



Australian Government

Department of Education, Employment and Workplace Relations

CPPSEC5003A Assess security risk management options

Release: 1

CPPSEC5003A Assess security risk management options

Modification History

Not Applicable

Unit Descriptor

Unit descriptor

This unit of competency specifies the outcomes required to assess options for the management of security risk in an organisational environment. It requires the ability to compare treatment options against identified security risks, rank suitable treatment options, and prepare and present recommended options and supporting analysis.

This unit may form part of the licensing requirements for persons engaged in risk assessment operations in those states and territories where these are regulated activities.

Application of the Unit

Application of the unit

This unit of competency has application in those work roles involving the assessment of security risks in an organisational environment. Competency requires legal and operational knowledge applicable to relevant sectors of the security industry. The knowledge and skills described in this unit are to be applied within relevant legislative and organisational guidelines.

Licensing/Regulatory Information

Refer to Unit Descriptor

Pre-Requisites

Not Applicable

Employability Skills Information

Employability skills This unit contains employability skills.

Elements and Performance Criteria Pre-Content

Elements describe the essential outcomes of a unit of competency.	Performance criteria describe the required performance needed to demonstrate achievement of the element. Where <i>bold italicised</i> text is used, further information is detailed in the required skills and knowledge section and/or the range statement. Assessment of performance is to be consistent with the evidence guide.
---	--

Elements and Performance Criteria

ELEMENT

PERFORMANCE CRITERIA

- | | |
|---|--|
| 1 Determine security risk. | <ul style="list-style-type: none">1.1 Applicable provisions of legislative and organisational requirements, and relevant standards for assessment activities are identified and complied with.1.2 Type and nature of security risks are determined based on an accurate and current assessment of the client's operating environment and core business operations.1.3 Security risks are ranked in terms of degree of risk and linked to potentially suitable treatment options.1.4 Degree of risk is determined by an assessment of current and valid data. |
| 2 Identify and assess treatment options. | <ul style="list-style-type: none">2.1 Treatment options are identified and confirmed to be commensurate with the identified type, nature and cause of security risk.2.2 Treatment options applied in a similar context are researched and assessed for effectiveness against documented and verifiable evidence.2.3 Criteria for assessment of risks against treatment options are consistent with recognised industry practice and relevant standards.2.4 Treatment options appropriate to the full range of potential security risks are selected and prioritised according to established criteria. |
| 3 Review and present findings. | <ul style="list-style-type: none">3.1 A report outlining assessment findings and recommended treatment options is prepared and presented to relevant persons.3.2 Analysis and recommendations are clear, coherent and consistent with terms of reference and supported by verifiable evidence.3.3 Advice outlining possible consequences of not implementing recommended treatment options is included in the analysis.3.4 Effective interpersonal techniques and presentation procedures are used to enhance understanding and acceptance of recommended treatment options. |

Required Skills and Knowledge

REQUIRED SKILLS AND KNOWLEDGE

REQUIRED SKILLS AND KNOWLEDGE

This section describes the skills and knowledge and their level required for this unit.

Required skills

- accurately determine identified risks and threats
- apply reasoning and logical analysis in assessment processes
- assess risks and threats
- coaching and mentoring to provide support to colleagues
- collate numerical data
- communicate in a clear and concise manner
- determine suitability of treatment option against security risk
- determine type and nature of security risks
- identify and assess assets
- prepare and present verbal and written reports
- prioritise tasks and organise schedules
- prioritise treatment options in terms of degree of security risk
- provide written communication to a standard required for compiling reports and summarising information
- relate to persons of different social and cultural backgrounds and varying physical and mental abilities
- research and analyse information
- source and access information
- use a variety of problem-solving techniques
- use business and information technology.

Required knowledge

- applicable Australian standards, industry codes of practice and legislation including Occupational Health and Safety (OHS)
- basic understanding of insurance in terms of acceptable risks, premium ranges and liabilities
- client's operating environment and business operations
- concept of integrated security measures including physical security; information technology security, and security of personnel and information
- concept of litigation
- current security systems and technologies available expertise
- distinction between information and intelligence
- preparation of documentation and presentation procedures
- principles of basic statistics and numeracy
- principles of effective communication
- principles of AS/NZS 4360: 2004 Risk management and related guidelines
- privacy and confidentiality requirements
- relevant industry codes of practice

REQUIRED SKILLS AND KNOWLEDGE

- relevant legislation and regulations including licensing requirements
- risk assessment techniques
- types of treatment options appropriate to the range of security risks and threats applicable to premises and businesses.

Evidence Guide

EVIDENCE GUIDE

The evidence guide provides advice on assessment and must be read in conjunction with the performance criteria, required skills and knowledge, range statement and the Assessment Guidelines for the Training Package.

Critical aspects for assessment and evidence required to demonstrate competency in this unit

A person who demonstrates competency in this unit must be able to provide evidence of understanding and knowledge of the following:

- evaluating risks against developed criteria and selecting treatment options commensurate with the level and nature of potential risks based on the principles of AS/NZS 4360: 2004
- identifying the nature, cause and range of potential security risks to client based on an assessment of valid and relevant data
- preparing and presenting an analysis and options related to management of security risks and using effective interpersonal skills to enhance client understanding and acceptance of recommendations.

Context of and specific resources for assessment

Context of assessment includes:

- a setting in the workplace or environment that simulates the conditions of performance described in the elements, performance criteria and range statement.

