PRSBIO502A Assess biometric systems

Unit Descriptor
This unit specifies the skills and knowledge 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.

It also requires the ability to interpret and apply effective principles and requirements relating to confidentiality, privacy and security in own work.

Employability Skills
The required outcomes described in this unit of competency contain applicable facets of Employability Skills. The Employability Skills Summary of the qualification in which this unit of competency is packaged, will assist in identifying Employability Skill requirements.

Application of the Unit
This unit has been developed for application in any industry involved with the maintenance of workplace security. It supports the attainment of skills and knowledge required for competent workplace performance in security operations of all sizes. Skills and knowledge are to be used within the scope of the person’s job and authority.

Competency Field
to be advised

Sector
to be advised

ELEMENT PERFORMANCE CRITERIA

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 and/or the Range Statement. Assessment of performance is to be consistent with the Evidence Guide.

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 *appropriate personnel* 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 appropriate style and format in accordance with organisational requirements.

3.2 Findings are presented to appropriate personnel 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 appropriate personnel to inform future practice.
3.6 *Records and reports* are completed and maintained in accordance with legislative and organisational requirements.

**REQUIRED SKILLS AND KNOWLEDGE**

This describes the essential skills and knowledge and their level, required for this unit.

**Required skills include:**

- comply with legislation, regulations, standards, codes of practice relevant to workplace biometric systems
- comply with applicable confidentiality and privacy requirements
- analyse organisational security plans, goals, objectives and existing safeguards
- read and interpret technical information including plans, designs and specifications
- assess the application, operation and outcomes of biometric technologies and systems
- assess data and information and identify errors or deficiencies
- undertake effective enrolment of biometric/biographical data
- determine resource requirements including personnel, tools and equipment
- determine skills and training requirements
- determine security requirements
- determine biometric technology and system requirements, including single or multiple biometric applications
- conduct and evaluate risk and threat assessments
- research and analyse data and specifications
- design effective treatment options
- plan for contingencies
- use appropriate communication and interpersonal techniques
- relate effectively to people from a range of social, cultural and ethnic backgrounds and varying physical and mental abilities
• make effective decisions
• resolve problems
• select and use equipment and technology appropriate to the work task
• accurately and securely maintain records, reports and other workplace information
• organise work priorities and arrangements and complete work tasks within designated timeframes
• work effectively on an individual basis and with teams/groups.

**Required knowledge and understanding include:**

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

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 in the Performance Criteria is detailed below. Add any 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.

OHS requirements are to be in accordance with commonwealth, state or territory legislation and regulations, and organisational safety policies and procedures. Requirements relate to:

• identifying hazards
• controlling and minimising risks
• elimination of hazardous materials and substances
• safe use and operation of equipment including
  - personal protective clothing and equipment
  - safety equipment
  - first aid equipment
  - fire safety equipment
  - business technology
• correct manual handling including shifting, lifting and carrying
• safety procedures for the protection of others.
Legislative requirements are to be in accordance with applicable legislation from all levels of government that affect organisational operation. Requirements may relate to:

- award and enterprise agreements
- industrial relations
- Australian Standards
- confidentiality and privacy
- OHS
- the environment
- equal opportunity
- relevant industry codes of practice
- duty of care
- anti-discrimination and diversity
- licensing arrangements
- Compliance Policy Guidelines (CPGs).

Organisational requirements may relate to:

- legal, organisational and site guidelines, policies and procedures relating to own role and responsibility
- standard operating procedures
- quality assurance
- procedural manuals
- continuous improvement processes and standards
- OHS
- emergency and evacuation
- ethical standards
- recording and reporting
- access and equity principles and practices
- equipment use, maintenance and storage
- ergonomic practices
- environmental management (waste disposal, recycling and re-use guidelines)
- procedures for following instructions and accessing information
- physical environment.

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
- signature recognition
- iris recognition
- retina recognition
- voice recognition
- vein 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 include:

- acquisition devices
  - optical scanners
  - microphones
  - cameras (video, infrared-enabled video, single-image)
  - chip or reader embedded in peripheral device
- software
  - server-based authentication software for biometric authentication and logging
  - software associated with acquisition devices
- hardware
- interconnecting infrastructure
- biometric servers.

