



**Australian Government**

**Department of Education, Employment and Workplace Relations**

# **PRSSM504A Prepare security risk management plan**

**Release: 1**

## **PRSSM504A Prepare security risk management plan**

### **Modification History**

Not applicable.

### **Unit Descriptor**

This competency standard covers the process of planning to deal with security risks. It requires the ability to plan and prepare a security risk management plan which incorporates suitable response strategies and contingency arrangements compatible to identified risk. This work would be carried out within organisational guidelines.

**Functional Area:** Elective, Security Management

This competency standard covers the process of planning to deal with security risks. It requires the ability to plan and prepare a security risk management plan which incorporates suitable response strategies and contingency arrangements compatible to identified risk. This work would be carried out within organisational guidelines.

**Functional Area:** Elective, Security Management

### **Application of the Unit**

Not applicable.

### **Licensing/Regulatory Information**

Not applicable.

### **Pre-Requisites**

Not applicable.

### **Employability Skills Information**

Not applicable.

### **Elements and Performance Criteria Pre-Content**

Not applicable.

# Elements and Performance Criteria

## Elements and Performance Criteria

| Element                            | Performance Criteria                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 Evaluate and prioritise risks    | <ul style="list-style-type: none"><li>1.1 Consequences of identified risks are understood and considered against possible likelihood of occurrence</li><li>1.2 Acceptable and unacceptable risks are clearly distinguished and confirmed in accordance with organisational requirements</li><li>1.3 High priority risks are emphasised and specified to ensure the development of appropriate management requirements</li><li>1.4 Existing controls are evaluated to determine impact on risk occurrence and modifications and improvements are identified in accordance with organisational requirements</li></ul> |
| 2 Develop action plans             | <ul style="list-style-type: none"><li>2.1 Action plans are structured, formatted and identify key tasks and functions associated with security risk management</li><li>2.2 Type of risk associated with security context is identifiable through available examples and incorporated into planning processes</li><li>2.3 Communication and reporting arrangements for maintenance of plans are established in line with client requirements and organisational needs</li><li>2.4 Contingency arrangements for occurrence of risks are developed and incorporated into plans</li></ul>                               |
| 3 Identify management requirements | <ul style="list-style-type: none"><li>3.1 Timelines and objectives specified in security risk plans are assessed against organisational processes and requirements</li><li>3.2 Documentation and checklists associated with plan are prepared in established formats to ensure focus on key activities in risk management</li><li>3.3 Project planning requirements are identified and reviewed to determine availability of suitable resources and expertise</li></ul>                                                                                                                                             |

- 3.4 Feedback and monitoring arrangements for operational staff are prepared and established using appropriate procedures
- 4 Design treatment options
  - 4.1 Operating environment, including potential changes, is researched, confirmed, reviewed and linked to potential and real risks, threats and treatment strategies
  - 4.2 Treatment options are selected in line with available industry practices, and implications of treatment options are researched, clarified and approved by the client
  - 4.3 Treatment options are feasible, documented and costed to ensure compatibility with nature of risk and client requirements, including future goals and potential changes to the operating environment
  - 4.4 Treatment options are linked to whole or part of security risks and are verified with clients for suitability to security context, this is documented, and the required resources are identified and allocated
  - 4.5 Tests are conducted on treatment options to determine applicability in field, and the results are statistically analysed if possible
- 5 Develop risk management plan
  - 5.1 Monitoring and review procedures are developed to ensure continuous improvement according to planning, client and organisational requirements
  - 5.2 All relevant information is collated and documented according to assessment, client and organisational requirements
  - 5.3 Plan is prepared and presented to client or authorised representatives for review and approval in accordance with organisational requirements

## Required Skills and Knowledge

Not applicable.

## Evidence Guide

The Evidence Guide identifies the requirements to be demonstrated to confirm competence for this unit. Assessment must confirm sufficient ability to use appropriate skills and knowledge to plan and prepare a security risk management plan. Assessment of performance should be over a period of time covering all categories within the Range of Variables statements that are applicable in the learning environment.

