



Australian Government

Department of Education, Employment and Workplace Relations

CPPSEC4010A Manage monitoring centres

Release: 1

CPPSEC4010A Manage monitoring centres

Modification History

Not Applicable

Unit Descriptor

Unit descriptor This unit of competency specifies the outcomes required to organise and control a security monitoring centre. It requires the ability to manage staffing and resources, implement and review operations, and promote continuous improvement strategies.

This unit may form part of the licensing requirements for persons responsible for managing the operations of security monitoring centres 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 management of security operations from a monitoring centre 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 Plan operational priorities.	1.1 Applicable provisions of legislative and organisational requirements relevant to managing monitor centres are identified and complied with. 1.2 Operational plans and other relevant information are accessed and reviewed. 1.3 Preventative and breakdown maintenance arrangements for security systems and technology are determined and confirmed. 1.4 Procedures for the allocation and replacement of security systems are determined and confirmed. 1.5 Designated operational roles and responsibilities are determined and confirmed with relevant persons. 1.6 Communication channels and processes are determined and confirmed with relevant persons. 1.7 Operational budgets and delegations are confirmed and maintained within agreed limits and allocations. 1.8 Occupational Health and Safety (OHS) issues are identified and appropriate risk control measures implemented in accordance with organisational requirements.
2 Monitor operations.	2.1 Performance of security systems and technology is monitored for operational efficiency and effectiveness. 2.2 Security operations are systematically monitored and reviewed against operational plans. 2.3 Implementation of security operations are confirmed within scope and competence of designated roles and responsibilities. 2.4 Operational plans are modified as required to maintain security requirements and communicated to relevant persons. 2.5 Assistance requirements for relevant persons are identified and actioned in accordance with organisational procedures. 2.6 Security operations are conducted in accordance with relevant OHS, legislative and organisational requirements.
3 Review operations.	3.1 A process of continual assessment is applied to review and evaluate effectiveness of security operations. 3.2 Operational outcomes and performance reports are reviewed and evaluated to identify opportunities for improvement. 3.3 Review findings and recommendations to inform future

ELEMENT**PERFORMANCE CRITERIA**

practice are prepared and presented to relevant persons in accordance with organisational procedures.

3.4 Presented information uses clear and concise language and meets organisational standards of style, format and accuracy.

3.5 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

- assess and implement appropriate response to received information
- coaching and mentoring to provide support to colleagues
- communicate in a clear and concise manner using appropriate terminology
- deliver project objectives within budget constraints
- develop and manage key performance indicators
- estimate and calculate resource and assistance requirements
- identify and diagnose faults or deficiencies in operation of security systems
- implement safe and environmentally sound workplace practices
- interpret security codes and alarm signals
- maintain operations within budgetary parameters
- monitor systems and monitor performance
- monitor, evaluate and interpret data and information
- negotiation
- operate and maintain a range of security systems
- phonetic alphabet
- prepare and present written/computer-based information
- read and interpret technical data and specifications
- relate to people from a range of social, cultural and ethnic backgrounds and varying physical and mental abilities
- risk assess incidents
- write reports and complete documentation.

Required knowledge

- approved communication terminology and codes and signals
- back-up procedures

REQUIRED SKILLS AND KNOWLEDGE

- change of shift procedures
- common faults and malfunctions in security systems
- emergency procedures
- interviewing, counselling, negotiation and mediation techniques
- management and leadership styles and culture
- operational principles and functions of security systems and software/hardware
- operations management
- principles of change management
- problem solving strategies
- range of security risk or incident situations and appropriate response procedures
- reporting and documentation procedures
- risk and conflict management
- risk assessment methods
- types of alarm systems and equipment
- workplace environmental and OHS hazards and risks.

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:

- effectively managing staff, systems and equipment resources to achieve operational plans for a monitoring centre within legislative parameters
- communicating with staff and colleagues to ensure the ongoing effectiveness of information receipt, interpretation and transmission
- identifying communication and resourcing problems and implementing learning opportunities for staff and continuous improvement strategies for monitoring operations
- accurately preparing and completing monitoring records and reports in compliance with legal parameters.

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:***
- Australian standards and quality assurance requirements
 - crowd control and control of persons under the influence of intoxicating substances
 - general 'duty of care' responsibilities
 - 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
 - telecommunications
 - trespass and the removal of persons.

- 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 information may include:***
- alarm response procedures
 - alarm service information
 - applicable legislation and codes of practice
 - communication and reporting channels
 - manufacturers specifications
 - operational plans
 - operations manuals

- personnel schedules
- terms of reference.
- alternative and backup systems and procedures
- Preventative and breakdown maintenance arrangements may include:***
 - emergency response plans
 - preventative maintenance plans
 - programmed maintenance.
- Security systems may relate to:***
 - access control systems
 - electronic, audio, visual, digital surveillance and recording systems
 - fire detection systems
 - intruder detection and alarm systems
 - process control or building management systems.
- Relevant persons may include:***
 - clients
 - colleagues
 - emergency services personnel
 - field staff
 - management
 - technical personnel.
- 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.
- Risk relates to:***
 - the chance of something happening that will have an impact on objectives.
- Documentation may include:***
 - activity logs
 - radio and telephone records
 - records of conversation
 - running sheets
 - security logs
 - security systems faults and diagnosis
 - situation reports
 - testing and inspection results
 - written and computer-based reports.

Unit Sector(s)

Unit sector Security

Competency field

Competency field Security and risk management