



Australian Government

Department of Education, Employment and Workplace Relations

CPPSEC4007A Assess threat

Release: 1

CPPSEC4007A Assess threat

Modification History

Not Applicable

Unit Descriptor

Unit descriptor	This unit of competency specifies the outcomes required to assess current, future and potential threats to identified assets or activities. It requires the ability to undertake an assessment of client operations, identify and analyse potential or existing threats, undertake a consequence analysis and present assessment findings. This unit may form part of the licensing requirements for persons engaged in threat 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 assessment of threats in a security 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 ***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 Undertake background assessment.	1.1 Applicable provisions of legislative and organisational requirements, and relevant standards for threat assessment activities are identified and complied with. 1.2 Client operations, goals and objectives are discussed and confirmed in consultation with relevant persons. 1.3 Relevant information is gathered from reliable sources and verified for accuracy. 1.4 A review is conducted of organisational assets and existing security arrangements to determine the range of potential or actual undesirable outcomes by following criteria in relevant standards. 1.5 Additional information is sourced as required from reliable and verifiable information sources.
2 Identify and analyse potential or existing threats.	2.1 Context for identifying threats is based on an accurate understanding of the threats to operational environments and core business operations of the client. 2.2 Potential causes and sources of potential or existing threats are identified based on an evaluation of gathered information and data. 2.3 Information gaps are identified and additional information is collected from appropriate sources to ensure all potentially relevant information is included in the process. 2.4 Assessment criteria for measuring level of potential or actual threat is developed in accordance with client terms of reference, relevant standards and organisational procedures. 2.5 Likelihood and realisation of threat is assessed against identified client information and data and organised in a format suitable for analysis and interpretation. 2.6 Threats to operational environments are systematically monitored to assess performance systems and processes with specific consideration given to changing roles, locations, and stability of operating environment.
3 Undertake consequence analysis.	3.1 Assessment criteria is agreed with relevant persons and used as a basis for measuring consequence analysis. 3.2 Assets and activities are assessed for criticality to client operations against consideration of all factors which impact on the operating environment including threat impact using agreed assessment criteria. 3.3 Reliability, availability and capacity of operational back-up systems for assets and activities are assessed in

ELEMENT	PERFORMANCE CRITERIA
4 Review and present findings.	terms of the impact to normal operations.
	3.4 Potential consequences of threats are confirmed through consultation with relevant persons and analysis of all relevant information.
	3.5 Client contingency requirements are identified and arranged based on an assessment of all factors.
	4.1 A report outlining assessment findings is prepared in the required format, style and structure and presented to the client within specified time, budget and quality constraints.
	4.2 Information is valid and relevant and analysis and recommendations are clear, justified and consistent with client terms of reference and organisational requirements.
	4.3 Feedback on client satisfaction with service delivery is sought and all queries are responded to promptly, courteously.
	4.4 Client satisfaction with service delivery is collected and reviewed using verifiable data.
	4.5 All information and material is securely retained and stored with due regard to client confidentiality requirements.

Required Skills and Knowledge

REQUIRED SKILLS AND KNOWLEDGE

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

Required skills

- access stored information
- accurately identify existing or potential threats
- apply reasoning and logical analysis to make decisions and solve problems
- coaching and mentoring to provide support to colleagues
- communicate in a clear and concise manner both orally and in writing
- obtain information using appropriate communication skills including interviewing, questioning and customer relations
- prepare and present verbal and written reports
- prioritise tasks and organise schedules
- relate to persons of different social and cultural backgrounds and of varying physical and mental abilities

REQUIRED SKILLS AND KNOWLEDGE

- research and analyse information
- use basic statistics
- use information technology.

Required knowledge

- client and organisational confidentiality policies
- concept of litigation
- distinction between information and intelligence
- organisational goals and objectives, activities and systems
- principles of AS/NZS 4360: 2004 Risk management and related guidelines
- principles of effective communication
- relevant industry codes of practice and standards
- relevant legislation and regulations including Occupational Health and Safety (OHS)
- security risk management
- threat assessment techniques and processes.

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 reviewing and preparing assessment findings in a format suitable for presentation
- analysing consequences of potential or existing threats, and measuring and determining their criticality to client operations
- identifying appropriate contingency requirements on the basis of an accurate assessment of all factors
- identifying causes and sources of potential or existing threats, and assessing the level, likelihood and impact of such threats on the basis of valid and verifiable information using agreed assessment criteria, techniques and processes
- obtaining information from a range of sources and consultative processes to ensure an accurate understanding of the threats to operational environment and core business operations of the client.

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
 - 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.
- Clients may include:**
- employer and employee groups
 - individuals
 - political parties
 - public and private entities
 - trade or professional associations.
- Relevant persons may include:**
- manufacturers
 - other professional, specialist or technical staff
 - security consultants
 - security personnel
 - supervisors.
- Relevant information may include:**
- client activities and functions
 - client business and operational plans
 - client current and proposed operating environment, assets and systems
 - existing client security management strategies
 - history of incidents
 - potential risks and threats experienced by similar organisations
 - terms of reference.
- Sources of information may include:**
- annual reports
 - competitors
 - current and past employees of the company, like organisation or like industry
 - field experts (for example qualified technicians)
 - government agencies
 - internet
 - media (journals, TV, radio, magazines)

- newspaper articles
 - organisational records
 - police
 - research papers
 - security contractors or consultants
 - security industry associations
 - service providers
 - similar organisations and industries (domestic and international).
- Assets may include:**
- business plans
 - equipment
 - facilities
 - goodwill
 - information, information systems and sources
 - intellectual property
 - output
 - people
 - reputation
 - systems
 - work processes and practices.
- Threats may:**
- affect the security of an asset
 - be an agent or event that could put an asset at risk (theft, vandalism, fire, flood, power loss, unauthorised access, viruses, corruption of data)
 - be deliberate, natural, accidental, perceived
 - cause loss of goodwill, reputation or credibility
 - cause loss, disclosure, destruction or compromise of asset
 - cause risk of litigation.
- The operating environment of an organisation may relate to:**
- competitors
 - core business functions
 - environmental issues
 - financial markets
 - key stakeholders
 - market share
 - nature of operations
 - neighbours
 - scale of operations
 - situational issues
 - size of company
 - stability of company, organisation, industry and market
 - type of industry
 - workforce.

- Causes and sources of threats may include:***
- a group of people
 - a nation, country or state
 - an individual
 - an organisation
 - natural events or the environment.
- Assessment criteria may be based on:***
- organisational or client requirements
 - qualitative factors
 - quantitative factors
 - semi-quantitative factors
 - the Australian Standard AS/NZS 4360:1999 Risk Management (or its equivalent).
- Consequences may include:***
- consideration of effect on client's ability to continue core functions
 - disruption to operations
 - impact on neighbours and subsequent litigation
 - loss of asset (eg property, lives, reputation, goodwill)
 - loss of privacy
 - loss of service or business
 - loss of trust
 - loss or reduction of productivity.
- Factors may include:***
- changes to the operational environment such as neighbours, financial markets and market share
 - those with regard to repair or replacement of assets and activities such as time, cost, training and availability.
- Threat impact evaluation may relate to:***
- factors related to the repair or replacement of assets and activities
 - level of seriousness
 - risk of litigation.
- Contingency arrangements may relate to:***
- cessation of operations
 - continuity of operations
 - partial closure
 - transfer of operations.
- Reports may include:***
- graphical representations of data
 - recommendations
 - summary of assessment outcomes
 - tables and information from approved data collection tools.

Unit Sector(s)

Unit sector Security

Competency field

Competency field Security and risk management