Occupational Standards of Competence

Cyber Security Level 3

Hastings House West, Balmoral Gap, Hastings, Christ Church, Barbados Telephone: (246) 435-3096 Fax: (246) 429 2060 E-mail: office@tvetcouncil.com.bb

Published by:
The Technical and Vocational Education and Training (TVET) Council
Hastings House West
Balmoral Gap
Christ Church
BARBADOS, W.I.
Tel: (246) 435-3096
Fax: (246) 429-2060
Email: office@tvetcouncil.com.bb Website: www.tvetcouncil.com.bb

ACKNOWLEDGEMENTS

The Technical and Vocational Education and Training Council thanks the following for their contribution to the development of this document:

Australian Government – National Register on Vocational Education and Training (VET)

Instructus Skills - National Occupational Standards, UK

Cyber Security National Occupational Standards (Canada)

Cyber Security for Due Diligence (SDD), G5 Cyber Security

Government Cyber Security Strategy, UK

National Cyber Security Centre (NCSC), UK

National Occupational Standards (NOS), UK

Technical Experts for Cyber Security Working Group

Ms. Ashell Ford	-	Manager, Information Security & Technology Risk Management, CIBC First Caribbean International Bank
Mr. Donovan Smith	-	Technical Director, Open Network Technical Solutions Inc, Barbados
Ms. Debra Hope	-	Consultant/External Technical Writer, Technical and Vocational Education and Training (TVET) Council

Validation Committee Members

Jason Clark	-	ICT Support and Information Systems, Tourism Marketing Inc., Barbados
Antonio Beckles	-	Senior Technical Analyst, Republic Bank Limited, Barbados
Khristina Rogers	-	Information Security Analyst, CIBC First, Caribbean, Barbados

Qualification Overview

NVQB

in

Cyber Security

Level 3

NVQ in Cyber Security – Level 3

Qualification Overview

The NVQ level 3 in Cyber Security is designed for persons in roles across all occupations and sectors of employment. The objective of the qualification is to provide learners with the knowledge, skills and attitudes related to cyber security awareness and practices. The duties of a person at this level are to assess, protect and defend data within systems and strive to prevent incidents and network attacks. The standard includes competencies for health and safety, teamwork, communication and improving personal performance.

Achievement at Level 3 recognises the ability to gain and apply fundamental knowledge and skills across a variety of areas to independently gather and analyse information and complete tasks in a range of contexts with guidance only as necessary. It will provide the learner with a chance to develop knowledge and learn practical skills, which can be used to seek employment or proceed onto further studies.

Like all NVQs, this qualification is competence based. This means that it is linked to a candidate's ability to competently perform a range of tasks connected with their work.

Who is the Qualification for?

This qualification is aimed at anyone seeking to acquire or improve their cyber security skills. It supports the development of knowledge, skills and attitudes required to take on responsibilities such as assessing risks to improve security policies and protocols; anticipating information security risks; protecting an organisation's systems and networks; responding to security alerts and preventing cyber-attacks of various types.

Candidates are not required to have any prior knowledge or experience of cyber security for this qualification; however, possession of a qualification at Level 2 in Digital Skills, Networking, Computer Science, Information Technology or a similar qualification is required or a basic knowledge of Windows and/or Linux operating systems.

Jobs within the occupational area:

- Security officer/specialist
- Cyber security analyst
- Incident responder
- Security systems administrator
- Junior cyber security specialist
- Junior cyber threat intelligence analyst

This list is not exhaustive and only serves to illustrate the breadth of the qualification.

A011603 - APPROVED NATIONAL VOCATIONAL QUALIFICATION STRUCTURE

CYBER SECURITY - LEVEL 3

To achieve the full qualification, candidates must complete all eleven (11) units.

Mandatory Units (All must be completed)	**CODES**
1. Evaluate an organisation's compliance with cyber security standards and law	**UA38803**
1.1 Research existing security standards and laws 1.2 Analyse compliance and non-compliance activities and make recommendations 1.3 Align organisational activities to required standards	
2. Respond to cyber security incidents	**UA38903**
2.1 Ascertain cyber security incidents and contribute to their containment 2.2 Communicate information on cyber security incidents 2.3 Contribute to post-incident activities	
3. Assess cyber security threats and vulnerabilities	**UA39003**
3.1 Review workplace cyber security threats and vulnerabilities 3.2 Assess risks and the potential business impact of cyber security threats 3.3 Finalise cyber security threat and vulnerability assessments	
4. Analyse cyber security insider risks and threats and devise recommendations	**UA39103**
4.1 Determine cyber security insider risks and threats 4.2 Complete an analysis of cyber security insider risks and threats 4.3 Devise and distribute recommendations arising from the analysis 4.4 Review the organisational training response to cyber security insider risks and threats	
5. Work within in a team	**UA39203**
5.1 Contribute to team activities 5.2 Share knowledge and information 5.3 Give and receive support	

Mandatory Units (All must be completed)		CODES
6.	**Promote workplace cyber security awareness and best practices**	**UA39303**
6.1	Develop cyber security awareness in the work area	
6.2	Support effective cyber security practices in the work area	
6.3	Review cyber security awareness in the work area	
7.	**Protect against cyber security threats**	**UA39403**
7.1	Establish cyber security policies and controls	
7.2	Secure sensitive data	
8.	**Manage safety and health in own area of responsibility**	**UA41703**
8.1	Evaluate responsibilities and liabilities in relation to safety and health legislation and regulations	
8.2	Assess and minimise safety and health risks in own area of responsibility	
8.3	Review health and safety policies in own area of responsibility	
8.4	Monitor safety and health in own area of responsibility	
9.	**Contribute to the protection of the cyber security environment**	**UA39503**
9.1	Work in an environmentally conscious way	
9.2	Contribute to continuous improvements in protecting the environment	
10.	**Maintain and improve personal performance**	**U65403**
10.1	Plan and organise work	
10.2	Maintain working relationships	
10.3	Improve own performance	
11.	**Communicate to develop and maintain networks and relationships**	**U78103**
11.1	Communicate ideas and information	
11.2	Develop trust and confidence	
11.3	Develop and maintain networks and relationships	
11.4	Manage difficulties into positive outcomes	

UA38803 Evaluate an organisation's compliance with cyber security standards and law

Unit Descriptor:

This unit describes the knowledge, skills and attitudes required to identify cyber security standards and laws and evaluate an organisation's working practices for compliance. It also includes determining what changes are required to continue compliance.

ELEMENT	PERFORMANCE CRITERIA
Candidates must be able to:	
1. Research existing security standards and laws	1.1 Identify the **standards and laws** required for organisational cyber security operations and summarise findings.
	1.2 Analyse and align required laws and standards to organisational cyber security operations.
	1.3 Obtain and analyse the organisation's existing **cyber security** compliance **strategies,** if available and document the outcomes of the findings.
	1.4 Review and determine the time periods and benchmarking of compliance evaluation requirements in accordance with organisational procedures or **industry best practices.**
2. Analyse compliance and non-compliance activities and make recommendations	2.1 Conduct compliance assessments and document findings according to organisational procedures or **industry best practices.**
	2.2 Identify and document areas of non-compliance and near misses in accordance with organisational procedures or **industry best practices**.
	2.3 Recommend suitable actions to address non-compliance to **required personnel.**

		2.4 Report areas of potential risk and non-compliance to **required personnel** in accordance with organisational procedures.
3.	Align organisational activities to required standards	3.1 Develop and document compliance requirements according to established organisational procedures or **industry best practice.**
		3.2 Distribute requirements to **required personnel** to facilitate the realignment of business operations to requirements.
		3.3 Develop an evaluation strategy as recommended by established cyber security standards**.**
		3.4 Submit documents relating to compliance requirements to **required personnel** and seek and respond to feedback.