Resource implications for assessment include:

- access to a registered provider of assessment services
- access to a suitable venue and equipment
- access to plain English version of relevant statutes and procedures
- assessment instruments including personal planner and assessment record book
- work schedules, organisational policies and duty statements.

Reasonable adjustments must be made to assessment processes where required for people with disabilities. This could include access to modified equipment and other physical resources, and the

provision of appropriate assessment support.

Method of assessment This unit of competency should be assessed using questioning of underpinning knowledge and skills.

Guidance information for assessment Assessment processes and techniques must be culturally appropriate and suitable to the language, literacy and numeracy capacity of the candidate and the competency being assessed. In all cases where practical assessment is used, it should be combined with targeted questioning to assess the underpinning knowledge.

Oral questioning or written assessment may be used to assess underpinning knowledge. In assessment situations where the candidate is offered a choice between oral questioning and written assessment, questions are to be identical.

Supplementary evidence may be obtained from relevant authenticated correspondence from existing supervisors, team leaders or specialist training staff.

Range Statement

RANGE STATEMENT

The range statement relates to the unit of competency as a whole. It allows for different work environments and situations that may affect performance. Bold italicised wording, if used in the performance criteria, is detailed below. Essential operating conditions that may be present with training and assessment (depending on the work situation, needs of the candidate, accessibility of the item, and local industry and regional contexts) may also be included.

Legislative requirements may relate to:

- apprehension and powers of arrest
- Australian standards and quality assurance requirements
- counter-terrorism
- crowd control and control of persons under the influence of intoxicating substances
- force continuum, use of force guidelines
- general 'duty of care' responsibilities
- inspection of people and property, and search and seizure of goods
- licensing or certification requirements
- privacy and confidentiality
- relevant commonwealth, state and territory legislation, codes and national standards for:
 - anti-discrimination

- cultural and ethnic diversity
- environmental issues
- equal employment opportunity
- industrial relations
- OHS
- relevant industry codes of practice
- trespass and the removal of persons
- use of restraints and weapons:
 - batons
 - firearms
 - handcuffs
 - spray.

Organisational requirements may relate to:

- access and equity policies, principles and practices
- business and performance plans
- client service standards
- code of conduct, code of ethics
- communication and reporting procedures
- complaint and dispute resolution procedures
- emergency and evacuation procedures
- employer and employee rights and responsibilities
- OHS policies, procedures and programs
- own role, responsibility and authority
- personal and professional development
- privacy and confidentiality of information
- quality assurance and continuous improvement processes and standards
- resource parameters and procedures
- roles, functions and responsibilities of security personnel
- storage and disposal of information.

Relevant standards:

- must include AS/NZS 4360: 2004 Risk management
- may relate to:
 - AS2630-1983 Guide to the selection and application of intruder alarm systems for domestic and business premises
 - HB 167:2006 Security Risk Management
 - HB 436 Risk Management Guidelines - Companion to AS/NZS 4360
 - HB 231:2000 Information security risk management guidelines
 - other standards relating to the treatment options as published and distributed by Standards Australia.

Security risks may be:

- acceptable
- across all aspects of operations
- across limited number of operations
- high likelihood
- long-term
- low likelihood
- potentially avoidable
- potentially unavoidable
- short-term
- unacceptable.

Risk relates to:

- the chance of something happening that will have an impact on objectives.

Risks may relate to:

- break-ins
- business operations
- confidentiality
- deliberate or accidental damage
- finance
- OHS
- personnel
- theft
- threats of loss, harm or damage to persons or property
- trespass
- unauthorised access
- vandalism
- workplace environment.

Assessment of operating environment may relate to:

- competitors
- core business functions
- environmental issues
- financial markets
- industrial relations
- market share
- nature of operations
- neighbours
- scale of operations
- situational issues
- size
- stability
- stability of company, organisation, industry and market
- stakeholders
- type of industry
- workforce.

- Security risk nature and causes may be:**
- client-based
 - external
 - financial
 - internal
 - mechanical
 - operational
 - skill based.
- Treatment options may relate to:**
- attendance
 - confidentiality
 - interventions
 - regularity of presence
 - rehearsals
 - surveillance.
- Verifiable evidence may include:**
- incident reports
 - insurance data
 - official records
 - organisational data
 - video evidence
 - witness statements.
- Criteria may include assessment of:**
- budgetary constraints
 - environmental issues
 - industrial relations
 - legal issues
 - nature of the task
 - operating environment of organisation
 - organisation structure
 - organisational image
 - political influences
 - terms of reference
 - timeframes.
- Presentation may involve:**
- charts and statistical reports
 - computer equipment including data projectors
 - models
 - real-time demonstration
 - simulation
 - the use of audio and video.
- Terms of reference may relate to:**
- client expectations
 - cost
 - limitations and exclusions of access to information
 - lines of authority
 - operational environment

Interpersonal techniques may involve:

- roles and responsibilities
- scale of the assessment eg full-scale operation or limited to a particular section or operation of the company
- security and other clearances
- timeframe.
- active listening
- being non-judgemental
- being respectful and non-discriminatory
- constructive feedback
- control of tone of voice and body language
- culturally aware and sensitive use of language and concepts
- demonstrating flexibility and willingness to negotiate
- effective verbal and non-verbal communication
- maintaining professionalism
- providing sufficient time for questions and responses
- reflection and summarising
- two-way interaction
- use of plain English
- use of positive, confident and cooperative language.

Unit Sector(s)

Unit sector Security

Competency field

Competency field Security and risk management