



Australian Government

Department of Education, Employment and Workplace Relations

CPPSEC5006A Determine strategy for the implementation of biometric technology

Release: 1

CPPSEC5006A Determine strategy for the implementation of biometric technology

Modification History

Not Applicable

Unit Descriptor

Unit descriptor

This unit of competency specifies the outcomes required to determine requirements and processes for the strategic implementation of biometric technology in the workplace. It requires the ability to determine security and biometric technology requirements, design treatment options and develop an implementation strategy for the integration of a biometrics system.

An understanding of the operating principles of biometric systems including software, hardware and acquisition devices is also required as well as the ability to interpret and apply effective principles and requirements relating to confidentiality, privacy and security in own work.

This unit may form part of the licensing requirements for persons engaged in security operations involving biometric technology 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 roles involving determining requirements for biometric technology in the workplace to maintain security. 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 <i>bold italicised</i> 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 Determine security requirements.	1.1 Applicable Occupational Health and Safety (OHS), legislative and organisational requirements relevant to workplace biometric technology are identified and complied with. 1.2 Relevant privacy legislation and codes of ethics relevant to the workplace application of biometric technology are accessed and interpreted. 1.3 Reliability and effectiveness of organisational security safeguards are evaluated. 1.4 Threats to organisational physical and technical security are identified. 1.5 Risks are identified and risk levels established and prioritised. 1.6 Effective communication and interpersonal techniques are used that reflect sensitivity to individual social and cultural differences. 1.7 Specialist assistance to examine and assess security requirements is sought as required in accordance with organisational requirements.
2 Determine requirements for implementing biometric technology.	2.1 Legislative and regulatory requirements applicable to the use of biometric technology are confirmed. 2.2 Options for single or multiple biometric technology are determined. 2.3 Physical and technical specifications of biometric equipment and systems to be installed are determined. 2.4 Workspace requirements are identified and locations determined. 2.5 Resources, skills and training requirements for the implementation of biometric technology are determined. 2.6 Existing architecture is assessed for effective integration with biometric technology and additional requirements determined.
3 Design implementation options.	3.1 Implementation options are selected in accordance with industry practices and organisational policies and procedures. 3.2 Implementation options are feasible and verifiable in accordance with organisational requirements. 3.3 Implementation options are in compliance with time schedules, available resources and budgetary guidelines. 3.4 Implementation options take into account organisational risk assessment and security requirements. 3.5 Implementation options are effective and applicable in the workplace.
4 Develop an	4.1 All relevant information is collated, documented and

ELEMENT	PERFORMANCE CRITERIA
implementation strategy.	presented in an <i>appropriate format</i> in accordance with organisational requirements. 4.2 <i>Implementation strategy</i> is developed in accordance with organisational requirements. 4.3 Strategy incorporates <i>contingencies</i> and allows for continuous improvement planning. 4.4 Strategy is presented to <i>relevant persons</i> and feedback is sought and used to evaluate and refine strategy. 4.5 <i>Records and reports</i> are completed and maintained in accordance with legislative and organisational 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

- accurately and securely maintain records, reports and other workplace information
- analyse organisational security plans, goals, objectives and existing safeguards
- coaching and mentoring to provide support to colleagues
- comply with applicable confidentiality and privacy requirements
- comply with legislation, regulations, standards, codes of practice relevant to workplace biometric technology
- conduct and evaluate risk and threat assessments
- design effective treatment options
- determine biometric technology and system requirements, including single or multiple biometrics applications
- determine resources including personnel, tools and equipment
- determine security requirements
- make effective decisions
- plan for contingencies
- read and interpret technical information including plans, designs and specifications
- relate effectively to people from a range of social, cultural and ethnic backgrounds and varying physical and mental abilities
- research and analyse data and specifications
- resolve problems
- select and use equipment and technology appropriate to the work task
- undertake effective enrolment of biometric and biographical data
- use appropriate communication and interpersonal skills including negotiation

REQUIRED SKILLS AND KNOWLEDGE

- written communication skills sufficient to complete relevant records and reports.

REQUIRED SKILLS AND KNOWLEDGE

Required knowledge

- accuracy metrics and ratios according to risk tolerance
- applicable commonwealth, state or territory legislation, regulations, standards and codes of practice relevant to the full range of processes relating to workplace biometric technology
- appropriate mathematical procedures for estimating, measuring and calculating
- biometric technology installation and implementation processes, procedures and requirements
- ergonomic and safe working practices and procedures
- established threshold levels and their impact on security
- feasibility and cost-benefit analysis techniques
- initial enrolment processes
- management of enrolment data
- operating systems and integration application requirements
- operational principles of information technology
- organisational procedures for recording, reporting and maintaining workplace information
- organisational security plans, goals and objectives
- organisational standards, requirements, policies and procedures for the use of biometric technology
- principles of cultural diversity and access and equity
- privacy and ethics issues associated with biometric technology
- product options for various biometric systems
- risk, threats and vulnerabilities associated with biometric technology
- security and risk assessment and management techniques and processes
- types, functions and parameters of biometric technology including software, hardware and acquisition devices
- workplace communication channels, protocols and procedures.

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

A person who demonstrates competency in this unit must be able to provide evidence of:

- accurately estimating resources to support implementation

**demonstrate
competency in this unit**

strategy and determining roles, responsibilities and work schedules

- complying with applicable legislation and codes of ethics applicable to privacy and client confidentiality
- complying with organisational policies and procedures, including OHS, relevant to biometric work tasks
- designing treatment options which are compatible with assessed risk and security requirements
- determining biometric technology requirements based on an accurate evaluation of existing security controls, assets, and potential risks and threats
- developing an effective strategy which incorporates the implementation of treatment options, contingency arrangements, and resources for the effective implementation of biometric technology in a workplace environment.

