Australian Government

Department of Education, Employment and Workplace Relations

CPPSEC4003A Advise on security needs

Release: 1

CPPSEC4003A Advise on security needs

Modification History

Not Applicable

Unit Descriptor

Unit descriptor

This unit of competency specifies the outcomes required to determine a client's security requirements and security risk. It requires the ability to provide accurate security services recommendations and alternative options, analyse security risk, present advice in a suitable format, and monitor and evaluate client feedback.

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 provision of advice, for example, a security consultant. 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 Determine client needs.	1.1 Applicable ***legislative*** and ***organisational requirements***, and ***relevant standards*** for providing security advice are identified and complied with. 1.2 Consultative processes are conducted to determine and verify the immediate, short and long term security needs and expectations of the ***client***. 1.3 Appropriate communication and ***interpersonal techniques*** are used which reflect sensitivity to individual ***social and cultural differences***. 1.4 Security ***risk*** assessment is undertaken in accordance with organisational procedures. 1.5 Existing or potential security issues are identified, anticipated and assessed to determine impact on ***client requirements***. 1.6 Specialist resources and sources of information are accessed and assessed as required. 1.7 Limitations in determining client needs are recognised and specialist advice is sought as required.
2 Provide advice.	2.1 ***Business equipment*** is used to prepare and present advice in required format and style. 2.2 Advice contains comprehensive information about available security products and services to meet identified security needs. 2.3 Recommendations and alternative options are prioritised and supported by verifiable evidence. 2.4 Advice is presented for review in accordance with organisational procedures. 2.5 Feedback on suitability and sufficiency of advice is obtained and reviewed for improved future processes. 2.6 Information is securely maintained with due regard to client confidentiality.
3 Evaluate effectiveness of advice.	3.1 Client service delivery is reviewed and evaluated to ensure client needs are satisfied. 3.2 Client satisfaction with service delivery is reviewed using verifiable data in accordance with organisational procedures. 3.3 Changes necessary to maintain client service standards are identified and recommendations to modify advice are presented to ***relevant persons***. 3.4 Industry trends are monitored and options for upgrading client services are presented to relevant persons.

ELEMENT	PERFORMANCE CRITERIA
	3.5 Relevant documentation is completed and processed 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

- apply active listening
- apply safe and efficient work practices
- assess security requirements
- coaching and mentoring to provide support to colleagues
- communicate in a clear and concise manner
- comply with relevant legislative and regulatory requirements
- enter data using basic keyboarding skills
- identify potential security threats to people, property and premises
- negotiation
- 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
- risk assessment
- seek feedback and take appropriate action.

Required knowledge

- applicable legislation relevant to implementing security services
- basic problem solving strategies
- basic requirements for installation of security systems
- building construction methods and types
- duty of care
- guidelines for use of force and restraints
- interpretation of security systems, including how and where security manpower can be effectively utilised
- operational principles of information technology for security systems and equipment
- organisational and client confidentiality requirements
- principles of AS/NZS 4360: 2004 Risk management and related guidelines

REQUIRED SKILLS AND KNOWLEDGE

- principles of effective communication
- relevant industry standards and codes of conduct
- reporting procedures and documentation requirements and processes
- security risk assessment methods
- types and functions of a range of security equipment and systems.

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 and concisely completing all necessary documentation summarising security requirements and assessed security risk
- accurately assessing client security requirements and determining appropriate security options to meet client needs and expectations
- monitoring client services, evaluating feedback and modifying services as required
- providing and presenting in a suitable format appropriate security recommendations and alternative options to benefit client and organisation
- using appropriate security assessment methods to determine client and risk assessment 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:

- 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
  - handcuffs
  - spray.

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.

Client may be:

- agent
- building supervisor
- government and legal instruments or agencies
- manager
- owner
- project manager
- property agent
- tenant.

Interpersonal techniques may involve:

- 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**:

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

***Risk* relates to**:

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

Security *risks* may relate to:

- assault or harm
- break-in
- burglary
- deliberate or accidental damage

- pilferage
- sabotage
- theft
- threats of loss, harm or damage to persons or property
- trespass
- unauthorised access
- vandalism.

***Client requirements* may include**:

- assets and areas to be protected
- available security system options
- budgetary parameters
- conformance with insurance, government or other requirements
- property or assets
- protection of persons
- systems or function requirements.

Business equipment and technology may include:

- calculators
- facsimile machines
- internet
- standard commercial computer software and hardware
- telephones.

***Relevant persons* may include**:

- client
- colleagues
- management
- manufacturers
- other professional or technical staff
- security consultants.

Unit Sector(s)

Unit sector Security

Competency field

Competency field Security and risk management