Australian Government

Department of Education, Employment and Workplace Relations

PRSTS301A Identify technical security requirements

Release: 1

PRSTS301A Identify technical security requirements

Modification History

Not applicable.

Unit Descriptor

This competency standard covers the skills and knowledge required to determine technical security requirements for small domestic or commercial environments. It requires the ability to source relevant information and use appropriate assessment methods to accurately determine security equipment/system options to meet client needs. This work would be carried out under routine supervision within organisational guidelines.
Functional Area: Core, Technical Security
This competency standard covers the skills and knowledge required to determine technical security requirements for small domestic or commercial environments. It requires the ability to source relevant information and use appropriate assessment methods to accurately determine security equipment/system options to meet client needs. This work would be carried out under routine supervision within organisational guidelines.
Functional Area: Core, Technical Security

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.

© Commonwealth of Australia, 2012 Government Skills Australia

Elements and Performance Criteria

Elements and Performance Criteria

Element	Performance Criteria
1 Prepare to identify security requirements	1.1 Assignment instructions are reviewed and clarified with appropriate person(s) as required in accordance with organisational requirements
	1.2 Discussions with client are conducted to establish perceived security risks and clarify scope of security requirements
	1.3 Specific site requirements are identified and appropriate arrangements made as required in accordance with client and organisational requirements
	1.4 Personal limitations in assessing security requirements are promptly identified and assistance is sought from appropriate person(s) in accordance with organisational procedures
2 Identify security requirements	2.1 Site restrictions, regulations and requirements are identified and complied with in accordance with legislative, client and organisational requirements
	2.2 Information is gathered from reliable sources and is relevant to assignment requirements in accordance with legislative, client and organisational requirements
	2.3 A site assessment is carried out where possible to facilitate an accurate determination of security system requirements
	2.4 Security risk factors that may affect the site are identified and assessed in accordance with organisational procedures
3 Document security requirements	3.1 Business equipment is used to manage information efficiently and effectively in accordance with manufacturers specifications and organisational procedures
	3.2 An assessment of client security requirements is completed within designated timeframes and presented for review to appropriate person(s)

© Commonwealth of Australia, 2012 Government Skills Australia

3.3 Assessment report uses clear and concise language, is free of inconsistencies and meets organisational standards of style, format and accuracy

3.4 Recommendations for security equipment / systems and alternative options are supported by gathered and verifiable information in accordance with organisational requirements

3.5 Documentation requirements are completed and processed in accordance with legislative, assignment and organisational requirements

Required Skills and Knowledge

Not applicable.

© Commonwealth of Australia, 2012 Government Skills Australia

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 assess technical security requirements for clients. 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?

Source and gather relevant information and conduct a comprehensive site assessment to identify client assets, activities and existing security arrangements.

Use appropriate research methods to determine suitable technical security requirements and options to meet client needs and expectations.

Prepare a summary of assessed client needs and recommended security options in a format suitable for review.

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:

available security equipment/system options and basic requirements for installation
types and functions of security equipment and systems
building construction methods and types
organisational and client confidentiality requirements
basic problem solving strategies
operational principles of information technology
principles of effective communication
documentation requirements and processes.

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:

recognise security threats to people, property and premises
observe and assess technical security requirements
read and interpret plans, designs and specifications
apply basic numeracy techniques
apply safe and efficient work practices
communicate in a clear and concise manner
relate to people from different social and cultural backgrounds
present a professional image
prepare and present reports
organise work tasks in a methodical manner
enter data using basic keyboarding skills.

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?

© Commonwealth of Australia, 2012 Government Skills Australia

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? (**2**)
Discussions may be conducted with relevant persons to clarify scope of client technical security requirements.
How can **information be collected**, **analysed and organised**? (**2**)
A site assessment may be carried out, accurately documented and organised by records or reports.
How are **activities planned and organised**? (**2**)
Site assessments may be arranged with minimal disruption to client, services or normal work routines.
How can **team work** be applied? (**2**)
Clarification may be sought from relevant persons to ensure a clear understanding of assignment requirements.
How can the use of **mathematical ideas and techniques** be applied? (**2**)
Mathematical techniques may be used to estimate resource and equipment/system requirements. It may also be used to plan and schedule work tasks.
How can **problem solving skills** be applied? (**2**)
Personal limitations in assessing technical security requirements may be promptly identified and appropriate assistance sought.
How can the **use of technology** be applied? (**2**)
Technology may be used to communicate, schedule, source and document information.
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 assess technical security requirements for clients. 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.

