



Australian Government

Department of Education, Employment and Workplace Relations

CPPSEC4006A Assess risks

Release: 1

CPPSEC4006A Assess risks

Modification History

Not Applicable

Unit Descriptor

Unit descriptor This unit of competency specifies the outcomes required to determine effective security policies and controls. It requires the ability to identify key systems and assets, and the likelihood of threat against each asset. It also requires an ability to calculate the current risk for each asset.

This unit may form part of the licensing requirements for persons engaged in risk 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 risk 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 Identify risks.

- 1.1 Applicable provisions of **legislative** and **organisational requirements**, and **relevant standards** for assessment activities are identified and complied with.
- 1.2 **Client** operations, goals and objectives are discussed and confirmed in consultation with the client.
- 1.3 Context for identifying **risk** is based on an understanding of the operating environment and core business operations of the client.
- 1.4 **Information** is collected and assessed for currency, accuracy and relevance.
- 1.5 **Terms of reference** are identified in consultation with **relevant persons** and other **sources** of information and are updated, modified and maintained.
- 1.6 A **structured plan** for identifying and assessing risks is developed based on the terms of reference, the type and scale of the assessment task and the timeframe given for the assessment task.
- 1.7 Threat, consequence and vulnerability for each **asset** is compared in accordance with terms of reference.

2 Analyse risks.

- 2.1 **Assessment criteria** for measuring level of potential or existing risk together with an assessment of consequences are developed in accordance with terms of reference.
- 2.2 Gaps in the predetermined methodology are identified and reported to relevant persons, and where appropriate, options to meet these gaps are proposed.
- 2.3 Impacts of possible change in organisational business are allowed for during conduct of risk assessment.
- 2.4 **Relevant information and data** is assessed for validity and reliability and organised in a format suitable for review.
- 2.5 Risk potential is determined by assessment of valid and relevant data.

3 Review and present findings.

- 3.1 Analysis and options to overcome identified obstacles are supported by gathered and verifiable information.
- 3.2 Presented information uses clear and concise language, is free of inconsistencies and meets organisational standards of style, format and accuracy.
- 3.3 Feedback is sought and all additional information and queries are responded to promptly, courteously and accurately.
- 3.4 **Countermeasures** are broadly identified for future

ELEMENT**PERFORMANCE CRITERIA**

management decision-making purposes.

3.5 Relevant documentation is completed and 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

- access stored information
- accurately identify existing or potential risks
- application of the hierarchy of controls
- 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
- negotiation
- prepare and present verbal and written reports
- prioritise tasks and organise schedules
- relate to persons of different social and cultural backgrounds and varying physical and mental abilities
- research and analyse information
- risk assessment
- use information technology
- use interviewing and questioning techniques to obtain information.

Required knowledge

- basic concepts relating to litigation
- client and organisational confidentiality policies
- distinction between information and intelligence
- organisational goals and objectives
- principles of effective communication
- principles of AS/NZS 4360: 2004 Risk management and related guidelines
- relevant industry codes of practice
- relevant legislation and regulations including OHS
- risk assessment techniques and processes
- types of potential security risks.

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:

- establishing terms of reference and assessment criteria, and determining a thorough action plan and structure for the assessment
- accurately reviewing and preparing risk assessment findings in a format suitable for presentation
- assessing threat, consequence and vulnerability of each asset against agreed terms of reference and assessment criteria, and determining risk potential through analysis of valid and relevant data
- obtaining information from a range of sources and consultative processes to ensure an accurate understanding of the operating 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
 - 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.
- Clients may include:**
- employer or employee groups
 - individuals
 - political parties
 - public and private entities
 - trade or professional associations.

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.

Information may include:

- analysis of stakeholder concerns and objectives
- contacts within and external to the organisation
- documentation regarding employment, contracts
- group workshops and brainstorming
- historical data
- key personnel
- operating environment of organisation (neighbours, situational issues, financial markets, competitors, stability, size, workforce, core business activities, functions, stakeholders)
- organisational structure and lines of responsibility
- questionnaires
- reports and relevant documentation
- structured interviews
- surveys.

Terms of reference may include:

- client expectations
- cost
- limitations and exclusions (who and what they can access and what they cannot access)

- lines of authority
 - operational environment
 - roles and responsibilities
 - scale of the task or assessment (whether a full-scale operation, or limited to a particular section or operation of the company)
 - security and other clearances
 - timeframe.
- Relevant persons may include:***
- clients
 - manufacturers
 - other professional, specialist or technical staff
 - security consultants
 - security personnel
 - supervisors.
- Sources of information may include:***
- colleagues
 - documentation and reports
 - group workshops and brainstorming
 - incident reporting systems (software or paper-based)
 - interviews
 - media (newspaper, radio, television, industry magazines)
 - questionnaires
 - statistical data and evaluative studies
 - structured interviews
 - surveys (organisational or industry based) and questionnaires.
- A structured plan can be constructed by using:***
- checklists
 - interview question sheets
 - spreadsheets, word-processing and other software
 - structured planning software
 - structured questionnaires
 - structured tables.
- Assets may include:***
- business plans
 - equipment
 - facilities
 - goodwill
 - information, information systems and sources
 - intellectual property
 - output
 - people
 - reputation
 - systems
 - work processes and practices.

Assessment criteria may be based on:

- AS/NZS 4360:2004 Risk management (or its equivalent)
- qualitative factors
- quantitative factors
- semi-quantitative factors.

Relevant information and data 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 or threats experienced by similar organisations or organisations in similar situations.

Countermeasures may relate to:

- acceptance of residual risk
- addition of security measures
- minimisation of harm through response mechanisms
- reduction of security measures
- risk avoidance through change of service and system specifications
- transfer of risk to other entity (such as insurance company, outsourcing an operational activity).

Unit Sector(s)

Unit sector Security

Competency field

Competency field Security and risk management