**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 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.

Occupational Health and Safety (OHS) requirements may relate to:

- controlling and minimising risks
- correct manual handling including shifting, lifting and carrying
- elimination of hazardous materials and substances
- identifying hazards
- safe use and operation of equipment including
 - business technology
 - first aid equipment
 - fire safety equipment
 - personal protective clothing and equipment
 - safety equipment
- safety procedures for the protection of self and others.
- Australian standards and quality assurance requirements
- award and enterprise agreements
- Compliance Policy Guidelines (CPGs)
- counter-terrorism
- general 'duty of care' responsibilities
- 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

Legislative requirements may relate to:

- OHS
- relevant industry codes of practice
- telecommunications.

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
- environmental management including waste disposal, recycling and re-use guidelines
- 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
- standard operating procedures
- storage and disposal of information
- use and maintenance of equipment and systems.

Biometric refers to:

- a measurable physical characteristic or personal behavioural trait used to recognise the identity or verify the identity of an individual.

Biometric technologies include:

- facial recognition
- fingerprint recognition
- hand geometry
- iris recognition
- retina recognition
- signature recognition
- vein recognition
- voice recognition.

Privacy legislation may include:

- Commonwealth, State and Territory Privacy Acts
- national information privacy principles
- national privacy principles.

Security safeguards may be:

- administrative and include:
 - contingency plans (data back-up, disaster recovery, and emergency mode operation plans)
 - information access management (access authorisation, establishment and modification)
 - security awareness and training (awareness, virus protection, log-in success or failure, password

management)

- security incident procedures (report and response procedures)
- security management (risk analysis and management)
- physical and include measures to protect information systems, buildings and equipment from natural and environmental hazards and unauthorised intrusions
- technical and include:
 - access control (user identification, emergency access procedures, automatic log-off, encryption and decryption)
 - audit control (logging, capturing data versions, times, sessions, workstations, events and user information)
 - transmission security (integrity controls, encryption).

- Threats:**
- are intentional or unintentional potential events that could compromise the security integrity of physical and technical organisational systems.
- Risk relates to:**
- the chance of something happening that will have an impact on objectives.
- Risks may relate to:**
- data and information
 - personnel
 - property.
- Communication may be:**
- face-to-face
 - group interaction
 - in Indigenous languages
 - in languages other than English
 - oral reporting
 - participation in routine meetings
 - reading independently
 - recording of discussions
 - speaking clearly and directly
 - through the use of assistive technology
 - via an interpreter
 - visual or written
 - writing to audience needs.
- Interpersonal techniques may involve:**
- active listening
 - being non-judgemental
 - being respectful and non-discriminatory
 - constructive feedback
 - control of tone of voice and body language
 - culturally aware and sensitive use of language and concepts
 - demonstrating flexibility and willingness to negotiate
 - effective verbal and non-verbal communication
 - maintaining professionalism
 - providing sufficient time for questions and responses
 - reflection and summarising
 - two-way interaction
 - use of plain English
 - use of positive, confident and cooperative language.
- Social and cultural differences may relate to:**
- dress and personal presentation
 - food
 - language
 - religion
 - social conventions
 - traditional practices

- values and beliefs.

- Options may relate to:**
- enrolment advice
 - motivation to verify
 - tolerance for rejected attempts.
- Multiple biometrics refers to:**
- a biometric system that integrates two or more biometric technologies (facial and iris recognition, and multiple instances of a single biometric eg one, two or ten fingerprints).
- Biometric equipment and systems are:**
- automated systems able to capture a biometric sample from an individual person, extract biometric data from the sample, compare the data with one or more reference templates, determine the quality of a match, and indicate whether or not an identification or verification of identity has been achieved.
- Biometric equipment and systems may include:**
- acquisition devices:
 - cameras (video, infrared-enabled video, single-image)
 - chip or reader embedded in peripheral device
 - microphones
 - optical scanners
 - biometric servers
 - hardware
 - interconnecting infrastructure
 - software:
 - server-based authentication software for biometric authentication and logging
 - software associated with acquisition devices.
- Resource requirements may include:**
- computer systems (hardware, software and infrastructure)
 - equipment
 - funding
 - personnel
 - time
 - tools.
- Existing architecture may include:**
- desktop PCs
 - local area networks (LANs)
 - mainframe systems
 - servers
 - websites
 - wide area networks (WANs).
- Additional requirements may relate to:**
- integration service requirements and interoperability
 - upgrading or replacing the system or components of the system.
- Feasibility may relate**
- economic and schedule feasibility

- to:**
- operational feasibility
 - technical feasibility.
- Relevant information may include:***
- assets (resources, data and information)
 - contingency plans
 - implementation issues
 - resource requirements including allocation and location
 - risk and threat assessment outcomes
 - treatment options.
- Appropriate format may include:***
- formats that cater for those with special needs for example, producing documents in large print.
- Implementation strategy may include:***
- analysis and comparison of biometrics system options
 - assessment of security risks
 - enrolment processes
 - integration requirement and system interoperability
 - resources necessary for implementation
 - staged rollouts.
- Contingencies may detail:***
- roles, responsibilities, teams and procedures associated with restoring a security system following a disruption
 - side manual door entry.
- Relevant persons may include:***
- biometric technology specialists
 - clients
 - colleagues
 - external consultants
 - information technology specialists
 - manager.
- Records and reports:***
- may be:
 - computer-based
 - manual
 - other appropriate organisational communication system
 - may detail:
 - biometric technologies and systems
 - organisational security requirements
 - resources requirements
 - risk assessment outcomes
 - technical data and specifications
 - timeframe and financial considerations.

Unit Sector(s)

Unit sector Security

Competency field

Competency field Biometrics