Australian Government
Department of Education, Employment and Workplace Relations

CPPSEC5004A Prepare security risk management plan

Release: 1

INDUSTRY SKILLS COUNCILS
Creating Australia's Future

CPPSEC5004A Prepare security risk management plan

Modification History

Not Applicable

Unit Descriptor

Unit descriptor

This unit of competency specifies the outcomes required to plan and prepare for security risks. It requires the ability to develop a security risk management plan which incorporates suitable strategies for risk identification and treatment, and contingency arrangements compatible to identified risk.

This unit may form part of the licensing requirements for persons engaged in security operations in those states and territories where these are regulated activities.

Application of the Unit

Application of the unit

This unit of competency has wide application in a range of managerial roles in the security industry. Work is performed under minimal supervision and competency requires a high level of judgement and decision-making. 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 Evaluate security risks.	1.1 ***Security risks*** are identified and consequences interpreted in accordance with client, ***organisational*** and ***legislative requirements*** and ***relevant standards***. 1.2 Acceptable and unacceptable risks are clearly distinguished and confirmed. 1.3 High priority risks are emphasised and specified to ensure the development of appropriate ***controls***. 1.4 Existing controls are evaluated to determine impact on risk occurrence and required modifications identified.
2 Develop action plans.	2.1 Action plans are developed identifying key tasks, activities and resources to achieve security risk management objectives. 2.2 ***Type of risk*** associated with security context is identified and appropriate controls incorporated into planning processes. 2.3 Communication and reporting arrangements for maintaining currency of action plans are established. 2.4 ***Contingency arrangements*** for actions are developed and incorporated into plans.
3 Design treatment options.	3.1 Operating environment monitored to confirm potential and real risks, threats and required treatments. 3.2 ***Treatment options*** are selected in line with available organisational practices, and implications researched, clarified and approved by ***relevant persons***. 3.3 Feasible treatment options are documented and costed to ensure compatibility with nature of risk and client requirements. 3.4 Treatment options are linked to whole or part of security risks and verified with clients for suitability to security context. 3.5 ***Tests*** on treatment options are conducted to determine applicability in the field, and results statistically analysed to confirm effectiveness of treatments.
4 Develop security risk management plan.	4.1 ***Management requirements*** are identified and accounted for in development of security risk management plan. 4.2 Procedures for monitoring and review of security risk management activities are developed to ensure continuous improvement. 4.3 Security risk management plan is developed incorporating all ***relevant information*** in line with appropriate ***format*** and relevant standards.

ELEMENT	PERFORMANCE CRITERIA
	4.4 Plan is finalised and presented to client for review and approval 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

- access and use workplace information
- active listening
- adapt personal communication style to a variety of situations
- analyse and evaluate information and data
- coaching and mentoring to provide support to colleagues
- collate numerical data
- communicate in a clear and concise manner
- design treatment options and tests
- negotiation
- numeracy skills to calculate resources and costings
- planning
- reading to interpret complex information
- relate to people from a range of social, cultural and ethnic backgrounds and physical and mental abilities
- solve problems to deal with complex and non routine difficulties
- use technology to research, analyse and report information
- writing to develop complex reports.

Required knowledge

- applicable Occupational Health and Safety (OHS) licensing and legislative compliance requirements
- application of the hierarchy of control
- approved communication terminology and call signs
- available support agencies and the types of services offered
- basic methods for statistical analysis and presentation of statistical data
- difference between negative and positive language
- differences between written and spoken English
- how to read and use body language to gain confidence of others
- how to record information which may be used for legal purposes
- how to safeguard confidential information

REQUIRED SKILLS AND KNOWLEDGE

- how to use business equipment to present information
- negotiation techniques
- OHS implications relating to use of guard dogs, apprehension or arrest of persons, use of firearms, use of restraints, handcuffs, batons and spray
- organisational standards for the presentation and maintenance of written information
- principles of AS/NZS 4360: 2004 Risk management
- risk management principles and practices
- sources of supply of security equipment or systems
- tactical response measures
- use of force guidelines.

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 and evaluating security risks and control measures in compliance with client, organisational and legislative requirements
- designing and developing effective action plans which incorporate strategies for treating risks, contingency arrangements, key tasks and resources, and communication and reporting
- designing and testing risk treatment options which are compatible with nature of risk and client requirements, and conducting an analysis of the results to confirm effectiveness of treatments
- developing a comprehensive risk management plan in an appropriate format which incorporates a broad range of relevant information, considers implementation issues, and incorporates continuous improvement mechanisms based on the principles of AS/NZS 4360:2004.

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 a registered provider of assessment services
- access to a suitable venue and equipment
- access to plain English version of relevant statutes and procedures
- 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 should be assessed using 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.

Security risks may

- biological hazards
- chemical spills

relate to:	• 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.
***Risk* relates to**:	• the chance of something happening that will have an impact on objectives.
Organisational requirements may relate to:	• client service standards • implementation of OHS system • policies for ensuring privacy and confidentiality of information • procedures for archiving electronic and hard-copy records • procedures for recording, storing and destroying information • standard of language, literacy and numeracy required • use of organisational equipment and resources.
Legislative requirements may relate to:	• anti-discrimination and diversity • Australian standards, codes of practice and regulations • award and enterprise agreements • duty of care • evidence collection • licensing arrangements and certification requirements • OHS issue resolution • relevant commonwealth, state and territory OHS legislation, codes of practice and regulations • roles and responsibilities of OHS representatives and committees • trade practices

- use of force.

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.

***Controls* may include**:

- communication
- deployment of specialist expertise or equipment
- development of procedures
- monitoring and surveillance
- physical attendance and security
- staff ratios and resource deployment
- training of personnel.

Type of risk may be:

- intermediate
- likely to occur
- major
- minor
- physical
- potentially avoidable
- potentially unavoidable
- property related
- unlikely to occur.

***Contingency arrangements* may include**:

- approvals and licenses
- availability of additional resources
- background information
- back-up
- checklists and reporting
- identification requirements
- instructions.

***Project planning requirements* may include**:

- key outcomes
- milestones
- personnel involvement
- resources
- tasks
- timelines.

Treatment options

- controlled interruptions to normal operations

may include:	• exercises • information collation and analysis • simulations • surveillance • verification requirements.
***Relevant persons* may include**:	• authorities • client • managers • technical specialists.
***Tests* may include**:	• alarms and other warning devices • exercises • inspections • interviews • rehearsals • simulations.
***Management requirements* may relate to**:	• adherence to organisational policies and procedures • allocation of suitable resources and expertise • feedback and monitoring arrangements • preparation of documentation and checklists • procedures to maximise safety of operatives • project planning • reporting procedures and timeframes • risk management timelines and objectives specified in action plans.
***Relevant information* may include**	• action plans • backup systems or processes • contingency plans • details and results of testing and relevant statistical analysis • identified assets • identified management requirements • implementation issues • operational issues • resource requirements including allocation and location of resources • review and monitoring procedures • risk assessment • supporting evidence • threat assessment • treatment options and strategies linked to risks and threats.

***Format* may relate to**:

- accuracy
- common industry terminology
- enclosures and attachments
- length
- sequence of coverage
- style
- use of abbreviations
- use of appendices
- use of plain English.

Unit Sector(s)

Unit sector Security

Competency field

Competency field Security and risk management