### **What critical aspects are required for evidence of competency?**

Identify and evaluate assets, identified risks, analyse threats and determine existing and other required controls and determine impact on risk occurrence.

Develop effective action plans which incorporate implementation of any new treatment options or strategies, contingency arrangements, key tasks and functions and resource, communication and reporting arrangements.

Develop effective project milestones.

Systematically review project planning requirements and establish feedback and monitoring arrangements for operational staff.

Design treatment options which are compatible with nature of risk and client requirements.

Develop a comprehensive risk management plan which incorporates a broad range of relevant information, considers implementation issues, and incorporates continuous improvement mechanisms.

### **What specific knowledge is needed to achieve the performance criteria?**

Knowledge and understanding are essential to apply this standard in the workplace, to transfer the skills to other contexts and to deal with unplanned events. The knowledge requirements for this competency standard are listed below:

familiarity with client activities and systems including future intentions

broad process of security risk management

sources of supply of security equipment/systems

broad understanding of building facilities and services that apply to risk/threats being reviewed (electrical and air-conditioning systems)

legislation as it applies to security risk management

applicable industry codes of practice

relevant Australian Standards, including AS/NZS 4360:1999 or subsequent amendments

responsibilities necessary to comply with applicable OHS regulations

basic statistical analysis and presentation of statistical data.

### **What specific skills are needed to achieve the performance criteria?**

To achieve the performance criteria, some specific skills are required. These include the ability to:

communicate in a variety of oral formats including negotiation and interviewing

summarise information and write reports to a high standard

communicate in writing to ensure comprehensive coverage of the topic, yet easily understood by the reader

collate numerical data

solve problems

identify and assess assets

research and analyse data

manage time effectively

**Are there other competency standards that could be assessed with this one?**

Competency in these units should be demonstrated either prior to, or in conjunction with assessment of the current unit:

PRSSM414A - Identification and assessment of assets

PRSSM409A - Risk assessment

PRSSM413A - Threat assessment

**What resources may be required for assessment?**

Access to a suitable venue and equipment.

Access to plain English version of relevant statutes and procedures.

Assignment instructions, work plans and schedules, policy documents and duty statements.

Assessment instruments, including personal planner and assessment record book.

Access to a registered provider of assessment services.

**What is required to achieve consistency of performance?**

For valid and reliable assessment of this unit, the competency should be demonstrated over a period of time and observed by the assessor. The competency is to be demonstrated in a range of situations, which may include involvement in related activities normally experienced in the workplace.

Evidence of underpinning knowledge understanding of processes and principles can be gained through thorough questioning and by observation of previous work.

**Assessment against this unit may involve the following:**

Continuous assessment in a setting that simulates the conditions of performance described in the elements, performance criteria and range of variables statement that make up the unit.

Continuous assessment in the workplace, taking into account the range of variables affecting performance.

Self-assessment on the same terms as those described above.

Simulated assessment or critical incident assessment, provided that the critical incident involves assessment against performance criteria and an evaluation of underpinning knowledge and skill required to achieve the required performance outcomes.

**Key competency levels**

There are a number of processes that are learnt throughout work and life which are required in all jobs. They are fundamental processes and generally transferable to other work functions. Some of these are covered by the key competencies, although others may be added.

Information below highlights how these processes are applied in this competency standard.

**1** - perform the process

**2** - perform and administer the process

**3** - perform, administer and design the process

How can **communication of ideas and information** be applied? **(3)**

Information may be conveyed through discussions and presentations on organisational processes.

How can **information be collected, analysed and organised**? **(3)**

Action plans may be developed which incorporate key tasks and functions, resource, communication and reporting requirements.

How are **activities planned and organised**? **(3)**

Tests may be conducted on treatment options to determine applicability in a field context.

How can **team work** be applied? **(2)**

Acceptable and unacceptable risks may be discussed and clarified.