RANGE STATEMENT

All range statements must be assessed:

1. Standards and laws may include but are not limited to:

- Local (e.g. Computer Misuse Act, Data Protection Act)
- International (e.g. EU Cyber Security Act, General Data Protect Regulation (GDPR), ISO 27000 Series
- Industry specific

2. Strategies may include but are not limited to:

- Assessing current cyber security and compliance posture
- Determining how to reduce risk
- Managing risk exposure in the future

3. Industry best practices may include but are not limited to:

- Industry regulations
- Government regulations or policies
- Cyber security frameworks
- Client/customer contractual terms
- Key business concerns (e.g. countries with data/privacy laws, markets with heavy regulations, clients with high confidentiality standards)

4. Required personnel may include but are not limited to:

- Legal entity
- Cyber security lawyer
- Cyber security policy advisor

UNDERPINNING KNOWLEDGE AND SKILLS

Candidates must know and understand:

1. What are the standards and laws to be followed in an organisation's cyber security operations.
2. How to summarise the findings of identified standards and laws required for an organisation's cyber security operations.
3. How to analyse and align required laws and standards to organisational cyber security operations.
4. What are the organisation's existing cyber security compliance strategies.
5. What are the organisational policies and procedures for documenting the outcomes of the findings and how to do so.
6. How to obtain and analyse the organisation's existing cyber security compliance strategies and document outcomes.
7. Why it is important to determine time periods and benchmarking of compliance evaluation requirements and how to do so.
8. What is a compliance assessment.
9. How to conduct a compliance assessment according to organisational or industry best practices.
10. How to document assessment findings according to organisational or industry best practices and standards and what are the policies and procedures for doing so.
11. What are areas of non-compliance.
12. What is a gap analysis and how to conduct one.
13. How to identify and document areas of non-compliance and near misses and what are the organisational or industry best practices for doing so.
14. Why it is important to recommend suitable actions to address non-compliance incidents to relevant personnel and how to do so.
15. How to report areas of potential risk and non-compliance to relevant personnel and what are the organisational procedures for doing so.
16. How to develop and document compliance requirements.
17. Why it is important to distribute requirements to required personnel to facilitate realignment of business activities to requirements and how to do so.
18. What is an evaluation strategy.
19. How to develop an evaluation strategy as recommended by cyber security standards and industry best practices.
20. When to submit documents to required personnel and seek and respond to feedback and how to do so.

EVIDENCE GUIDE

For assessment purposes:

(1) Critical Aspects of Evidence

Candidates must prove that they can carry out **all** of the elements, meeting **all** the performance criteria, range and underpinning knowledge **on more than one occasion**. This evidence must come from a real work environment.

(2) Methods of Assessment

Assessors should gather a range of evidence that is valid, sufficient, current and authentic.

Evidence may be collected in a variety of ways including:

- Observation
- Written/oral questioning
- Written evidence
- Witness testimony
- Professional discussion
- Products of work

Questioning techniques should not require language, literacy or numeracy skills beyond those required in this unit of competency.

(3) Context of Assessment

This unit may be assessed on the job, off the job or a combination of both. Where assessment occurs off the job, that is the candidate is not in productive work, then an appropriate simulation must be used where the range of conditions reflects realistic workplace situations. The competencies covered by this unit would be demonstrated by a candidate working alone or as part of a team. The assessment environment should not disadvantage the candidate.

The candidate must have access to all tools, equipment, materials and documentation required. The candidate must be permitted to refer to any relevant workplace procedures, product and manufacturing specifications, codes, standards, manuals and reference materials.

Simulation **should not be used**, except in exceptional circumstances where natural work evidence is unlikely to occur.

UA38903 Respond to cyber security incidents

Unit Descriptor:

This unit describes the knowledge, skills and attitudes required to respond to and contain cyber security incidents. It applies to those working in a broad range of industries and job roles who work alongside technical experts to develop cyber security risk-management strategies.

ELEMENT	PERFORMANCE CRITERIA
Candidates must be able to:	
1. Ascertain cyber security incidents and contribute to their containment	1.1 Identify and confirm the nature and location of **cyber security incidents** in accordance with **legislative requirements or industry best practices**.
	1.2 Evaluate the potential risk of different **cyber security incidents** to an organisation's assets in terms of loss of confidentiality, integrity and availability.
	1.3 Report security incidents in a timely manner following organisational policies and procedures**.**
	1.4 Assess the severity of incidents following organisational procedures or **industry best practices** on incident response procedures.
	1.5 Contain cyber security incidents following **legislative requirements** or **industry best practices** or **cyber security incident response** procedures and planning.
	1.6 Confirm that the root cause of incidents have been eradicated following **legislative requirements** or **industry best practices** on cyber security incident response procedures and planning.
2. Communicate information on cyber security incidents	2.1 Escalate **cyber security incidents** to **required personnel** according to organisational policies and procedures.

		2.2 Consult with required internal and external stakeholders on communication needs relating to **cyber security incidents**.
		2.3 Alert required external parties of cyber security incidents following organisational procedures or **industry best practices** and legislative requirements.
3.	Contribute to post-incident activities	3.1 Conduct post-incident review and disseminate the report to relevant persons according to organisational policy and procedures.
		3.2 Identify lessons learnt from incident response and recommend changes to the organisational policy and procedures or cyber security response plan.
		3.3 Update the organisational policy and procedures or cyber security response plan to reflect the review outcomes following **industry best practices**.
		3.4 Communicate lessons learnt and recommendations to required personnel according to organisational procedures.

RANGE STATEMENT

All range statements must be assessed:

1. **Cyber security incidents** may include but are not limited to:

    - Attempts to gain unauthorised access to a system and/or to data.
    - Unauthorised use of systems
    - Unauthorised changes to a systems
    - Unlawful consent
    - Malicious disruption and/or denial of service

2. **Legislative requirements** may include but are not limited to:

    - Data protection
    - Notifiable data breach legislation
    - Privacy laws
    - Established international legislation
    - Cyber security regulations

3. **Organisational cyber security incident response** may include but not is limited to:

    - Assessing potential risk
    - Confirming the nature and location of incidents
    - Assessing the severity of incidents
    - Containing the incident
    - Eliminating the root cause of the incident
    - Notifying internal and external stakeholders of the incident
    - Communicating with internal and external stakeholders
    - Conducting post-breach reviews

4. **Industry best practices** may include but are not limited to:

    - Industry regulations
    - Government policies
    - Cyber security frameworks
    - Cyber security standards and laws

5. **Required personnel** may include but are not limited to:

    - End users
    - Information Technology (IT) staff
    - Senior management
    - Senior cyber security information officer

UNDERPINNING KNOWLEDGE AND SKILLS

Candidates must know and understand:

1. What is a cyber security incident.
2. What are the different types of cyber security incidents.
3. How to identify and confirm the nature and location of cyber security incidents.
4. What are the different cyber security threats to an organisation's assets in terms of loss of confidentiality, integrity and availability and how to evaluate the potential risks.
5. Why it is important to report security incidents in a timely manner and how to do so.
6. Why it is important to estimate risk, likelihood and potential consequences of an incident.
7. How to assess the severity of incidents following organisational procedures or industry best practices.
8. What are the legislative requirements and industry best practices that relate to cyber security.
9. What are the organisational policies and procedures or industry best practices relating to cyber security incident response procedures and planning.
10. What are the risk mitigation strategies and procedures relating to cyber security.
11. What are the key features of a cyber security incident response plan.
12. How to ensure that cyber security incidents are contained and what are the legislative requirements and the industry best practices on cyber security incident response procedures for doing so.
13. How to confirm that the root cause of the incident has been eradicated following legislative requirements and industry best practices.
14. Why it is important to escalate a cyber security incident to required personnel and how to do so.
15. Who are internal and external stakeholders.
16. What are the organisational procedures for developing communication plans.
17. Why it is important to consult with required internal and external stakeholders on their communication needs relating to cyber security incidents and how to do so.
18. Why it is important to alert required external parties and what are the legislative requirements and organisational procedures for doing so.
19. How to conduct a post-incident review and disseminate the report to relevant persons.
20. Why it is important to identify lessons learnt from incident responses and recommend changes to the organisational policy and procedures or cyber security response plan and how to do so.
21. What are the reporting methods for cyber security incidents, including official government channels.

22. Why it is important to update the organisational policy and procedures or cyber security response plan to reflect review outcomes following industry best practices and how to do so.

23. Why it is important to communicate lessons learnt and make recommendations to required personnel.

EVIDENCE GUIDE

For assessment purposes:

(1) Critical Aspects of Evidence

Candidates must prove that they can carry out **all** of the elements, meeting **all** the performance criteria, range and underpinning knowledge **on more than one occasion**. This evidence must come from a real work environment.

(2) Methods of Assessment

Assessors should gather a range of evidence that is valid, sufficient, current and authentic.

Evidence may be collected in a variety of ways including:

- Observation
- Written/oral questioning
- Written evidence
- Witness testimony
- Professional discussion
- Products of work

Questioning techniques should not require language, literacy or numeracy skills beyond those required in this unit of competency.

(3) Context of Assessment

This unit may be assessed on the job, off the job or a combination of both. Where assessment occurs off the job, that is the candidate is not in productive work, then an appropriate simulation must be used where the range of conditions reflects realistic workplace situations. The competencies covered by this unit would be demonstrated by a candidate working alone or as part of a team. The assessment environment should not disadvantage the candidate.

The candidate must have access to all tools, equipment, materials and documentation required. The candidate must be permitted to refer to any relevant workplace procedures, product and manufacturing specifications, codes, standards, manuals and reference materials.

Simulation **should not be used**, except in exceptional circumstances where natural work evidence is unlikely to occur.

UA39003 Assess cyber security threats and vulnerabilities

Unit Descriptor:

This unit describes the knowledge, skills and attitude required to maintain a secure network through identifying and assessing cyber security threats and vulnerabilities for an organisation.

It applies to those working in a broad range of industries who as part of their job role, contribute to assessing the level of risk relating to real and potential cyber security breaches.

ELEMENT	PERFORMANCE CRITERIA
Candidates must be able to:	
1. Review workplace cyber security threats and vulnerabilities	1.1 Research and collect information from a range of **threat intelligence sources** to identify new threats and threat actors.
	1.2 Identify relevant **legislative requirements**, organisational data security/protection policies and procedures.
	1.3 Conduct organisation-wide cyber security audits following organisational policy and procedures or **industry best practices.**
	1.4 Identify threats and vulnerabilities to workplace security and document in accordance with organisational requirements or **industry best practices**.
2. Assess risks and the potential impact of cyber security threats	2.1 Evaluate cyber security risks and their likelihood, impact, consequences and suggested mitigation strategies.
	2.2 Review industry level threats, vulnerabilities and best practice **cyber security strategies** to facilitate the evaluation of risks and their potential impact.
	2.3 Assign risk levels for identified cyber risks based on measurement scale.
	2.4 Conduct **threat modelling** to examine the impact of threats on the infrastructure and key assets.

		2.5 Document newly identified threats and trends and make recommendations on how to mitigate these in line with organisational requirements or **industry best practices**.
		2.6 Apply **threat analysis tools** in line with organisational procedures or **industry best practices**.
		2.7 Comply with cyber security legislation and **industry best practices** when carrying out threat analysis and modelling activities.
3.	Finalise cyber security threat and vulnerability assessments	3.1 Document impact findings and include analysis and recommendations for mitigating identified risks.
		3.2 Support the communication of cyber security threat and vulnerability assessment outcomes and recommendations to **required personnel**.
		3.3 Seek feedback as required on assessment findings.
		3.4 Integrate feedback to finalise threat and vulnerability assessments.
		3.5 Track risks identified in vulnerability assessments to remediation in accordance with organisational data security/protection policies and procedures or **industry best practices.**

RANGE STATEMENT

All range statements must be assessed:

1. **Threat intelligence sources** may include but are not limited to:

   - Threat intelligence databases
   - Open Source Intelligence (OSINT)
   - Warning, Advice and Reporting Point communities (WARP)
   - Relevant news media sources
   - Human Intelligence (HUMINT)
   - Social Media Intelligence (SOCINT)

2. **Legislative requirements** may include but are not limited to:

   - Data privacy and protection
   - Notifiable data breach legislation
   - Privacy laws
   - Established international legislation
   - Cyber security regulations

3. **Industry best practices** may include but are not limited to:

   - Industry regulations
   - Government policies
   - Cyber security frameworks
   - Cyber security standards and laws

4. **Cyber security strategies** may include but are not limited to:

   - Technical controls
   - Administrative controls
   - Physical controls

5. **Threat modelling** may include but is not limited to:

   - Identifying security requirements
   - Pinpointing security threats and potential vulnerabilities
   - Quantifying threat and vulnerability critically
   - Prioritising remediation methods

6. **Threat analysis tools** may include but are not limited to:

   - Firewalls
   - Antivirus software
   - Anti-spyware
   - Password management software

7. **Required personnel** may include but are not limited to**:**

   - End users
   - Information Technology (IT) staff
   - Senior management
   - Senior cyber security information officer

UNDERPINNING KNOWLEDGE AND SKILLS

Candidates must know and understand:

1. What are the legislative requirements which relate to cyber security.
2. What are threat intelligence sources.
3. Why it is important to research and collect information from a range of threat intelligence sources to identify new threats and threat actors.
4. What are the organisational data security/protection policies and procedures.
5. Why it is important to identify relevant organisational data security/protection policies and procedures and how to do so.
6. What is the potential impact of cyber-attacks on an organisation.
7. What are the cyber security risks affecting organisational operations.
8. What is an organisation-wide cyber security audit.
9. How to conduct organisation-wide cyber security audits and what is the organisational policy for doing so.
10. How to identify and document threats and vulnerabilities to workplace security.
11. What are mitigation strategies.
12. How to evaluate cyber security risks and their likelihood, impact, consequences and suggested mitigation strategies.
13. What are industry level threats, vulnerabilities and best practice cyber security strategies and how they are reviewed.
14. What are risk levels.
15. What is a measurement scale.
16. How to assign risk levels for identified cyber risks based on measurement scale.
17. What is a threat model and what are threat modelling activities.
18. What are the common procedures for cyber threat rating and modelling.
19. How to carry out threat modelling to examine the impact of threats on the infrastructure and key assets.
20. Why it is important to document new threats and trends identified and make recommendations on how to mitigate them.
21. What are threat analysis tools.
22. What are the strategies, techniques and tools that improve an organisation's cyber security and audit processes.
23. How to apply threat analysis tools and what are the organisational procedures or industry best practices for doing so.

