment and identify and incorporate corrective contingency measures into security risk management plan.
 - 2.3 Regularly review risk management targets and outcomes against action plans to confirm aims and objectives are achieved.
 - 2.4 Prepare documentation and guidelines explaining incidence, nature and causes of emerging security risks and contingencies implemented.
- 3 Review treatment options and update security risk management plan.
 - 3.1 Systematically review effectiveness of security risk treatment options in meeting risk management objectives.
 - 3.2 Identify and test required corrective measures to confirm suitability to meet risk management objectives.
 - 3.3 Modify security risk management plan to incorporate corrective measures and address discrepancies between treatment options and risk incidence.

- 3.4 Seek feedback from relevant persons on effectiveness of treatment options and make required adjustments to incorporate feedback.
- 3.5 Cost long and short-term options to accurately estimate resource allocations to support security risk management plan.
- 3.6 Confirm stages of implementation for security risk management plan and coordinate required resources to ensure availability.
- 3.7 Finalise updated security risk management plan 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 negotiate agreements
- writing skills to prepare succinct and logically structured security risk management documents and guidelines
- numeracy skills to apply statistical methods and present statistical data.

Unit Mapping Information

Supersedes and equivalent to CPPSEC5005A Implement security risk management plan.

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 CPPSEC5005 Implement security risk management plans

Modification History

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

Supersedes and is equivalent to CPSEC5005A Implement security risk assessment plan. Updated to meet the Standards for Training Packages.

Performance Evidence

To demonstrate competency, a candidate must meet the performance criteria of this unit by implementing two different security risk management plans.

Knowledge Evidence

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

- legislative and regulatory requirements that apply when implementing security risk management plans:
 - key requirements of legislation, regulations and codes of conduct for security risk management in the jurisdiction of operation
 - legal rights and responsibilities of employers, supervisors and employees associated with work health and safety and duty of care
 - licensing requirements in the security industry
 - trespass and removal of persons
 - use of force
- application of integrated security measures including physical security, manpower, security technologies and security of personnel and information
- distinction between information and intelligence and methods for validating information sources
- work scheduling methods
- activities and targets contained in risk management action plans
- methods for achieving efficiencies when allocating resources, equipment and materials to the implementation of security risk management plans
- implications for security risk management arising from:
 - *National Guidelines for the Protection of Places of Mass gathering from Terrorism*
 - *Active Armed Offender Guidelines for Crowded Places*
 - *Improvised Explosive Device Guidelines for Crowded Places*
 - *Chemical Weapon Guidelines for Crowded Places*

- *Hostile Vehicle Guidelines for Crowded Places*
- methods for determining the type, nature and causes of potential and actual security risks
- methods for distinguishing between acceptable and unacceptable security risks
- methods for prioritising security risks and treatment options based on degree of risk
- methods for testing treatment options in the field
- process and application of dynamic risk assessment and risk management methods
- purpose of *Australia's Strategy for Protecting Crowded Places from Terrorism* and understanding of:
 - definition of crowded places
 - key security issues for crowded places
 - objectives, characteristics and identification of active armed offenders
 - definition of hostile vehicles and methods of attack
 - signs of chemical weapons attack and recommend response
 - general features of improvised explosive devices and recommended incident response
- recognised industry practice and application of *ISO 31000:2018 Risk management – Guidelines* (ISO 31000) when implementing and updating security risk management plans
- types of treatment options appropriate to the range of security risks and threats to various client operating environments:
 - assets
 - buildings
 - crowded places
 - mass gatherings.

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 and codes of practice that apply when implementing security risk management plans in the jurisdiction of operation
- risk management plans including action plans, resources and information technologies required to achieve the performance evidence
- ISO 31000
- *National Guidelines for the Protection of Places of Mass gathering from Terrorism*
- *Australia's Strategy for Protecting Crowded Places from Terrorism*
- *National Guidelines for the Protection of Places of Mass gathering from Terrorism*

- *Active Armed Offender Guidelines for Crowded Places*
- *Improvised Explosive Device Guidelines for Crowded Places*
- *Chemical Weapon Guidelines for Crowded Places*
- *Hostile Vehicle Guidelines for Crowded Places.*

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>