How can the use of **mathematical ideas and techniques** be applied? **(3)**

Mathematical techniques may be used in the analysis of data and costing resource requirements.

How can **problem solving skills** be applied? (3)

Contingency arrangements may be planned for and incorporated in security risk management plan.

How can the **use of technology** be applied? (3)

Technology may be used to communicate, research and manage information. It may also be used in aspects of project management.

The Evidence Guide identifies the requirements to be demonstrated to confirm competence for this unit. Assessment must confirm sufficient ability to use appropriate skills and knowledge to plan and prepare a security risk management plan. Assessment of performance should be over a period of time covering all categories within the Range of Variables statements that are applicable in the learning environment.

**What critical aspects are required for evidence of competency?**

Identify and evaluate assets, identified risks, analyse threats and determine existing and other required controls and determine impact on risk occurrence.

Develop effective action plans which incorporate implementation of any new treatment options or strategies, contingency arrangements, key tasks and functions and resource, communication and reporting arrangements.

Develop effective project milestones.

Systematically review project planning requirements and establish feedback and monitoring arrangements for operational staff.

Design treatment options which are compatible with nature of risk and client requirements.

Develop a comprehensive risk management plan which incorporates a broad range of relevant information, considers implementation issues, and incorporates continuous improvement mechanisms.

**What specific knowledge is needed to achieve the performance criteria?**

Knowledge and understanding are essential to apply this standard in the workplace, to transfer the skills to other contexts and to deal with unplanned events. The knowledge requirements for this competency standard are listed below:

familiarity with client activities and systems including future intentions

broad process of security risk management

sources of supply of security equipment/systems

broad understanding of building facilities and services that apply to risk/threats being reviewed (electrical and air-conditioning systems)

legislation as it applies to security risk management

applicable industry codes of practice

relevant Australian Standards, including AS/NZS 4360:1999 or subsequent amendments

responsibilities necessary to comply with applicable OHS regulations

basic statistical analysis and presentation of statistical data.

**What specific skills are needed to achieve the performance criteria?**

To achieve the performance criteria, some specific skills are required. These include the ability to:

communicate in a variety of oral formats including negotiation and interviewing

summarise information and write reports to a high standard

communicate in writing to ensure comprehensive coverage of the topic, yet easily understood by the reader

collate numerical data

solve problems

identify and assess assets

research and analyse data  
manage time effectively

**Are there other competency standards that could be assessed with this one?**

Competency in these units should be demonstrated either prior to, or in conjunction with assessment of the current unit:

PRSSM414A - Identification and assessment of assets

PRSSM409A - Risk assessment

PRSSM413A - Threat assessment

**What resources may be required for assessment?**

Access to a suitable venue and equipment.

Access to plain English version of relevant statutes and procedures.

Assignment instructions, work plans and schedules, policy documents and duty statements.

Assessment instruments, including personal planner and assessment record book.

Access to a registered provider of assessment services.

**What is required to achieve consistency of performance?**

For valid and reliable assessment of this unit, the competency should be demonstrated over a period of time and observed by the assessor. The competency is to be demonstrated in a range of situations, which may include involvement in related activities normally experienced in the workplace.

Evidence of underpinning knowledge understanding of processes and principles can be gained through thorough questioning and by observation of previous work.

**Assessment against this unit may involve the following:**

Continuous assessment in a setting that simulates the conditions of performance described in the elements, performance criteria and range of variables statement that make up the unit.

Continuous assessment in the workplace, taking into account the range of variables affecting performance.

Self-assessment on the same terms as those described above.

Simulated assessment or critical incident assessment, provided that the critical incident involves assessment against performance criteria and an evaluation of underpinning knowledge and skill required to achieve the required performance outcomes.

**Key competency levels**

There are a number of processes that are learnt throughout work and life which are required in all jobs. They are fundamental processes and generally transferable to other work functions. Some of these are covered by the key competencies, although others may be added.

Information below highlights how these processes are applied in this competency standard.

