



Australian Government

Department of Education, Employment and Workplace Relations

CPPSEC3003A Determine response to security risk situation

Release: 1

CPPSEC3003A Determine response to security risk situation

Modification History

Not Applicable

Unit Descriptor

Unit descriptor This unit of competency specifies the outcomes required to determine an appropriate response to a security risk situation. It requires the ability to analyse the nature and degree of risk and determine response options according to changing circumstances.

This unit may form part of the licensing requirements for persons engaged in guarding 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 guarding in a security 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 Identify security risk situation.	1.1 Applicable provisions of legislative and organisational requirements relevant to security risk operations identified and complied with. 1.2 Information on security risk situation is received and verified for reliability and authenticity. 1.3 Environmental factors relevant to security risk situation are identified and monitored for changes in characteristics that may impact on security response. 1.4 Additional information required to assess degree of risk is sourced as required. 1.5 Communication channels and processes are used to maintain an accurate and up to date exchange of information with relevant persons.
2 Assess security risk situation.	2.1 Assessment of security risk situation is conducted in accordance with organisational procedures. 2.2 Security risk situation is assessed for degree of risk to persons, property and premises. 2.3 Appropriate risk control measures to ensure the safety and security of persons, property and premises are determined. 2.4 Suitable equipment and resource requirements appropriate to security risk situation are determined. 2.5 Specialist advice is sought as required in accordance with organisational procedures.
3 Determine response options.	3.1 Options for response to security risk situation are evaluated and determined. 3.2 Response is within the scope of own responsibility, competence and authority. 3.3 Response maximises the safety and security of persons, property and premises. 3.4 Response involves the appropriate selection and efficient use of equipment and resources. 3.5 Relevant documentation is completed and securely maintained with due regard to confidentiality in accordance with organisational procedures.

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

- assess information and determine response appropriate to security risk situation
- communicate effectively with people from different social, cultural and ethnic backgrounds and of varying physical and mental abilities
- communicate using appropriate channels and clear and concise language
- conduct risk assessment of security risk situation
- determine suitable security and personal protection equipment
- facilitate commonsense solutions within operating parameters
- identify and comply with applicable legal and procedural requirements including licensing requirements
- identify and comply with security incident response procedures
- identify support and assistance requirements
- operate security and communications equipment.

Required knowledge

- approved communication terminology and codes and signals
- emergency and evacuation procedures and instructions
- instructions and procedures for responding to security risk situations
- observation and monitoring techniques
- operational functions and procedures for the use of communications, security and personal protection equipment
- phonetic alphabet
- principles of effective communication including interpersonal techniques
- procedures and requirements for documenting security incidents
- range of available resources and equipment
- range of potential security incidents and appropriate responses
- reporting processes
- risk assessment processes
- structure and responsibilities of the emergency services agencies.

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:

- determining response options which are most effective for the security risk
- determining response options within specified legal and strategic limits
- identifying current and potential risk factors and their impact on the security risk situation
- interpreting and complying with legal and procedural requirements including licensing requirements
- reviewing and adjusting response strategies to meet changing circumstances
- using appropriate communication modes and terminology to receive and convey information.

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 could be assessed using the following methods of assessment:

- observation of processes and procedures
- 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
 - Occupational Health and Safety (OHS)
- relevant industry codes of practice
- trespass and the removal of persons
- use of restraints and weapons:
 - batons
 - firearms

Relevant legislation may include:

- handcuffs
- spray.
- Crimes Act 1900
- Firearms Act 1996 and Firearms (General) Regulations 1997
- general principles of Common Law
- Inclosed Lands Protection Act 1901
- Law Enforcement (Powers and Responsibilities) Act 2002
- Liquor Act 1982
- Listening Devices Act 1984
- Registered Clubs Act 1976
- Security Industry Act 1997 and Regulations 1998
- Trade Practices Act
- Workplace Surveillance Act 2005.

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.

Security risk situation may relate to:

- biological hazards
- chemical spills
- electrical faults
- explosives
- injury to personnel
- noise, light, heat, smoke
- persons carrying weapons
- persons causing a public nuisance
- persons demonstrating suspicious behaviour
- persons suffering from emotional or physical distress
- persons under the influence of intoxicating substances

- persons with criminal intent
 - persons, vehicles and equipment in unsuitable locations
 - suspicious packages or substances
 - terrorism
 - violence or physical threats.
- Environmental factors*** may relate to:
- access to assistance and resources
 - availability of exits and opportunities for escape
 - crowds
 - different degrees of light including low light and darkness
 - presence of several sources of threat
 - time of day
 - weather.
- Communication channels and processes may relate to:***
- direct line supervision paths
 - established communication protocols
 - formal communication pathways
 - lateral supervision paths
 - organisational communication networks
 - verbal and non-verbal communication procedures eg pro-words, phonetic alphabet, call signs, coded messages, use of abbreviations, hand signals.
- Relevant persons*** may include:
- clients
 - colleagues
 - emergency services personnel
 - supervisor.
- Factors for assessment may include:***
- available resources including emergency support, team back-up or security equipment
 - known information about persons involved in the security risk
 - known information about the circumstances of the security risk
 - observation of the environment and physical conditions
 - options for controlling and defusing security risk
 - potential triggers for escalation of security risk
 - the nature of the security risk.
- Resources and equipment may include:***
- communications equipment
 - pager
 - portable and mounted two-way radio
 - telephone and mobile phone
 - maps
 - pen and security notebook
 - personal protection equipment
 - security equipment

Response may involve:

- restraints
- weapons
- security personnel and specialist services
- transport.
- defusing the situation
- evacuating the premises
- isolating area of potential risk
- isolating risk
- notifying relevant emergency services agencies
- providing access for emergency services
- provision of first aid
- request for support and assistance
- restraint of person
- tactical withdrawal
- use of batons, handcuffs or spray
- use of empty hand techniques
- use of negotiation techniques
- use of restraints.

Documentation may include:

- activity logs
- incident reports
- request for assistance forms
- vehicle and personnel movements
- written and electronic reports.

Unit Sector(s)

Unit sector Security

Competency field

Competency field Operations