

- Troubleshooting techniques
- Types of maintenance techniques
- Data protection laws

Required skills

The individual needs to demonstrate the following skills:

- Report Writing
- Data collection
- Analytical skills
- Problem solving skills
- Communication skills
- Time management
- Critical thinking

EVIDENCE GUIDE

This provides advice on assessment and must be read in conjunction with the performance criteria, required knowledge and skills range.

1. Critical aspects of competency	Assessment requires evidence that the candidate: 1.1 Documented website user requirements specifications process as per the user needs. 1.2 Developed <i>website application visual hierarchy</i> as per the user needs. 1.3 Created website application site map as per the user needs. 1.4 Created front end web pages per website application design. 1.5 Created back-end web pages as per website application design. 1.6 Integrated website application to the backend as per workplace procedure. 1.7 Uploaded website application files as per host requirements. 1.8 Configured website server as per host requirements. 1.9 Fixed website application bugs as per monitoring report.
-----------------------------------	---

	1.10 Updated website application as per the workplace procedures.
2. Resource implications	The following resources should be provided: 2.1 Appropriately simulated environment where assessment can take place. 2.2 Access to relevant work environment. 2.3 Resources relevant to the proposed activities or tasks.
3. Methods of assessment	Competency may be assessed through: 3.1 Practical 3.2 Projects 3.3 Third Party Reports 3.4 Portfolio of evidence 3.5 Written tests
4. Context of assessment	Competency may be assessed in a workplace or in a simulated workplace.
5. Guidance information for assessment	Holistic assessment with other units relevant to the industry sector, workplace job role is recommended.

MANAGE ICT SECURITY

ISCED UNIT CODE: 0612 551 04A

TVET CDACC CODE: IT/OS/ICTA/CR/02/6/MA

UNIT DESCRIPTION

This unit covers the competencies required to manage ICT security. It involves assessing security needs, installing security control measures and maintaining ICT system security.

ELEMENTS AND PERFORMANCE CRITERIA

ELEMENT	PERFORMANCE CRITERIA
These describe the key outcomes which make up workplace functions	These are assessable statements which specify the required level of performance for each of the elements <i>(Bold and italicized terms are elaborated in the range)</i>
1. Assess security needs	1.1 ICT security assets are documented based on organization's policy. 1.2 ICT security threats are identified as per organization policy. 1.3 ICT security risk impact assessment is performed as per industry standards. 1.4 ICT security risk assessment report is compiled as per risk impact assessment performed.
2. Install security control measures	2.1 Physical control measures are implemented according to the organisation ICT security policy. 2.2 Logical security control measures are implemented according to the organisation ICT security policy. 2.3 ICT security control measures implemented are tested according to the organization ICT security policy.

3. Maintain ICT system security	3.1 ICT system security regular monitoring is carried out as per the organization policy. 3.2 ICT system security monitoring report is prepared as per the organisation policy. 3.3 ICT system security is updated as per the monitoring report.
---------------------------------	---

RANGE

This section provides work environment and conditions to which the performance criteria apply. It allows for different work environment and situations that will affect performance.

Variable	Range
	<i>May include but not limited to:</i>
1. ICT security assets may include but are not limited to:	• Software • Hardware • Firmware • Data
2. ICT security threats may include but are not limited to:	• Malware • Virus • Phishing • Hacking • Denial of service
3. Physical control measures may include but are not limited to:	• Grills • Security guards • Firewall • Locks
4. Logical security control measures may include but are not limited to:	• Firewall • Password policy • Encryption • Authentication • Access right policy

REQUIRED KNOWLEDGE AND SKILLS

This section describes the knowledge and skills required for this unit of competency.

Required Knowledge

The individual needs to demonstrate knowledge of:

- Documentation processes
- Computer and devices settings
- Cyber security threats and measures
- Technology trends in manage ICT threats
- Troubleshooting techniques
- Types of maintenance techniques
- Data protection laws

Required skills

The individual needs to demonstrate the following skills:

- Report Writing
- Data collection
- Analytical skills
- Problem solving skills
- Communication skills
- Time management
- Critical thinking

EVIDENCE GUIDE

This provides advice on assessment and must be read in conjunction with the performance criteria, required knowledge and skills range.

1. Critical aspects of competency	Assessment requires evidence that the candidate: 1.1 Identified <i>ICT security threats</i> as per organization policy. 1.2 Implemented <i>Physical control measures</i> according to the organisation ICT security policy.
-----------------------------------	---

	1.3 Implemented <i>Logical security control measures</i> according to the organisation ICT security policy. 1.4 Monitored ICT security system as per the organization policy. 1.5 Updated ICT security system as per the monitoring report.
2. Resource implications	The following resources should be provided: 4.1.Appropriately simulated environment where assessment can take place. 4.2.Access to relevant work environment. 4.3.Resources relevant to the proposed activities or tasks.
3. Methods of assessment	Competency may be assessed through: 5.1 Practical 5.2 Projects 5.3 Third Party Reports 5.4 Portfolio of evidence 5.5 Written tests
4. Context of assessment	Competency may be assessed in a workplace or in a simulated workplace.
5. Guidance information for assessment	Holistic assessment with other units relevant to the industry sector, workplace job role is recommended.

