



Australian Government

Department of Education, Employment and Workplace Relations

CPPSEC3035A Identify technical security requirements

Release: 1

CPPSEC3035A Identify technical security requirements

Modification History

Not Applicable

Unit Descriptor

Unit descriptor

This unit of competency specifies the outcomes required to determine the technical security requirements for small domestic or commercial environments. It requires the ability to use appropriate methods and techniques to gather and assess information to accurately determine and recommend security options to meet identified client needs.

This unit may form part of the licensing requirements for persons providing advice, solutions or strategies to minimise security risks 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 technical security requirements for domestic and commercial environments. 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 Prepare to identify security requirements.	1.1 Applicable provisions of legislative and organisational requirements relevant to assignment instructions are identified and complied with. 1.2 Assignment instructions are obtained, reviewed and clarified as required with relevant persons. 1.3 Consultative processes are conducted to establish the scope and immediate, short and long term security requirements of the client. 1.4 Appropriate communication and interpersonal techniques are used which reflect sensitivity to individual social and cultural differences. 1.5 Specialist resources and sources of information are accessed and assessed as required. 1.6 Limitations in determining client needs are recognised and specialist advice is sought as required.
2 Identify security requirements.	2.1 Site access and specific site requirements are identified and appropriate arrangements made in accordance with organisational procedures. 2.2 Relevant information appropriate to assignment instructions is gathered from reliable sources in accordance with organisational procedures. 2.3 A site assessment is conducted and documented in accordance with organisational procedures. 2.4 Site security risk factors are identified and assessed in accordance with organisational procedures.
3 Document security requirements.	3.1 Business equipment and technology is used to prepare and present information in required format and style. 3.2 An assessment of client security requirements is completed within designated timeframes and presented for review to relevant persons. 3.3 Assessment contains comprehensive information about available security equipment, systems and services to meet identified security requirements. 3.4 Recommendations and alternative options are prioritised and supported by verifiable evidence. 3.5 Information is securely maintained with due regard to client confidentiality.

Required Skills and Knowledge

REQUIRED SKILLS AND KNOWLEDGE

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

Required skills

- apply active listening
- apply basic numeracy techniques
- apply safe and efficient work practices
- assess existing site security systems
- communicate in a clear and concise manner
- comply with relevant legislative and regulatory requirements including licensing
- determine site technical security requirements
- enter data using basic keyboarding skills
- identify potential security threats to people, property and premises
- organise work tasks in a methodical manner
- prepare and present reports
- present a professional image to members of the public and colleagues
- prioritise tasks and complete work within designated timeframes
- read and interpret plans, designs and specifications
- relate to people from different social and cultural backgrounds.

Required knowledge

- basic problem solving strategies
- building construction methods and types
- duty of care
- legislative and organisational policies and procedures including licensing requirements
- operational principles of business equipment and information technology
- organisational and client confidentiality requirements
- principles of effective communication
- procedures to assess security systems including security manpower
- relevant industry standards and codes of conduct
- reporting procedures and documentation requirements and processes
- security risk assessment methods
- types and functions of technical security equipment, systems and services.

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:

- identifying applicable legislative requirements which will impact on security assessment and accurately completing all documentation
- preparing a summary of assessed client needs and prioritising security recommendations in a format suitable for review
- sourcing and gathering relevant information and conducting a comprehensive site assessment to identify client assets, activities and existing security arrangements
- using appropriate methods to determine suitable technical security requirements and options to meet client needs and expectations
- using appropriate security assessment methods to determine client security requirements.

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:

- applicable commonwealth, state and territory legislation which affects work such as:
 - workplace safety
 - environmental issues
 - equal employment opportunity
 - industrial relations
 - anti-discrimination and diversity
- Australian building codes and regulations
- Australian Communications Authority cabling standards
- Australian standards and quality assurance requirements
- award and enterprise agreements
- evidence collection
- freedom of information
- licensing arrangements and certification requirements
- privacy requirements
- relevant industry codes of practice
- telecommunications
- trade practices.

Organisational requirements may

- access and equity policies, principles and practices
- business and performance plans

relate to:

- 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
- Occupational Health and Safety (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.

Assignment instructions may include:

- access to site, security clearance and specific site requirements
- budget constraints
- equipment requirements:
 - business equipment
 - communication equipment
- reporting and documentation requirements
- specific client requirements
- timeframes
- work schedules and completion dates
- work tasks and procedures.

Relevant persons may include:

- clients
- colleagues
- engineers and technicians
- equipment and systems manufacturers
- security consultants
- security personnel
- site managers or project managers
- supervisor.

Scope may relate to:

- conformance with insurance requirements
- legislative, regulatory or industry requirements
- protection of persons, property or assets.

Client may be:

- building supervisor
- government authorities
- manager
- project manager

Interpersonal techniques may involve:

- property agent
- property owner
- tenant.
- 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.

Social and cultural differences may relate to:

- dress and personal presentation
- food
- language
- religion
- social conventions
- traditional practices
- values and beliefs.

Site access and specific site requirements may relate to:

- access and egress points
- access codes, keys or passes
- building codes and regulations
- heritage requirements
- noise control
- obtaining security clearance
- OHS requirements
- time of access to site
- union requirements.

Relevant information may include:

- areas requiring a higher level of security
- business and operational plans
- core business activities and functions
- current and proposed operating environments, assets and systems
- current management strategies
- existing security systems and equipment
- insurance policies

- Site assessment may involve identifying:***
- security incident history.
 - access and egress patterns
 - existing security equipment and systems
 - floor plan
 - site restrictions and regulations
 - type and condition of building structures.
- Assessment documentation may include:***
- checklists
 - client briefs
 - existing security equipment and systems
 - floor plans
 - recommendations
 - specifications
 - written and electronic reports.
- Security risks factors may relate to:***
- adequacy of street lighting
 - break-in
 - burglary
 - client habits eg doors left unlocked
 - deliberate or accidental damage
 - entry points screened from public view
 - external doors without deadlocks or with hinges opening outward
 - neighbourhood crime rating
 - pilferage
 - proximity of other buildings
 - sabotage
 - theft
 - threats of loss, harm or damage to persons or property
 - traffic flow
 - trespass
 - unauthorised access
 - unsecured windows and doors
 - vandalism.
- Business equipment and technology may include:***
- calculators
 - facsimile machines
 - internet
 - personal schedulers
 - photocopiers
 - printers
 - standard commercial computer software and hardware
 - telephones.

Unit Sector(s)

Unit sector Security

Competency field

Competency field Technical security