Australian Government

Department of Education, Employment and Workplace Relations

CSCSAS401A Monitor and review security systems

Revision Number: 2

CSCSAS401A Monitor and review security systems

Modification History

CSCSAS401A Release 2: Layout adjusted. No changes to content.
CSCSAS401A Release 1: Primary release.

Unit Descriptor

This unit of competency describes the outcomes required to supervise the security and safety of a secure custodial environment.

Application of the Unit

This unit applies to all people working with offenders/detainees in prisons, secure custodial centres and community facilities under custodial supervision, with responsibility for coordinating and monitoring security functions and the effectiveness of the local system. Variables will determine different applications of the standards depending on the nature and complexity of security requirements, security ratings and defined work role and responsibilities.
The language used in this unit implies an institutional setting. Adaptation of the language will be necessary to reflect the practices of non-institutional settings and work sites. Customisation should occur through the introduction of specific organisation security equipment, functions and procedures.

Licensing/Regulatory Information

Not applicable.

Pre-Requisites

Not applicable.

Employability Skills Information

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 and/or the range statement. Assessment of performance is to be consistent with the evidence guide.

Elements and Performance Criteria

ELEMENT	PERFORMANCE CRITERIA
1 Monitor the effectiveness of security.	1.1 Ensure that staff members are rostered and duties assigned to maintain effective operation of the ***security system***.
	1.2 Routinely check security information and reports according to ***organisational requirements***.
	1.3 Routinely assess the safety and welfare of all individuals regarding ***possible hazards*** and in line with organisational procedures.
	1.4 Routinely monitor reports on effective working of equipment, and inaccuracies and malfunctions.
	1.5 Ensure that effective communication and information exchange are maintained between team members, units and key centres in the organisation.
	1.6 Report all security concerns promptly, clearly and accurately to management and key specialist teams.
2 Support team members.	2.1 Provide team members with current information necessary to ensure the effective maintenance of the security system.
	2.2 Confirm and interpret security information and procedures and promote a positive approach to change with team members.
	2.3 Identify and analyse the resources needed by team members to maintain the security system and provide advice to management.
	2.4 Identify the skills and performance development required to maintain the security system and provide advice to management and specialist units.
	2.5 Promote the safety and welfare of offenders, team members and the public at all times and in components of the security system.
3 Coordinate emergency response.	3.1 Interpret alarm signals correctly and immediately and ***respond*** according to procedures and degree of urgency.
	3.2 Coordinate team response according to the status of the emergency, the safety and welfare of individuals and emergency response procedures.
	3.3 Assess the risk of escalation of incidents and coordinate team action to minimise risks.
	3.4 Use codes and call systems accurately and effectively according to organisational procedures.
	3.5 Complete security and incident reports, records and

ELEMENT	PERFORMANCE CRITERIA
	registers accurately and comprehensively and provide reports to management or special inquiries.
	3.6 Coordinate debriefing and post-emergency analysis according to organisational guidelines and team practices.

Required Skills and Knowledge

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

Required skills:

- coordinating staff rosters and duty assignments
- supervising, coordinating and monitoring all security equipment and strategies required by the security system of the work site and consistent with work role, responsibilities and delegation
- anticipating and interpreting the efficiencies and risks of the security system and incidents against security plans and procedures
- providing advice on the implementation of security technology and the resources required to maintain the security system
- coordinating team responses at incidents and deploying back-up and specialist resources in response to incidents and alarms
- coping with a high degree of pressure and using a range of communication equipment and information sources during incidents
- decision-making skills when evaluating security incidents and potential risks or emergencies.

Required knowledge:

- organisation's security plan, procedures and guidelines and the requirements for all security equipment and technology
- organisation's procedures and guidelines for the use of security, surveillance and information equipment
- organisation's procedures and guidelines for rostering staff and assigning duties
- organisation's emergency response system and procedures
- organisation's codes and alarm signals
- organisation's records and information system
- Environmental or sustainability legislation, regulations and codes of practice applicable to industry
- reporting requirements, including procedures, protocols and chain of command
- occupational health and safety policy relevant to security, workplace pressure and incident debriefing
- code of conduct and methods of promoting a positive response to change.