Privacy legislation may include:

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

Appropriate personnel may include:

- managers
- supervisors
- colleagues
- clients
- information technology specialists
- biometric technology specialists.
Security requirements may relate to:

- security objectives
  - authentication
  - integrity
  - privacy protection
  - recovery
  - auditability

- 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)

- risk and threat assessments
  - authentication
  - integrity
  - privacy protection
  - recovery
  - auditability.

Assessment plan may include:

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

Communication may be:

- face-to-face
- visual or written
- listening and understanding
- speaking clearly and directly
- reading independently
- writing to audience needs
- group interaction
- questioning to obtain information and/or clarify information and understanding
- oral reporting
• participation in routine meetings
• recording of discussions.

Interpersonal techniques may include:
• verbal or non-verbal language
• two-way interaction
• constructive feedback
• active listening
• questioning to clarify and confirm understanding
• interpreting non-verbal and verbal messages
• observation techniques
• use of positive, confident and co-operative language
• control of tone of voice and body language
• use of language and concepts appropriate to cultural differences
• use of clear presentations of options and consequences
• demonstrating flexibility and willingness to negotiate.

Social and cultural differences may include:
• language (verbal, non-verbal, non-English)
• traditional practices and observations
• beliefs, values and practices
• food and diet
• dress
• religious and spiritual observances
• social conventions
• cultural stereotypes
• conventions of gender/sexuality.

Existing architecture may include:
• servers
• websites
• local area networks (LANs)
• wide area networks (WANs)
• mainframe systems
• desktop PCs.

Multiple biometric 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).
System improvements may relate to:

- threshold levels
- changes to biometrics settings
- backup systems
- contingency plans

Records and reports:

- may be
  - manual
  - computer-based
  - other appropriate organisational communication system
- may detail
  - security arrangements and additional requirements
  - risk and threat assessments
  - functional operations of biometric technologies and systems
  - applications of biometric technologies and systems
  - resource requirements.

EVIDENCE GUIDE

The Evidence Guide provides advice on assessment and must be read in conjunction with the Performance Criteria, Required Skills and Knowledge, the Range Statement and the Assessment Guidelines for this Training Package.

Overview of assessment

- A person who demonstrates competency in this unit must be able to efficiently and effectively conduct an assessment of biometric technologies and systems in a workplace environment in compliance with applicable legal, privacy, safety and organisational requirements.

Critical aspects for assessment and evidence required to demonstrate competency in this unit

- Compliance with organisational policies and procedures, including OHS, relevant to work tasks undertaken in the workplace.
- Compliance with applicable legislation and codes of ethics applicable to privacy and client confidentiality.
- Establish purpose and context of assessment and plan, organise and coordinate assessment activities.
- Determine security requirements based on an accurate assessment of existing security controls, assets, and existing and potential risks and threats.
- Efficiently and effectively assess the application, operation and outcomes of biometric technologies and systems, including an accurate assessment of data and information.
• Determine skill and training requirements to support the application of biometric technologies and systems.

• Prepare and present assessment findings, seek and review feedback, and recommend opportunities for improvement to inform future practices.

### Context of and specific resources for assessment

• Competency may be assessed in an actual workplace or simulated environment that provides access to the required resources.

• Assessment is to occur under standard and authorised work practices, safety requirements and environmental constraints.

• The following resources must be available:
  - workplace location or simulated workplace
  - materials and equipment relevant to own work, role and responsibilities
  - specifications and work instructions.

### Method of assessment

The focus of this unit is on the technical skills and knowledge related to workplace biometric systems.

• Assessment must satisfy the endorsed Assessment Guidelines of the Asset Security Training Package.

• Assessment methods must confirm consistency and accuracy of performance (over time and in a range of workplace relevant contexts) together with application of underpinning knowledge.

• Assessment methods must confirm the ability to access and correctly interpret and apply the essential underpinning knowledge.

• Assessment may be in conjunction with assessment of other units of competency.