24. What is the cyber security legislation or industry best practices related to carrying out threat analyses and modelling activities and why it is important to comply with these.
25. Why it is important to document impact findings that include recommendations for required responses to control risk and how to do so.
26. What are the different ways to communicate cyber security threat and vulnerability assessment outcomes.
27. How to communicate cyber security threats and vulnerability assessment outcomes and recommendations to required personnel.
28. Why it is important to seek feedback as required on the assessment findings and how to do so.
29. How to integrate feedback to finalise a threat and vulnerability assessment.
30. How to track risks identified in vulnerability assessments to remediation and what are the organisational data security protection policies and procedures or industry best practices for doing so.

EVIDENCE GUIDE

For assessment purposes:

(1) Critical Aspects of Evidence

Candidates must prove that they can carry out **all** of the elements, meeting **all** the performance criteria, range and underpinning knowledge **on more than one occasion**. This evidence must come from a real work environment.

(2) Methods of Assessment

Assessors should gather a range of evidence that is valid, sufficient, current and authentic.

Evidence may be collected in a variety of ways including:

- Observation
- Written/oral questioning
- Written evidence
- Witness testimony
- Professional discussion
- Products of work

Questioning techniques should not require language, literacy or numeracy skills beyond those required in this unit of competency.

(3) Context of Assessment

This unit may be assessed on the job, off the job or a combination of both. Where assessment occurs off the job, that is the candidate is not in productive work, then an appropriate simulation must be used where the range of conditions reflects realistic workplace situations. The competencies covered by this unit would be demonstrated by a candidate working alone or as part of a team. The assessment environment should not disadvantage the candidate.

The candidate must have access to all tools, equipment, materials and documentation required. The candidate must be permitted to refer to any relevant workplace procedures, product and manufacturing specifications, codes, standards, manuals and reference materials.

Simulation **should not be used**, except in exceptional circumstances where natural work evidence is unlikely to occur.

UA39103 Analyse cyber security insider risks and threats and devise recommendations

Unit Descriptor:

This unit describes the knowledge, skills and attitudes required to analyse intentional and unintentional cyber security insider risks and threats in an organisation or workplace context. Candidates will be required to devise recommendations to minimise risks and threats and recommend organisational training in response.

ELEMENT	PERFORMANCE CRITERIA
Candidates must be able to:	
1. Determine cyber security insider risks and threats	1.1 Obtain work details and scope from **required personnel** and arrange for access to required technology in accordance with **organisational security arrangements** and **required legislation, codes, regulations and standards**.
	1.2 Evaluate and apply privacy requirements in accordance with organisational policies and procedures or **industry best practices**.
	1.3 Identify systems of a **critical nature** to business and key **data** logs for detection of **cyber security insider risks and threat** activity.
	1.4 Ascertain high-risk **data** using an organisational risk framework.
	1.5 Monitor organisational behaviour patterns to identify **cyber security insider risks and threats.**
2. Complete an analysis of cyber security insider risks and threats	2.1 Identify the **model or standard** required to analyse **cyber security insider risks and threats**.
	2.2 Analyse sensors and data logs and perform risk assessments to identify high-risk users and behaviours.

3.	Devise and distribute recommendations arising from the analysis	3.1 Prioritise **insider risks** and threats based on analysis according to organisational policies and procedures or industry best practices.
		3.2 Develop recommendations to minimise or eliminate insider risks and threats based on analysis findings.
		3.3 Seek and integrate feedback of **required personnel** on draft recommendations.
		3.4 Distribute information and documentation to required personnel in accordance with legislative requirements and organisational policies and procedures.
4.	Review the organisational training response to cyber security insider risks and threats	4.1 Assess identified **cyber security insider risks and threats** to identify training requirements.
		4.2 Develop recommendations for training to address **cyber security insider risks and threats** in accordance with organisational data protection policies and procedures and **industry best practices.**
		4.3 Seek feedback on training recommendations from **required personnel**.
		4.4 Finalise and distribute training recommendations according to organisational policies and procedures.
		4.5 Recommend cyber security training to **required personnel** in accordance with organisational policy and procedures and industry best practices.

RANGE STATEMENT

All range statements must be assessed:

1. **Organisational security arrangements** and **required legislation, codes, regulations and standards** may include but are not limited to:

   - Data loss mitigation
   - Risk framework
   - Security arrangements
   - Security control standards

2. **Cyber security insider risks and threats** may include but are not limited to:

   - Careless insiders
   - Compromised insiders
   - Expired users with valid credentials
   - Malicious insiders
   - Misinformed insiders

3. **Data** may include but is not limited to:

   - Classified
   - Confidential
   - Private
   - Protected
   - Public
   - Restricted
   - Secret
   - Sensitive
   - Internal
   - Top secret

4. **Model or standard** may include but is not limited to:

   - National Institute of Standards and Technology (NIST)
   - ISO 27000 Best practices for information security management systems
   - Centre for Internet Security (CIS 20)
   - Impact Metrics

5. **Required personnel** may include but is not limited to**:**

   - End users
   - Information Technology (IT) staff
   - Senior management
   - Senior cyber security information officer

6. **Industry best practices** may include but is not limited to:

   - Industry regulations
   - Government policies
   - Cyber security frameworks
   - Cyber security standards and laws

UNDERPINNING KNOWLEDGE AND SKILLS

Candidates must know and understand:

1. What are the key requirements of legislation, codes, regulations and standards relating to analysing cyber security insider risks and threats.
2. What are the organisational cyber security policies and procedures.
3. How to obtain work details and scope from required personnel and arrange for access to required technology and what are the organisational security arrangements and required legislation, codes, regulations and the standards for doing so.
4. Why it is important to evaluate and apply privacy requirements and how to do so.
5. What are systems of a critical nature.
6. What are sensors and data logs.
7. What are the key features of different data classifications.
8. Why it is important to identify systems of a critical nature to business and key data logs for detection of cyber security insider risk and threat activity and how to do so.
9. What is high risk data.
10. What is an organisational risk framework.
11. How to determine high-risk data using an organisational risk framework.
12. What are organisational behaviour patterns.
13. What are cyber security insider risks and threats.
14. What are intentional and unintentional cyber security insider risks and threats.
15. What are key organisational behavioural patterns that indicate cyber security insider risks and threats.
16. Why it is important to monitor organisational behaviour patterns to identify cyber security insider risks and threats and how to do so.
17. What are key data loss mitigation controls.
18. What are the different types of cyber security models and standards.
19. What is model-based analysis.
20. What are the key types of model-based insider risk and threat analysis tools.
21. How to identify the model required to analyse cyber security insider risks and threats.
22. How to perform a model-based analysis of cyber security insider risks and threats.
23. What is a risk assessment.
24. What are the procedures for assessing risks, including identifying different types of high-risk users.
25. Where are the sensitive locations at risk of cyber security insider risks and threats.