© Commonwealth of Australia, 2012 Government Skills Australia

What critical aspects are required for evidence of competency?
Source and gather relevant information and conduct a comprehensive site assessment to identify client assets, activities and existing security arrangements.
Use appropriate research methods to determine suitable technical security requirements and options to meet client needs and expectations.
Prepare a summary of assessed client needs and recommended security options in a format suitable for review.
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:
available security equipment/system options and basic requirements for installation
types and functions of security equipment and systems
building construction methods and types
organisational and client confidentiality requirements
basic problem solving strategies
operational principles of information technology
principles of effective communication
documentation requirements and processes.
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:
recognise security threats to people, property and premises
observe and assess technical security requirements
read and interpret plans, designs and specifications
apply basic numeracy techniques
apply safe and efficient work practices
communicate in a clear and concise manner
relate to people from different social and cultural backgrounds
present a professional image
prepare and present reports
organise work tasks in a methodical manner
enter data using basic keyboarding skills.
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:

© Commonwealth of Australia, 2012 Government Skills Australia

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? (**2**)
Discussions may be conducted with relevant persons to clarify scope of client technical security requirements.

How can **information be collected**, **analysed and organised**? (**2**)
A site assessment may be carried out, accurately documented and organised by records or reports.

How are **activities planned and organised**? (**2**)
Site assessments may be arranged with minimal disruption to client, services or normal work routines.

How can **team work** be applied? (**2**)
Clarification may be sought from relevant persons to ensure a clear understanding of assignment requirements.

How can the use of **mathematical ideas and techniques** be applied? (**2**)
Mathematical techniques may be used to estimate resource and equipment/system requirements. It may also be used to plan and schedule work tasks.

How can **problem solving skills** be applied? (**2**)
Personal limitations in assessing technical security requirements may be promptly identified and appropriate assistance sought.

How can the **use of technology** be applied? (**2**)
Technology may be used to communicate, schedule, source and document information.

© Commonwealth of Australia, 2012 Government Skills Australia

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:

Assignment instructions may include:
instructions from supervisor/management
work schedules and completion dates
specific client requirements
site requirements, security clearance and access requirements
reporting and documentation requirements
budget allocations.

Appropriate person(s) may include:
clients
site managers
project managers
engineers and technicians
technical experts
line managers/supervisors
colleagues
regulatory personnel
security consultants.

Organisational requirements may relate to:
legal and organisational operational policies and procedures
operations manuals, induction and training materials
insurance policy agreements
client and organisational confidentiality requirements
organisational goals, objectives, plans, systems and processes
employer and employee rights and responsibilities
own role, responsibility and delegation
quality and continuous improvement processes and standards
client service standards
defined resource parameters
OHS policies, procedures and programs
emergency and evacuation procedures
duty of care, code of conduct, code of ethics
access and equity policy, principles and practice
records and information systems and processes
communication channels and reporting procedures.

Client may include:
owner
property agent
tenant
building supervisor
manager
project manager
agent

© Commonwealth of Australia, 2012 Government Skills Australia

government and legal instruments/agencies.
Scope may include:
protection of persons, property or assets
conformance with insurance
government or other requirements.
Site access and specific site requirements may relate to:
access and egress points, time of access
access codes, keys, passes, security clearances
union requirements
OHS requirements
building codes and regulations
heritage listings
noise control.
Assessment may involve
discussions with client
visual inspections
review of client floor plans and supporting documentation
questioning police, insurance companies and other bodies.
Applicable legislation, **codes and national standards may relate to**:
relevant Commonwealth/State/Territory legislation which affect organisational operation:
Occupational Health and Safety
environmental issues
equal employment opportunity
industrial relations
anti-discrimination and diversity.

licensing arrangements
Australian Standards, quality assurance and certification requirements
relevant industry Codes of Practice
trade practices, award and enterprise agreements
privacy related legislation.
Information may include:
insurance policy agreements
special rooms or areas requiring higher level of protection
current/proposed operating environments, assets and systems
activities and functions
existing security systems/equipment
existing management strategies
business and operational plans
incident history.
Site assessment may involve:
type and condition of building structures
site restrictions, regulations and requirements
access and egress patterns
floor plan
existing security equipment/systems.
Security risks factors may include:
vandalism, trespass, break-in, burglary

© Commonwealth of Australia, 2012 Government Skills Australia

unsecured windows
entry points screened from public view
external doors without deadlocks or with hinges opening outward
flimsy building materials
client habits (e.g. doors left unlocked)
adequacy of street lighting
traffic flow
neighbourhood crime rating
proximity of other buildings.