Evidence Guide

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

Overview of assessment

Assessment of this unit should be based on evidence produced from routine work applications and performance. This unit contains requirements specific to the organisation and the role and responsibility of workers and should be assessed in an organisation-determined learning process with application in the workplace where possible or where necessary, in structured simulation.

Evidence needs to be gathered over time in a range of contexts to ensure the person can achieve the unit outcome and/or apply the principles in a different situation or change of environment.

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

In addition to integrated demonstration of the elements and their related performance criteria, look for evidence that confirms:

- the knowledge requirements of this unit
- the skill requirements of this unit
- application of employability skills as they relate to this unit
- ability to monitor and review security systems in a range of (two or more) contexts or occasions, over time.

Context of and specific resources for assessment

Valid assessment of this unit requires:

- a workplace environment or one that closely resembles normal work practice and replicates the range of conditions likely to be encountered when monitoring and reviewing the security system, including coping with difficulties, irregularities and breakdowns in routine
- copies of legislation, policies, procedures and guidelines relating to supervision, coordination and monitoring of the security system
- access to appropriate learning and assessment support when required.

Method of assessment

Evidence must include observation and information generated in the workplace as well as observation of performance in routine work functions or, where this is not possible, in a simulated exercise to confirm the transferability of the competencies.

The following assessment methods are suggested:

- observation of performance in routine workplace activities within a range of agreed responsibilities and in various work locations
- written and/or oral questioning to assess knowledge and understanding
- completion of workplace documents and reports produced as part of routine work activities
- third-party reports from experienced practitioners
- completion of performance feedback from supervisors and colleagues
- scenarios
- simulations or role plays.

Guidance information for assessment

Assessment methods should reflect workplace demands, and any identified special needs of the candidate, including language and literacy implications and cultural factors that may affect responses to the questions.

In all cases where practical assessment is used it will be combined with targeted questioning to assess the underpinning knowledge.

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 in the performance criteria is detailed below. Add any 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.

Components of the ***security system*** may include:

- organisation's codes and alarm signals
- communication technology and equipment
- management of access and exit
- management of visitors
- management of vehicles
- surveillance methods and technology
- central control
- key control
- rosters and duties
- counts and musters
- searches
- registers
- escorts and transfers
- control and use of defensive equipment and firearms
- staff duties and roster
- incident response and debriefing.

Organisational requirements may include:

- legal and organisational policy and procedures, including personnel practices and guidelines
- organisational goals, objectives, plans, systems and processes
- legislation relevant to monitoring activities, incident or response, and collection and presentation of evidence
- employer and employee rights and responsibilities
- business and performance plans
- policies and procedures relating to own role, responsibility and delegation
- quality and continuous improvement processes and standards
- client service standards
- defined resource parameters
- occupational health and safety policies, procedures and guidelines
- emergency and evacuation procedures
- duty of care, code of conduct and code of ethics

	• access and equity policy, principles and practice • records and information systems and processes • communication channels and reporting procedures • professional conduct, such as grooming, personal presence, uniform standards, attitude and professional expectations of staff.
Possible hazards may include:	• deficient or ineffective security arrangements • loss of communications • unreported faults • unsafe practices • used emergency equipment not being replaced or replenished • blocking egress • emergency lighting and or exit lighting being damaged, missing or under service • interference with radio transmissions or alarm signals.
Responding to alarms and incidents may involve:	• notifying relevant personnel • notifying emergency services • dispatching field support staff • executing standard operating procedures for the occurrence of particular events • applying restraints according to organisational requirements.

Unit Sector(s)

Safety and security.

Competency field

Not applicable.