26. Why it is important to analyse sensors and data logs and perform risk assessments to identify high-risk users and behaviours and how to do so.
27. How to prioritise risks and threats based on analysis.
28. What are the strategies for minimising and eliminating cyber security insider risks and threats in an organisation.
29. What are the technology protocols used for user identification.
30. How to develop recommendations to minimise or eliminate insider risks and threats based on analysis findings.
31. How to seek and integrate feedback of required personnel on draft recommendations.
32. How to distribute information and documentation to required personnel in accordance with legislative requirements and organisational policies and procedures.
33. Why it is important to review identified cyber security insider risks and threats to identify training requirements and how to do so.
34. How to develop recommendations for training to address cyber security insider risks and threats.
35. How to seek feedback on training recommendations from required personnel.
36. How to finalise and distribute training recommendations in accordance with organisational policies and procedures.
37. How to recommend cyber security training in accordance with organisational procedures and industry best practices.

EVIDENCE GUIDE

For assessment purposes:

(1) Critical Aspects of Evidence

Candidates must prove that they can carry out **all** of the elements, meeting **all** the performance criteria, range and underpinning knowledge **on more than one occasion**. This evidence must come from a real work environment.

(2) Methods of Assessment

Assessors should gather a range of evidence that is valid, sufficient, current and authentic.

Evidence may be collected in a variety of ways including:

- Observation
- Written/oral questioning
- Written evidence
- Witness testimony
- Professional discussion
- Products of work

Questioning techniques should not require language, literacy or numeracy skills beyond those required in this unit of competency.

(3) Context of Assessment

This unit may be assessed on the job, off the job or a combination of both. Where assessment occurs off the job, that is the candidate is not in productive work, then an appropriate simulation must be used where the range of conditions reflects realistic workplace situations. The competencies covered by this unit would be demonstrated by a candidate working alone or as part of a team. The assessment environment should not disadvantage the candidate.

The candidate must have access to all tools, equipment, materials and documentation required. The candidate must be permitted to refer to any relevant workplace procedures, product and manufacturing specifications, codes, standards, manuals and reference materials.

Simulation **should not be used**, except in exceptional circumstances where natural work evidence is unlikely to occur.

UA39203 Work within in a team

Unit Descriptor:

This unit describes the knowledge, skills and attitudes required to work with others in a team and make a positive contribution to the effectiveness and efficiency of a teamwork environment.

ELEMENT	PERFORMANCE CRITERIA
Candidates must be able to:	
1. Contribute to team activities	1.1 Identify and confirm that team members know and understand their roles and responsibilities within the team.
	1.2 Participate in identifying and communicating team goals and objectives to ensure they align with those of the organisation.
	1.3 Confirm that activities are completed to the required standard and within agreed timeframes.
	1.4 Request assistance in the completion of tasks from other team members where appropriate.
	1.5 Support team members to ensure efficient and safe completion of tasks to the agreed standard.
	1.6 Encourage and acknowledge participation of team members to help the achievement of the team purpose.
	1.7 Implement changes in allocated role responsibilities as directed by team leader.
	1.8 Confirm that team meetings are attended as required in accordance with meeting **protocols**.
2. Share knowledge and information	2.1 Communicate information relevant to work with team members to enable efficient completion of tasks.

		2.2 Confirm that knowledge and skills are shared between team members to facilitate the completion of tasks and activities.
3.	Give and receive support	3.1 Provide **feedback** or assistance as required to other team members.
		3.2 Support team members in achieving organisational goals.
		3.3 Act upon **feedback** received from other team members to continue achieving workplace goals in accordance with organisational procedures.

RANGE STATEMENT

All range statements must be assessed:

1. **Protocols** may include but are not limited to:

    - Operational procedures and performance standards
    - Organisational personnel practices
    - Policies and procedures
    - Organisational quality standards

2. **Feedback** may include but are not limited to:

    - Oral
    - Written
    - Informal and formal
    - Descriptive
    - Peer and self-assessed

UNDERPINNING KNOWLEDGE AND SKILLS

Candidates must know and understand:

1. What is a team.
2. Why it is important to identify the roles and responsibilities of each team member and how to do so.
3. What are team goals and objectives.
4. Why it is important to identify team goals and objectives to ensure they align with those of the organisation and how to do so.
5. What is the organisation's mission statement.
6. How to effectively use interpersonal skills.
7. Why it is important to complete activities to the required standard and within agreed timeframes.
8. How to request assistance in the completion of tasks from other team members and when to do so.
9. What are the techniques for supporting others.
10. How to support team members to complete tasks efficiently and safely.
11. Why it is important to encourage and acknowledge participation by team members and how to do so.
12. How to implement changes in allocated role responsibilities.
13. Why it is important to confirm that team meetings are attended as required and in accordance with meeting protocols.
14. How to listen and use a variety of communication skills.
15. How to report information.
16. How to follow instructions.
17. How to communicate relevant information to team members.
18. Why it is important that knowledge and skills be shared between team members.
19. What are the techniques for providing feedback to team members in a constructive manner.
20. How to support team members in achieving workplace goals.
21. How to act upon feedback received from other team members.

EVIDENCE GUIDE

For assessment purposes:

(1) Critical Aspects of Evidence

Candidates must prove that they can carry out **all** of the elements, meeting **all** the performance criteria, range and underpinning knowledge. It is essential for this unit that competence be demonstrated in the effective communication and contribution to the achievement of tasks consistent with agreed goals.

Evidence will need to be gathered **over time in a variety of team situations** including regular work groups and occasional or one-off work groups.

(2) Method of Assessment

Assessors should gather a range of evidence that is valid, sufficient, current and authentic.

Evidence may be collected in a variety of ways:

- Oral questioning
- Observation
- Written evidence (case study, projects, assignments)
- Witness testimony
- Personal statement

Questioning techniques should not require language, literacy or numeracy skills beyond those required in this unit of competency.

(3) Context of Assessment

This unit may be assessed on the job, off the job or a combination of both. Where assessment occurs off the job, that is, the candidate is not in productive work, then an appropriate simulation must be used where the range of conditions reflects realistic workplace situations. The competencies covered by this unit would be demonstrated by an individual working alone or as part of a team. The assessment environment should not disadvantage the candidate.

The candidate must have access to all tools, equipment, materials and documentation required. The candidate must be permitted to refer to any relevant workplace procedures, product and manufacturing specifications, codes, standards, manuals and reference materials.

Simulation **should not be used**, except in exceptional circumstances where natural work evidence is unlikely to occur.

UA39303 Promote workplace cyber security awareness and best practices

Unit Descriptor: This unit describes the knowledge, skills and attitudes required to promote cyber security in a work area. It includes developing and reviewing cyber security awareness and supporting cyber security practices in the work area.

ELEMENT	PERFORMANCE CRITERIA
Candidates must be able to:	
1. Develop cyber security awareness in the work area	1.1 Establish the current level of awareness in the work area relating to cyber security.
	1.2 Participate in creating and maintaining a cyber security awareness programme that reflects established best practice.
	1.3 Contribute to developing organisational **cyber security policies and procedures** and communicate to **required personnel**.
2. Support effective cyber security practices in the work area	2.1 Review cyber security practices to ascertain their alignment with best practices and establish requirements for improvement.
	2.2 Participate in arranging training and information updates as required and maintain related records.
	2.3 Present insights from the review and training and potential related impact to **required personnel**.
3. Review cyber security awareness in the work area	3.1 Evaluate latest **cyber security threats** and trends impacting organisations.
	3.2 Document outcomes of the review and suggest improvements for consideration by **required personnel.**
	3.3 Communicate the review outcomes and cyber security improvement requirements according to organisational policies and procedures.

