



Australian Government

Department of Education, Employment and Workplace Relations

CPPSEC5007A Assess biometric system

Release: 1

CPPSEC5007A Assess biometric system

Modification History

Not Applicable

Unit Descriptor

Unit descriptor

This unit of competency specifies the outcomes required to conduct an assessment of the application and operations of biometric technologies and systems in a workplace environment.

It requires the ability to determine security arrangements and requirements, measure and assess the operation, application and outcomes of biometric technologies and systems in terms of efficiency and effectiveness. It also involves the preparation and presentation of assessment results.

An understanding of the operating principles of biometric systems including software, hardware and acquisition devices, and principles of measurement and assessment are 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 the assessment of biometric technologies and systems in the workplace. 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 Plan for assessment.	1.1 Applicable Occupational Health and Safety (OHS), legislative and organisational requirements relevant to biometric technologies and systems are confirmed. 1.2 Relevant privacy legislation and codes of ethics relevant to the workplace application of biometric technology are accessed and interpreted. 1.3 Context and purpose of assessment is determined and clarified with relevant persons as required. 1.4 Organisational security requirements are determined. 1.5 Resources relevant to assessment activities are determined and organised in accordance with workplace procedures. 1.6 Assessment plan is constructed in accordance with client requirements and workplace procedures.
2 Conduct assessment.	2.1 Effective communication and interpersonal techniques are used that reflect sensitivity to individual social and cultural differences. 2.2 Integration of biometric systems with existing architecture is assessed. 2.3 Operational functions of biometric technologies and systems are assessed. 2.4 Application of single or multiple biometric technologies are assessed. 2.5 Data and information is assessed and errors or deficiencies identified. 2.6 Skills and training requirements for the use, operation and maintenance of biometric systems are determined.
3 Complete assessment.	3.1 Assessment results are analysed, accurately documented and prepared in an appropriate format in accordance with organisational requirements. 3.2 Findings are presented to relevant persons in accordance with workplace procedures. 3.3 Findings are supported by verifiable evidence in accordance with organisational requirements. 3.4 Feedback is sought, received and used in a constructive manner. 3.5 Recommendations or identified opportunities for system improvements are forwarded to relevant persons to inform future practice. 3.6 Records and reports 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
- assess data and information and identify errors or deficiencies
- assess the application, operation and outcomes of biometric technologies and systems
- 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 systems
- conduct and evaluate risk and threat assessments
- conduct contingency planning
- design effective treatment options
- determine biometric technology and system requirements, including single or multiple biometric applications
- determine resource requirements including personnel, tools and equipment
- determine security requirements
- determine skills and training requirements
- make effective decisions
- 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
- 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.
- written communication skills sufficient to complete relevant records and reports
- written communication skills sufficient to write assessment plan, document assessment results and complete relevant records and reports.

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 systems

REQUIRED SKILLS AND KNOWLEDGE

- appropriate mathematical procedures for estimating, measuring and calculating
- assessment methods and techniques
- biometric technology and systems 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 systems
- principles of cultural diversity and access and equity
- privacy and ethics issues associated with biometric systems
- problem identification and resolution procedures
- 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 systems 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 demonstrate competency in this unit

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

- 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

- determining security requirements based on an accurate assessment of existing security controls, assets, and existing and potential risks and threats
- determining skill and training requirements to support the application of biometric technologies and systems
- efficiently and effectively assessing the application, operation and outcomes of biometric technologies and systems, including an accurate assessment of data and information
- establishing purpose and context of assessment and plan, organising and coordinating assessment activities
- preparing and presenting assessment findings, seeking and reviewing feedback, and recommending opportunities for improvement to inform future practices.

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:

- Organisational requirements may relate to:**
- OHS
 - relevant industry codes of practice
 - telecommunications.
 - 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.
- Biometric 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 systems may**
- acquisition devices

- include:***
- 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.
- Privacy legislation may include:***
- Commonwealth, State and Territory Privacy Acts
 - national information privacy principles
 - national privacy principles.
- Relevant persons may include:***
- biometric technology specialists
 - clients
 - colleagues
 - external consultants
 - information technology specialists
 - manager.
- Security requirements may be:***
- risk and threat assessments
 - auditability
 - authentication
 - integrity
 - privacy protection
 - recovery
 - security objectives
 - auditability
 - authentication
 - integrity
 - privacy protection
 - recovery
 - security safeguards
 - administrative (licensing, authorisations, contingency plans, information access management, security incident procedures, security management, security awareness and training)
 - physical (include measures to protect information systems, buildings and equipment from natural and environmental hazards and unauthorised intrusions)
 - technical (access control, audit control, transmission

security).

Assessment plan may include:

- enrolment requirements
- level of assessment
- measurement and testing details and methods
- necessary resources (eg number of tests)
- privacy and ethics requirements
- timelines.

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.

- Existing architecture may include:**
- desktop PCs
 - local area networks (LANs)
 - mainframe systems
 - servers
 - websites
 - wide area networks (WANs).
- 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).
- Appropriate format may include:**
- formats that cater for those with special needs for example, producing documents in large print.
- System improvements may relate to:**
- backup systems
 - changes to biometrics settings
 - contingency plans
 - threshold levels.
- Records and reports:**
- may be:
 - computer-based
 - manual
 - other appropriate organisational communication system
 - may detail:
 - applications of biometric technologies and systems
 - functional operations of biometric technologies and systems
 - resource requirements
 - risk and threat assessments
 - security arrangements and additional requirements.

Unit Sector(s)

Unit sector Security

Competency field

Competency field Biometrics