**1** - perform the process

**2** - perform and administer the process

**3** - perform, administer and design the process

How can **communication of ideas and information** be applied? **(3)**

Information may be conveyed through discussions and presentations on organisational processes.

How can **information be collected, analysed and organised**? **(3)**

Action plans may be developed which incorporate key tasks and functions, resource, communication and reporting requirements.

How are **activities planned and organised**? **(3)**

Tests may be conducted on treatment options to determine applicability in a field context.

How can **team work** be applied? **(2)**

Acceptable and unacceptable risks may be discussed and clarified.

How can the use of **mathematical ideas and techniques** be applied? (3)

Mathematical techniques may be used in the analysis of data and costing resource requirements.

How can **problem solving skills** be applied? (3)

Contingency arrangements may be planned for and incorporated in security risk management plan.

How can the **use of technology** be applied? (3)

Technology may be used to communicate, research and manage information. It may also be used in aspects of project management.

## Range Statement

The Range of Variables provides information about the context in which the unit of competency is carried out. It allows for different work practices and work and knowledge requirements as well as for differences between organisations and workplaces. The following variables may be present for this particular unit:

**Identified risks may include:**

- property risks
- risks associated with people
- process failures
- security systems
- client contact risks
- financial risks.

**Organisational requirements may include:**

- verification by senior management
- cost limits
- response times
- client acceptance
- application of organisational routines.

**Controls may include:**

- monitoring and surveillance
- physical attendance
- training
- development of procedures
- staff ratios and resource deployment.

**Type of risk may be:**

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

**Contingency arrangements may include:**

- checklists and reporting
- training
- organisational instructions
- approvals
- identification requirements
- internal licenses
- confidentiality requirements.

**Project planning requirements may include:**

- milestones
- timelines
- resources
- key outcomes

personnel involvement  
tasks.

**Treatment options may include:**

surveillance  
controlled interruptions to normal operations  
simulations  
information collation and analysis  
exercises  
verification requirements.

**Tests may include:**

alarms and other warning devices  
interviews  
rehearsals  
inspections  
exercises.

**Relevant information may include:**

identified assets  
risk assessment  
threat assessment  
management requirements  
supporting evidence  
treatment options and strategies linked to risks and threats  
operational issues  
any test results and relevant statistical analysis of the results  
implementation issues  
resource requirements including allocation and location of resources  
review and monitoring procedures  
action plans  
contingency plans  
backup systems or processes.

The Range of Variables provides information about the context in which the unit of competency is carried out. It allows for different work practices and work and knowledge requirements as well as for differences between organisations and workplaces. The following variables may be present for this particular unit:

**Identified risks may include:**

property risks  
risks associated with people  
process failures  
security systems  
client contact risks  
financial risks.

**Organisational requirements may include:**

verification by senior management  
cost limits  
response times  
client acceptance  
application of organisational routines.

**Controls may include:**

monitoring and surveillance  
physical attendance  
training  
development of procedures  
staff ratios and resource deployment.

**Type of risk may be:**

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

**Contingency arrangements may include:**

checklists and reporting  
training  
organisational instructions  
approvals  
identification requirements  
internal licenses  
confidentiality requirements.

**Project planning requirements may include:**

milestones  
timelines  
resources  
key outcomes  
personnel involvement  
tasks.

**Treatment options may include:**

surveillance  
controlled interruptions to normal operations  
simulations  
information collation and analysis  
exercises  
verification requirements.

**Tests may include:**

alarms and other warning devices  
interviews  
rehearsals  
inspections  
exercises.

**Relevant information may include:**

identified assets  
risk assessment  
threat assessment  
management requirements

supporting evidence  
treatment options and strategies linked to risks and threats  
operational issues  
any test results and relevant statistical analysis of the results  
implementation issues  
resource requirements including allocation and location of resources  
review and monitoring procedures  
action plans  
contingency plans  
backup systems or processes.

## **Unit Sector(s)**

Not applicable.