RANGE STATEMENT

All range statements must be assessed:

1. **Cyber security policies and procedures** may include but are not limited to:

    - Information security policy
    - Acceptable Use Policy (AUP)
    - Access control policy
    - Business continuity policy
    - Data breach response policy
    - Remote access policy
    - End user
    - Password policy

2. **Required personnel** may include but are not limited to:

    - End users
    - Information technology (IT) staff
    - Senior management
    - Senior cyber security information officer

3. **Cyber security threats** may include but are not limited to:

    - Intentional (e.g. malware, ransomware, phishing, malicious code)
    - Unintentional threats (e.g. forgetting to update antivirus software, unnecessary access to sensitive data, being unaware of threats)
    - Natural disasters (e.g. storms, flooding)

UNDERPINNING KNOWLEDGE AND SKILLS

Candidates must know and understand:

1. Why it is important to establish the current level of awareness in the work area relating to cyber security and how to do so.
2. What is an awareness programme.
3. How to participate in creating and maintaining a cyber security awareness programme that reflects organisation-wide best practice.
4. What are the organisation's cyber security policies and procedures.
5. How to contribute to developing and communicating cyber security policies and procedures to required personnel.
6. How to review cyber security practices to ascertain best practices and requirements for improvement.
7. How to participate in arranging training and information updates as required and maintaining related records.
8. How to present insights from the review and training and the potential related impact on the workplace to required personnel.
9. What are the current cyber security threats and trends impacting organisations.
10. How to review current cyber security threats and trends impacting organisations.
11. How to document the outcomes of a review and suggest improvements for consideration by required personnel.
12. How to communicate the review outcomes and cyber security improvement requirements according to organisational policies and procedures.

EVIDENCE GUIDE

For assessment purposes:

(1) Critical Aspects of Evidence

Candidates must prove that they can carry out **all** of the elements, meeting **all** the performance criteria, range and underpinning knowledge **on more than one occasion**. This evidence must come from a real work environment.

(2) Methods of Assessment

Assessors should gather a range of evidence that is valid, sufficient, current and authentic.

Evidence may be collected in a variety of ways including:

- Observation
- Written/oral questioning
- Written evidence
- Witness testimony
- Professional discussion
- Products of work

Questioning techniques should not require language, literacy or numeracy skills beyond those required in this unit of competency.

(3) Context of Assessment

This unit may be assessed on the job, off the job or a combination of both. Where assessment occurs off the job, that is the candidate is not in productive work, then an appropriate simulation must be used where the range of conditions reflects realistic workplace situations. The competencies covered by this unit would be demonstrated by a candidate working alone or as part of a team. The assessment environment should not disadvantage the candidate.

The candidate must have access to all tools, equipment, materials and documentation required. The candidate must be permitted to refer to any relevant workplace procedures, product and manufacturing specifications, codes, standards, manuals and reference materials.

Simulation **should not be used**, except in exceptional circumstances where natural work evidence is unlikely to occur.

UA39403 Protect against cyber security threats

Unit Descriptor:

This unit describes the knowledge, skills and attitudes required to contribute towards the cyber security resilience of an organisation. This includes the ability to protect against cyber security threats by following organisational policies and procedures that document the cyber security controls to be utilised.

ELEMENT	PERFORMANCE CRITERIA
Candidates must be able to:	
1. Establish cyber security policies and controls	1.1 Locate and review organisational or industry **cyber security policies** that must be complied with in the workplace.
	1.2 Identify the technical, administrative and physical **cyber security controls** implemented by the organisation that contribute to cyber security resilience.
	1.3 Maintain anti-malware protection to protect computer systems and data in line with organisational requirements.
	1.4 Identify **fraudulent communication attempts** and respond as appropriate in accordance with organisational data security and protection policy and procedures.
	1.5 Comply with organisational identity and access control policies and procedures across the organisation.
2. Secure sensitive data	2.1 Apply data encryption to secure sensitive data (at rest and in transit) in line with organisational standards.
	2.2 Select strong, unique passwords and preserve their non-disclosure in line with organisational password policies and procedures.

2.3 Implement appropriate multifactor authentication in accordance with organisational data security and protection policy and procedures.

2.4 Maintain software versions in accordance with organisational policies and standards.

2.5 Identify and remove software that is no longer supported or required.

2.6 Follow organisational standards for secure use of all devices in the work environment to maintain systems security.

2.7 Follow secure usage guidelines for unsecured USB ports and CD drives to prevent malicious or accidental transfer of malware to organisational systems and unauthorised extraction of data.

2.8 Maintain up to date cyber security awareness training in line with organisational requirements.

RANGE STATEMENT

All range statements must be assessed:

1. **Cyber security policies and procedures** may include but are not limited to:

   - Information security policy
   - Acceptable Use Policy (AUP)
   - Access control policy
   - Business continuity policy
   - Data breach response policy
   - Remote access policy
   - End user policy
   - Password policy

2. **Cyber security controls** may include but are not limited to:

   - Physical (preventative, detective, corrective)
   - Technical (preventative, detective, corrective)
   - Administrative (preventative, detective, corrective)

3. **Fraudulent communication attempts** may include but are not limited to:

   - Dumpster diving
   - Piggy backing
   - Tailgating
   - Phishing (emails, text, phone calls, social media messages, advertisements)

UNDERPINNING KNOWLEDGE AND SKILLS

Candidates must know and understand:

1. What are the main types of cyber security controls.
2. What are the main functions of cyber security controls.
3. Which cyber security controls are needed to protect the privacy, confidentiality, integrity and availability of data.
4. How to use cyber security controls to protect the privacy, confidentiality, integrity and availability of assets.
5. What are the organisational policies and procedures for cyber security.
6. How vulnerabilities can be remediated through technical, administrative and physical controls.
7. What are the different types of malicious communications and how do they occur.
8. Why it is important to know and understand phishing risks that can arise from communications.
9. What are the roles of identity and access controls in restricting admission of different levels of authorised users and in granting privileged operations.
10. How physical and environmental controls reduce the risk posed by threats within the physical environment, including natural or environmental hazards and physical intrusion by unauthorised individuals.
11. Why it is important that the organisation's computer network infrastructure is secured with appropriate technologies and processes.
12. Why it is important to identify and secure physical communication assets such as cabling, unsecured USB ports and CD read drives and how to do so.
13. Why passwords used across business and social domains should be discrete, strong and unique.
14. What are the different types of multifactor authentication (MFA) used in access control systems.
15. Why it is important to implement appropriate multifactor authentication in accordance with organisational data security and protection policies and procedures and how to do so.
16. What are the systems and procedures for encrypting sensitive data both in transit and at rest.
17. Why it is important to keep software versions up to date in line with organisational policies.
18. Why it is important to retire software that is no longer supported or required by the organisation and how to do so.
19. Why it is important to apply security controls across all devices whether fixed, mobile or from outside the organisation and how to do so.
20. Why it is important to keep up to date with training and to manage own learning whether prescribed by the organisation or self-directed and how to do so.

EVIDENCE GUIDE

For assessment purposes:

(1) Critical Aspects of Evidence

Candidates must prove that they can carry out **all** of the elements, meeting **all** the performance criteria, range and underpinning knowledge **on more than one occasion**. This evidence must come from a real work environment.