DEVELOP DESKTOP APPLICATION

ISCED UNIT CODE: 0613 551 05A

TVET CDACC CODE: IT/OS/ICTA/CR/03/6/MA

UNIT DESCRIPTION

This unit covers the competencies required to develop desktop application. It involves assessing desktop application requirements, designing desktop application, creating desktop application, deploying desktop application and maintaining desktop application.

ELEMENTS AND PERFORMANCE CRITERIA

ELEMENT	PERFORMANCE CRITERIA
These describe the key outcomes which make up workplace functions	These are assessable statements which specify the required level of performance for each of the elements <i>(Bold and italicized terms are elaborated in the range)</i>
1. Assess desktop application requirements.	1.1 Desktop application requirements are identified as per the user needs. 1.2 Desktop application requirements specifications process is documented as per the user needs. 1.3 Desktop application requirements specifications are reviewed as per user need report.
2. Design desktop application.	2.1 Desktop application design requirements are identified as per user needs. 2.2 Desktop application design methods are implemented as per requirements specifications document 2.3 Desktop application visual hierarchy is developed as per the design method

ELEMENT	PERFORMANCE CRITERIA
These describe the key outcomes which make up workplace functions	These are assessable statements which specify the required level of performance for each of the elements <i>(Bold and italicized terms are elaborated in the range)</i>
3. Create desktop application.	3.1 Desktop application development environment is set up as per the user manual. 3.2 Desktop application <i>programming fundamentals</i> are applied as per the workplace procedures. 3.3 Desktop application is developed as per design methods 3.4 Desktop application is tested as per the workplace procedures. 3.5 Desktop application is optimized as per the workplace procedures.
4. Deploy desktop application	4.1 Desktop application is packaged as per user the workplace procedures. 4.2 Desktop application deployment plan is developed as per the user requirements. 4.3 Desktop application is installed per the workplace procedures. 4.4 Desktop application user training is conducted as per workplace procedures.
5. Maintain desktop application.	5.1 Desktop application maintenance schedule is prepared as per workplace procedure. 5.2 Desktop application maintenance is performed as per application maintenance schedule. 5.3 Desktop application maintenance report is developed as per work procedure

RANGE

This section provides work environment and conditions to which the performance criteria apply. It allows for different work environment and situations that will affect performance.

Variable	Range
1. Desktop application design methods may include but are not limited to:	• User-centred Design • Visual Design • Interaction Design • Wireframing and Prototyping
2. Desktop application programming fundamentals may include but are not limited to:	• Basic syntax • Variables • Data types • Control structures • Objects • Functions • Data structures • Debugging
3. Desktop application visual hierarchy may include but are not limited to:	• Graphical user interface • Hierarchy of Elements • Typography • Colour • Spacing and Layout

REQUIRED KNOWLEDGE AND SKILLS

This section describes the knowledge and skills required for this unit of competency.

Required Knowledge

The individual needs to demonstrate knowledge of:

- Documentation processes
- Computer and devices settings
- Technology trends in desktop application
- Troubleshooting techniques

- Types of maintenance techniques
- Data protection laws

Required skills

The individual needs to demonstrate the following skills:

- Report Writing
- Data collection
- Analytical skills
- Problem solving skills
- Communication skills
- Time management
- Critical thinking

EVIDENCE GUIDE

This provides advice on assessment and must be read in conjunction with the performance criteria, required knowledge and skills range.

1. Critical aspects of competency	Assessment requires evidence that the candidate: 1.1 Desktop application requirements specifications process is documented as per the user needs. 1.2 <i>Desktop application visual hierarchy</i> is developed as per the design method. 1.3 Desktop application is developed as per design methods. 1.4 Desktop application is optimized as per the workplace procedures 1.5 Desktop application is installed per the workplace procedures. 1.6 Desktop application is packaged as per user the workplace procedures. 1.7 Desktop application maintenance is performed as per application maintenance schedule.
-----------------------------------	---

2. Resource implications	The following resources should be provided: 6.1. Appropriately simulated environment where assessment can take place. 6.2. Access to relevant work environment. 6.3. Resources relevant to the proposed activities or tasks.
3. Methods of assessment	Competency may be assessed through: 7.1 Practical 7.2 Projects 7.3 Third Party Reports 7.4 Portfolio of evidence 7.5 Written tests
4. Context of assessment	Competency may be assessed in a workplace or in a simulated workplace.
5. Guidance information for assessment	Holistic assessment with other units relevant to the industry sector, workplace job role is recommended.