Australian Government

Department of Education, Employment and Workplace Relations

CPPSEC4012A Identify and assess security of assets

Release: 1

CPPSEC4012A Identify and assess security of assets

Modification History

Not Applicable

Unit Descriptor

Unit descriptor

This unit of competency specifies the outcomes required to conduct a security assessment and market evaluation of assets. It requires the ability to research, analyse and present information and data, and evaluate security control measures.

This unit may form part of the licensing requirements for persons engaged in security assessment 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 security assessment and valuation of assets. 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 List assets.	1.1 Applicable provisions of ***legislative*** and ***organisational requirements***, and ***relevant standards*** for security assessment activities are identified and complied with.
	1.2 Advice is sought from authorised ***relevant persons*** on the location and nature of all ***assets***.
	1.3 ***Source documents*** are obtained and validated in accordance with legislative requirements.
	1.4 List of assets is reviewed and confirmed in consultation with client using effective ***interpersonal techniques***.
	1.5 Asset listing is developed in a format suitable for analysis, interpretation and dissemination in accordance with requirements of relevant standards.
2 Confirm status of assets.	2.1 ***Status of assets*** is evaluated based on information obtained from source documents.
	2.2 Findings are supported by valid and reliable evidence in accordance with relevant standards.
	2.3 ***Market value*** of assets is calculated and confirmed in accordance with client instructions and organisational procedures.
	2.4 Comprehensive asset valuation is developed based on assessment of all ***factors***.
3 Assess vulnerability of assets.	3.1 ***Access to assets*** and information on existing and planned ***security measures*** and ***risk*** is confirmed with relevant persons.
	3.2 All ***treatments*** and incident reporting mechanisms arranged on behalf of the organisation are identified and an audit conducted.
	3.3 ***Operating parameters*** of identified treatments are obtained from relevant persons in accordance with legislative requirements.
	3.4 Operational effectiveness of treatments are assessed through ***planned testing*** in accordance with relevant standards and organisational procedures.
	3.5 Failure or potential failure of existing control mechanisms are immediately reported to client.
4 Present information.	4.1 Assessment details including asset valuation, vulnerability and any recommendations are documented in accordance with ***organisational standards***.
	4.2 ***Report*** is presented to relevant persons within specified time and budget.
	4.4 ***Feedback*** on client satisfaction with service delivery is

ELEMENT	PERFORMANCE CRITERIA
	sought and queries or areas of dissatisfaction responded to promptly.
	4.5 All information is securely maintained and stored 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

- accurately record and report information
- active listening and questioning
- assessment and analysis
- calculate market value of assets
- coaching and mentoring to provide support to colleagues
- data collection and analysis
- design of tools and questionnaires
- information technology
- observation
- planning
- read and interpret maps, plans and schematic drawings
- relate to people from a range of social, cultural and ethnic backgrounds and physical and mental abilities
- research.

Required knowledge

- auditing and assessment techniques and methodologies
- basic accounting procedures, such as depreciation methods for determining market value of assets
- broad application of security risk management
- legislation, standards, regulations and codes of practice applicable to valuing assets
- organisational or client standards and procedures for the presentation of information
- principles of AS/NZS 4360: 2004 Risk management and related guidelines
- processes for testing operational effectiveness of assets and treatments
- reporting procedures and documentation requirements and processes
- risk assessment techniques and processes
- sources of information for asset valuation.

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:

- obtaining and using information from a range of sources and consultative processes to develop an accurate listing of assets in compliance with client, organisational and legislative requirements
- accurately evaluating and confirming status, market value and vulnerability of assets using valid and reliable evidence in compliance with relevant standards
- using effective communication skills to obtain information and present information and reports.

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
- force continuum, use of force guidelines
- 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
  - Occupational Health and Safety (OHS)
- relevant industry codes of practice
- trespass and the removal of persons.