(2) Methods of Assessment

Assessors should gather a range of evidence that is valid, sufficient, current and authentic.

Evidence may be collected in a variety of ways including:

- Observation
- Written/oral questioning
- Written evidence
- Witness testimony
- Professional discussion
- Products of work

Questioning techniques should not require language, literacy or numeracy skills beyond those required in this unit of competency.

(3) Context of Assessment

This unit may be assessed on the job, off the job or a combination of both. Where assessment occurs off the job, that is the candidate is not in productive work, then an appropriate simulation must be used where the range of conditions reflects realistic workplace situations. The competencies covered by this unit would be demonstrated by a candidate working alone or as part of a team. The assessment environment should not disadvantage the candidate.

The candidate must have access to all tools, equipment, materials and documentation required. The candidate must be permitted to refer to any relevant workplace procedures, product and manufacturing specifications, codes, standards, manuals and reference materials.

Simulation **should not be used**, except in exceptional circumstances where natural work evidence is unlikely to occur.

UA41703 Manage safety and health in own area of responsibility

Unit Descriptor:

This unit describes the knowledge, skills and attitudes required to manage safety and health requirements in own area of responsibility. It details the outcomes required to evaluate responsibilities and liabilities, assess risks and communicate and monitor safety and health policies to comply with regulatory and organisational requirements for safety and health.

ELEMENT	PERFORMANCE CRITERIA
Candidates must be able to:	
1. Evaluate responsibilities and liabilities in relation to safety and health legislation and regulations	1.1 Assess personal responsibilities and liabilities under legislative and organisational **safety and health policies and procedures**.
	1.2 Identify and confirm with **key stakeholders**, organisational responsibilities under health and safety legislation.
	1.3 Identify and consult with relevant health and safety specialists when identified issues cannot be dealt with within own remit.
2. Assess and minimise safety and health risks in own area of responsibility	2.1 Confirm that the work environment and practices in own area of responsibility comply with organisational safety and health policy statements and are reviewed at regular intervals.
	2.2 Consult with persons in own area of responsibility or their representatives on safety and health issues in accordance with organisational and legislative **safety and health policies and procedures**.
	2.3 Confirm that a system is in place within the organisation for identifying health and safety hazards and assessing **risks** in own area of responsibility.

		2.4 Take action to eliminate and manage identified hazards and **risks** within the limits of own responsibility in accordance with organisational **safety and health policies and procedures.**
		2.5 Refer identified hazards and **risks** outside own scope of authority to appropriate persons in accordance with organisational **safety and health policies and procedures.**
		2.6 Confirm that sufficient resources are allocated across own area of responsibility to deal with safety, health and hygiene issues.
3.	Review health and safety policies in own area of responsibility	3.1 Confirm that the safety and health of persons and the security of resources and information are prime considerations when designing or reviewing the work environment and practices.
		3.2 Evaluate written **safety and health policies and procedures** against requirements for own area of responsibility.
4.	Monitor safety and health in own area of responsibility	4.1 Evaluate the effectiveness of systems used to identify and assess health and safety hazards and **risks** within own area of responsibility in accordance with organisational **safety and health policies and procedures.**
		4.2 Communicate and discuss written organisational **safety and health policies and procedures** with persons in own area of responsibility and other relevant parties and confirm understanding.
		4.3 Assess the work environment within own area of responsibility against organisational **safety and health policies and procedures**.
		4.4 Identify and report to **key stakeholders**, non-compliance with organisational **safety and health policies and policies** within own area of responsibility.

4.5 Identify and evaluate the safety and health requirements in project or operational plans within own area of responsibility to ensure compliance with legislative and organisational **safety and health policies and procedures**.

RANGE STATEMENT

All range statements must be assessed:

1. **Safety and health policies and procedures** may include but are not limited to:

    - Safe work techniques
    - Safe work environment
    - Emergency, fire and accident
    - Security of documents, cash, equipment, people
    - Hygiene practices

2. **Risks** may include but are not limited to:

    - Use and maintenance of equipment and materials
    - Poor working practices
    - Unsafe behaviour
    - Ill health issues
    - Condition of workplace

3. **Key stakeholders** may include but are not limited to:

    - Senior management
    - Person responsible for organisational health and safety policy and implementation
    - Staff
    - Customers

UNDERPINNING KNOWLEDGE AND SKILLS

Candidates must know and understand:

1. Why it is important to evaluate personal responsibilities and liabilities under safety and health legislation and the organisational safety and health policies and procedures and how to do so.
2. What are the organisation's responsibilities under health and safety legislation.
3. What are the types of health and safety specialists within the organisation and industry.
4. Why it is important to identify and consult with a health and safety specialist when identified issues are outside own remit and what are the organisational procedures for doing so.
5. How to confirm with key stakeholders that the work environment and practices in own area of responsibility comply with organisational safety and health policy statements and are reviewed at regular intervals.
6. Why it is important to consult regularly with persons in own area of responsibility or their representatives on safety and health issues and what are the requirements for doing so.
7. What systems are in place within the organisation for identifying hazards and assessing risks and how to use them.
8. What action can be taken within the limits of own responsibility to eliminate and manage identified hazards and risks and what are the organisational safety and health policies and procedures for doing so.
9. What are the types of hazards and risks that may arise in the workplace in relation to safety and health.
10. How to refer identified hazards and risks outside own scope of authority to the appropriate person and what are the organisational safety and health policies and procedures for doing so.
11. Why it is important to make the safety and health of persons and the security of resources and information prime considerations when designing or reviewing working environments and practices and how to do so.
12. What are the resources required to deal with safety, health and hygiene issues.
13. How to allocate sufficient resources across own area of responsibility to deal with safety, health and hygiene issues.
14. How to review written safety and health policies against the requirements for own area of responsibility.
15. How to communicate recommendations for changes to safety and health policies to individuals within own area of responsibility and what are the organisational requirements for doing so.
16. Why it is important to share and discuss written safety and health policies to persons in own area of responsibility and other relevant parties and confirm understanding.
17. How to evaluate systems for identifying and assessing health and safety hazards and risks within own area of responsibility.

18. How to assess the work environment within own area of responsibility against organisational safety and health policies and procedures.
19. How to identify and report non-compliance with organisational safety and health policies and practices within own area of responsibility to key stakeholders.
20. How to identify and evaluate the safety and health requirements in project or operational plans within own area of responsibility to ensure compliance to legislative and organisational safety and health policies and procedures.

EVIDENCE GUIDE

For assessment purposes:

(1) Critical Aspects of Evidence

Candidates must prove that they can carry out **all** of the elements, meeting **all** the performance criteria, range and underpinning knowledge **on more than one occasion**. This evidence must come from a real work environment.

(2) Methods of Assessment

Assessors should gather a range of evidence that is valid, sufficient, current and authentic.

Evidence may be collected in a variety of ways including:

- Observation
- Written/oral questioning
- Case study
- Personal statement
- Witness testimony
- Professional discussion
- Products of work

Questioning techniques should not require language, literacy or numeracy skills beyond those required in this unit of competency.

(3) Context of Assessment

This unit may be assessed on the job, off the job or a combination of both. Where assessment occurs off the job, that is the candidate is not in productive work, then an appropriate simulation must be used where the range of conditions reflects realistic workplace situations. The competencies covered by this unit would be demonstrated by a candidate working alone or as part of a team. The assessment environment should not disadvantage the candidate.