Business equipment may include:
computers, computer applications, modems
personal schedulers
e-mail, internet/intranet
facsimile machines
printers
photocopiers
scanners.

Security equipment and systems may include:
detection devices, audible/visual warning devices
cameras, monitors and control equipment
control panels, intercoms
wireless equipment, car alarms
electronic readers, electronic recognition controls
locks and locking systems
grills, lighting, boom gates, turnstiles
bank pop-up screens
smoke detection devices
electric/mechanical fire safety and fire locking systems
power supplies, batteries
security doors and door controls.

Security systems may be:
electronic
mechanical
computerised
procedural.

Documentation may include:
checklists
reports
floor plans
client briefs
specifications
schedules.

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:

Assignment instructions may include:
instructions from supervisor/management

© Commonwealth of Australia, 2012 Government Skills Australia

work schedules and completion dates
specific client requirements
site requirements, security clearance and access requirements
reporting and documentation requirements
budget allocations.

Appropriate person(s) may include:
clients
site managers
project managers
engineers and technicians
technical experts
line managers/supervisors
colleagues
regulatory personnel
security consultants.

Organisational requirements may relate to:
legal and organisational operational policies and procedures
operations manuals, induction and training materials
insurance policy agreements
client and organisational confidentiality requirements
organisational goals, objectives, plans, systems and processes
employer and employee rights and responsibilities
own role, responsibility and delegation
quality and continuous improvement processes and standards
client service standards
defined resource parameters
OHS policies, procedures and programs
emergency and evacuation procedures
duty of care, code of conduct, code of ethics
access and equity policy, principles and practice
records and information systems and processes
communication channels and reporting procedures.

Client may include:
owner
property agent
tenant
building supervisor
manager
project manager
agent
government and legal instruments/agencies.

Scope may include:
protection of persons, property or assets
conformance with insurance
government or other requirements.

Site access and specific site requirements may relate to:
access and egress points, time of access
access codes, keys, passes, security clearances

© Commonwealth of Australia, 2012 Government Skills Australia

union requirements
OHS requirements
building codes and regulations
heritage listings
noise control.

Assessment may involve

discussions with client
visual inspections
review of client floor plans and supporting documentation
questioning police, insurance companies and other bodies.

Applicable legislation, **codes and national standards may relate to**:

relevant Commonwealth/State/Territory legislation which affect organisational operation:
Occupational Health and Safety
environmental issues
equal employment opportunity
industrial relations
anti-discrimination and diversity.

licensing arrangements
Australian Standards, quality assurance and certification requirements
relevant industry Codes of Practice
trade practices, award and enterprise agreements
privacy related legislation.

Information may include:

insurance policy agreements
special rooms or areas requiring higher level of protection
current/proposed operating environments, assets and systems
activities and functions
existing security systems/equipment
existing management strategies
business and operational plans
incident history.

Site assessment may involve:

type and condition of building structures
site restrictions, regulations and requirements
access and egress patterns
floor plan
existing security equipment/systems.

Security risks factors may include:

vandalism, trespass, break-in, burglary
unsecured windows
entry points screened from public view
external doors without deadlocks or with hinges opening outward
flimsy building materials
client habits (e.g. doors left unlocked)
adequacy of street lighting
traffic flow
neighbourhood crime rating

© Commonwealth of Australia, 2012 Government Skills Australia

proximity of other buildings.
Business equipment may include:
computers, computer applications, modems
personal schedulers
e-mail, internet/intranet
facsimile machines
printers
photocopiers
scanners.
Security equipment and systems may include:
detection devices, audible/visual warning devices
cameras, monitors and control equipment
control panels, intercoms
wireless equipment, car alarms
electronic readers, electronic recognition controls
locks and locking systems
grills, lighting, boom gates, turnstiles
bank pop-up screens
smoke detection devices
electric/mechanical fire safety and fire locking systems
power supplies, batteries
security doors and door controls.
Security systems may be:
electronic
mechanical
computerised
procedural.
Documentation may include:
checklists
reports
floor plans
client briefs
specifications
schedules.

Unit Sector(s)

Not applicable.

© Commonwealth of Australia, 2012 Government Skills Australia