Australian Government

Department of Education, Employment and Workplace Relations

CPPSEC4004A Monitor and review security operations

Release: 1

CPPSEC4004A Monitor and review security operations

Modification History

Not Applicable

Unit Descriptor

Unit descriptor

This unit of competency specifies the outcomes required to supervise field staff during the conduct of security operations. It requires the ability to source and apply security information, organise equipment and resources, address operational problems, and evaluate operational effectiveness.

This unit may form part of the licensing requirements for persons responsible for supervising security 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 supervision of security options in a security environment other than a control room. 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 ***bold italicised*** 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 Prepare for security operations.	1.1 Applicable provisions of ***legislative*** and ***organisational requirements***, and ***relevant standards*** for the implementation of security operations are identified and complied with.
	1.2 ***Assignment instructions*** and ***relevant information*** are obtained and reviewed.
	1.3 ***Security systems*** and technology required to monitor security operations are confirmed and checked for operational effectiveness.
	1.4 ***Equipment and resource requirements*** are determined and organised in accordance with organisational procedures.
	1.5 ***Communication channels and processes*** are confirmed with ***relevant persons***.
	1.6 Occupational Health and Safety (OHS) issues are identified and appropriate ***risk*** control measures implemented in accordance with organisational requirements.
2 Monitor security operations.	2.1 Security operations are systematically ***monitored*** in accordance with organisational procedures.
	2.2 Security systems and technology are used in accordance with manufacturer's instructions.
	2.3 ***Factors*** affecting the achievement of security operations are identified and recommendations for variation to operational plan are confirmed with relevant persons.
	2.4 Requests for ***assistance*** are received, confirmed and organised in accordance with organisational procedures.
	2.5 Specialist advice is sought as required in accordance with organisational procedures.
	2.6 Operational information is recorded and reported in accordance with organisational procedures.
3 Review security operations.	3.1 A process of continual assessment is applied to review and evaluate effectiveness of security operations.
	3.2 Briefings and debriefings are planned, scheduled and conducted in accordance with organisational procedures.
	3.3 Incident observations are provided accurately and constructively and ***opportunities for improvement*** are identified to inform future practice.
	3.4 Review findings and recommendations are prepared and presented to relevant persons in accordance with organisational procedures.

ELEMENT	PERFORMANCE CRITERIA
	3.5 Presented information uses clear and concise language and meets organisational standards of style, format and accuracy.
	3.6 Relevant ***documentation*** is completed and securely maintained in accordance with organisational procedures.

Required Skills and Knowledge

REQUIRED SKILLS AND KNOWLEDGE

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

Required skills

- coaching and mentoring to provide support to colleagues
- display team leadership
- estimate and calculate resource and equipment requirements
- facilitate review and debrief processes
- interpret and comply with relevant legislative, regulatory and licensing requirements
- interpret security codes and alarm signals and implement responses maintain communication with field staff
- maintain effective client and colleague relationships
- monitor and manage OHS in the workplace environment
- prioritise work tasks and maintain schedules
- supervise field staff and security operations.

Required knowledge

- applicable provisions of legislation relevant to security operations including OHS and licensing and certification
- briefing and debriefing techniques
- communication protocols and terminology
- emergency and evacuation procedures
- operational principles and functions of security technology and equipment
- principles of AS/NZS 4360: 2004 Risk management and related guidelines
- principles of effective communication and interpersonal techniques
- problem-solving strategies
- reporting, documentation requirements and processes
- security issues and incident management techniques
- security risk assessment methods
- teamwork principles and strategies

REQUIRED SKILLS AND KNOWLEDGE

- time management principles.

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:

- accurately completing, preparing and presenting documentation related to security operations in a suitable style and format to relevant personnel for review
- accurately interpreting, communicating and implementing assignment instructions
- identifying problems or issues with operational efficiency and implementing suitable contingency measures
- maintaining communication with field staff using established communication channels and equipment
- monitoring work of security personnel to ensure the efficiency and effectiveness of security operations is maintained
- reviewing and evaluating effectiveness of security operations through a process of continual assessment, feedback and review.

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 plain English version of relevant statutes and procedures
- access to a registered provider of assessment services
- access to a suitable venue and equipment
- 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
  - OHS
- relevant industry codes of practice
- trespass and the removal of persons
- use of restraints and weapons:
  - batons
  - firearms
  - handcuffs
  - spray.

Relevant legislation may include:

- 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
- Telecommunications Act
- 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.

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.

Assignment instructions may include:	• assignment purpose and objective • assignment tasks and procedures • assignment timeframe • client information • incident and security risk response procedures • personal presentation • reporting and documentation requirements • resource and equipment requirements.
***Relevant information* may include**:	• client competition • core business functions • key stakeholders • nature of client business and type of industry • scale of operations • size of company and number of employees.
Security systems may include:	• access control systems • acoustic sensors • automatic entrance and exit devices • biometric devices • electronic field detection systems • infra-red sensors • intelligent building systems • intruder alarm systems • motion sensors • movement detectors.

Equipment and resources may include:	• communication equipment:
	  • pager
	  • portable and mounted two-way radio

- telephone and mobile phone
- defensive equipment:
  - batons, firearm, and the relevant licenses and permits
- maps
- pen and security notebook
- personal protection equipment
- security equipment:
  - alarms and signals
  - electronic screening equipment
  - motion sensors
  - personal duress alarms
  - static alarms
  - video cameras and monitors
- security personnel and specialist services
- transport.

***Communication channels and processes* may include**:

- 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 and agencies
- human resource personnel
- management
- legal representatives.

***Risk* relates to**:

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

Security risks may relate to:

- biological hazards
- chemical spills
- client contact
- electrical faults
- explosives
- financial viability
- 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
- property or people
- security systems
- suspicious packages or substances
- systems or process failures
- terrorism
- violence or physical threats.

Monitoring **may be conducted**:

- using an audio recording device
- by camera (eg optical recording device)
- electronically and digitally
- visually (eg observation).

Factors **may include**:

- access to resources and materials
- budget constraints
- competing work demands
- environmental factors (eg time, weather)
- technology or equipment breakdowns
- unforeseen incidents
- workplace environment hazards and risks.

Assistance **may include**:

- back-up support
- explaining and clarifying
- problem-solving
- providing encouragement
- providing feedback
- undertaking extra tasks.

Opportunities for improvement **may relate to**:

- gaps in operational coverage as determined in internal auditing or assessment processes
- on-the-job instruction
- operational effectiveness assessment
- organisational assessment and evaluations provision of learning opportunities
- relevant organisational changes such as need to alter policies or procedures
- structured feedback.

Documentation **may include**:

- activity reports
- field notes
- incident reports
- radio and telephone communication records
- request for assistance forms

- security logs
- shift reference files
- vehicle and personnel movements.

Unit Sector(s)

Unit sector Security

Competency field

Competency field Security and risk management