Organisational requirements may relate

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

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 • 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
	  • AS3911:1992 Guidelines for auditing quality systems
	  • HB 167:2006 Security Risk Management
	  • HB 436 Risk Management Guidelines - Companion to AS/NZS 4360
	  • HB 231:2000 Information security risk management guidelines.

Relevant persons may be:	• accountants • contractors • inventory or administration personnel • managers • operational personnel • security personnel • technicians.
***Assets* may include**:	• assets owned, leased or in the custody of an organisation • buildings • equipment • facilities • goodwill • information and documentation • information systems and sources

- intellectual property
- people
- reputation
- security systems.

***Source documents* may include**:

- asset register
- depreciation register
- employee records
- lease or hire purchase contracts
- organisation chart
- profit and loss analysis for an asset or division of the organisation
- those obtained from accounting personnel.

***Interpersonal techniques* may include**:

- active listening
- being respectful and non-discriminatory to others
- control of tone of voice and body language
- demonstrating flexibility and willingness to negotiate
- interpreting non-verbal and verbal messages
- maintaining professionalism
- providing and receiving constructive feedback
- questioning to clarify and confirm understanding
- two-way communication
- use of communication appropriate to cultural differences
- use of positive, confident and cooperative language.

***Status of assets* may relate to**:

- borrowing
- current condition of asset (damaged, in repair, lost, stolen, on leave, undergoing routine maintenance)
- held in custody
- hire
- importance
- lease
- ownership
- security.

***Market value* of assets may be based on**:

- assessment of purchase price
- depreciated value
- formal valuation
- replacement costs.

***Factors* which may influence value of assets may include**:

- dollar cost
- function
- harm to short or long term operation of the organisation
- importance to normal operation of the organisation
- replacement availability, time and cost
- the value of production or output lost as a result of loss

	of the asset.
***Access to assets* or sources of information may involve**:	• entry to locations where assets are kept, used or stored • entry to storage facilities • obtaining authority to access restricted data, areas or personnel • obtaining relevant security clearance • on-site visits.
***Security measures* may relate to**:	• access control systems • Closed Circuit Television (CCTV) and monitoring systems • deployment or increase of security personnel • safes, vaults and locking mechanisms • standard operating procedures for security of assets.
***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.
***Treatments* may relate to**:	• additional personnel • contracted contingency services • identified countermeasures • internal contingency plans • risk reduction strategies • use of stored resources

	• use of superseded equipment.
An *audit* may be completed by using:	• inspection of records and documents • internal auditing procedures as outlined in AS3911:1992 Guidelines for auditing quality systems • interviews • monitoring and inspecting procedures and processes • professional internal or external auditors • questionnaires • site visits and inspections.
***Operating parameters* may include**:	• adherence to procedures • adverse conditions for system efficiency • availability and condition of systems and equipment • availability and use of back-up systems • call out of support and specialist personnel • clarity of communication systems • fault-finding procedures • normal function of duties • OHS requirements • optimal conditions for system efficiency • reaction time • safe and timely deployment • sound and light intensity • standard operating procedures.
***Planned testing* may include**:	• computer modelling • conceptual analysis • controlled interruptions to normal operations • debriefing sessions • inspection • interception • interviews • penetration exercises • rehearsals • simulation and replication • testing of alarms, CCTV and other warning devices • testing or access control systems.
***Organisational standards for written information* may relate to**:	• ability to be used for legal purposes • accuracy of costings • appropriate level of literacy • format and presentation • relevance of written information • use of clear, concise language and plain English.

***Report* should include**:	• evidence and supporting materials to validate the findings • graphical representations of data • recommendations where applicable • summary of assessment objectives and outcomes • tables and information from approved data collection tools.
***Feedback* may be obtained through**:	• comments from client or colleagues • completion and analysis of formal client satisfaction survey • effectiveness of assessment outcomes in meeting assessment objectives • formal or informal performance discussion.

Unit Sector(s)

Unit sector Security

Competency field

Competency field Security and risk management