The candidate must have access to all tools, equipment, materials and documentation required. The candidate must be permitted to refer to any relevant workplace procedures, product and manufacturing specifications, codes, standards, manuals and reference materials.

Simulation **should not be used**, except in exceptional circumstances where natural work evidence is unlikely to occur.

UA39503 Contribute to the protection of the cyber security environment

Unit Descriptor: This unit deals with the knowledge, skills and attitudes required to conduct work activities in a manner that protects the environment. Candidates should take steps to minimise any negative impact on the environment by completing tasks and activities in a way which causes as little damage or disturbance as possible to the environment while following organisational procedures.

ELEMENT	PERFORMANCE CRITERIA
Candidates must be able to:	
1. Work in an environmentally conscious way	1.1 Perform duties in accordance with **relevant policies and legislation**.
	1.2 Execute duties in a **manner which minimises environmental damage**.
	1.3 Operate and handle **equipment** and **materials** in a **manner that minimises environmental damage**.
2. Contribute to continuous improvements in protecting the environment	2.1 Identify instances of likely or actual environmental damage and take appropriate action.
	2.2 Identify improvements to procedures and practices in terms of good environmental practice and report to relevant persons.
	2.3 Dispose of **hazardous** and **non-hazardous waste** according to approved legislative procedures and practices.
	2.4 Contribute to sustainable development particularly in the conservation of energy, water, use of resources and equipment to minimise environmental damage.

RANGE STATEMENT

All range statements must be assessed:

1. **Relevant policies and legislation** may include but not limited to:

    - Organisational policies
    - Health and safety at work
    - Environmental legislation

2. **Manner which minimises environmental damage** may include but not limited to:

    - Using recycled/reused items and materials where appropriate
    - Disposing of polluting substances safely
    - Reducing the volume of waste
    - Using biodegradable and eco-friendly chemicals
    - Planning tasks to reduce the use of fuel and electricity

3. **Equipment and materials** may include but not limited to:

    - Tools
    - Personal protective equipment
    - Cleaning chemicals

4. **Hazardous waste** may include but not limited to:

    - Oils
    - Chemicals and solutions
    - Harmful materials (asbestos, fibreglass)
    - Electronic equipment

5. **Non-hazardous waste:**

    - Food
    - Plant matter
    - Paper

UNDERPINNING KNOWLEDGE AND SKILLS

You need to know and understand:

1. What are the relevant policies and legislation governing environmental protection.
2. How to identify any likely or actual environmental damage.
3. What are the appropriate actions to take in the discovery of likely or actual environmental damage.
4. What are the ways in which tools and materials should be used to minimise environmental damage.
5. What are the different types of pollution.
6. What are the consequences of pollution.
7. How to identify wastage of energy, water, equipment and materials.
8. What are the methods of working that will minimise pollution and wastage of resources.
9. What are the types of damage which may occur, the impact these can have on the environment and corrective actions to be taken.
10. What are the methods of waste disposal which will minimise the risk to the environment.
11. What are the organisational requirements to prevent wastage.

EVIDENCE GUIDE

For assessment purposes:

(1) Critical Aspects of Evidence

Candidates must prove that they can carry out **all** the elements, meeting **all** of the performance criteria, range and underpinning knowledge **on no less than three (3) occasions**. This evidence must come from a real working environment.

(2) Methods of Assessment

Assessors should gather a range of evidence that is valid, sufficient, current and authentic.

Evidence may be collected in a variety of ways including:

- Observation
- Written/oral questioning
- Witness testimony
- Personal statement
- Written evidence (projects or assignments)
- Case study and scenario analysis
- Role play/simulation

(3) Context of Assessment

This unit may be assessed on the job, off the job or using a combination of both. Where assessment occurs off the job, that is, the candidate is not in productive work, then an appropriate simulation must be used where the range of conditions reflects realistic workplace situations. The competencies covered by this unit would be demonstrated by a candidate working alone or as part of a team. The assessment environment should not disadvantage the candidate.

The candidate must have access to all tools, equipment, materials and documentation required. The candidate must be permitted to refer to any relevant workplace procedures, products and manufacturing specifications, codes, standards, manuals and reference materials.

Simulation **must not be used**, except in exceptional circumstances where natural work evidence is unlikely to occur.

U65403 Maintain and improve personal performance

Unit Descriptor:

This unit describes the knowledge, skills and attitudes required to perform the personal and organisational aspects of your role. Candidates are required to show how to plan, prioritise and organise work effectively, as well as demonstrate how to work effectively with others by offering assistance, resolving difficulties and meeting deadlines. Candidates are also required to demonstrate personal development through learning and acquiring new skills.

ELEMENT	PERFORMANCE CRITERIA
Candidates must be able to:	
1. Plan and organise work	1.1 Identify and prioritise **tasks** according to organisational procedures and regulatory requirements.
	1.2 Identify changes in priorities and adapt work plans and resource allocations accordingly.
	1.3 Use appropriate **planning aids** to plan and monitor work progress.
	1.4 Identify, negotiate and coordinate appropriate and relevant assistance to meet specific demands and deadlines.
	1.5 Report anticipated difficulties in meeting deadlines to the **appropriate person**.
	1.6 Check conformation of work methods with legal and regulatory requirements.
2. Maintain working relationships	2.1 **Communicate** in accordance with organisational procedures.
	2.2 Discuss and agree on realistic objectives, resources, working methods and schedules with others in a way that promotes good working relationships.
	2.3 Meet commitments to colleagues within agreed timescales.

	2.4 Offer assistance and support within own work constraints and commitments where colleagues cannot meet deadlines.
	2.5 Find workable solutions for any conflicts and dissatisfaction which reduce personal and team effectiveness.
	2.6 Refer any difficulties in working relationships which are beyond the scope of own authority to **appropriate persons** in accordance with organisational procedures.
	2.7 Treat others in a courteous manner and perform work in a way that shows respect for others.
	2.8 Maintain strict confidentiality of information relating to colleagues and data protection requirements in accordance with organisational procedures.
3. Improve own performance	3.1 Consider current work activities and career goals to **identify own development needs**.
	3.2 Define and agree on development objectives with **appropriate persons**.
	3.3 Research appropriate ways of acquiring new skills and knowledge.
	3.4 Seek resources and support from relevant persons to ensure that development opportunities are realistic and achievable.
	3.5 **Review and evaluate performance and progress** to agreed timescales.
	3.6 Develop and maintain specialist knowledge relevant to own working environment.
	3.7 Monitor understanding of developments relating to own job role.
	3.8 Undertake learning opportunities to assist in improving own performance.

RANGE STATEMENT

All range statements must be assessed:

1. **Tasks** may include but are not limited to:

   - Routine
   - Unexpected

2. **Planning aids** may include but are not limited to:

   - Diaries
   - Schedules
   - Action plans

3. **Appropriate persons** may include but are not limited to:

   - Line manager
   - Project manager
   - Colleagues

4. **Communicate** may include but are not limited to:

   - Face to face
   - By telephone
   - By fax
   - By email
   - In writing

5. **Identify own development needs** may include but are not limited to:

   - Training
   - Discussions with supervisor/line manager/HR personnel

6. **Review and evaluate performance and progress** may include but are not limited to:

   - Alone
   - In conjunction with others

UNDERPINNING KNOWLEDGE AND SKILLS

Candidates must know and understand:

1. What are the work methods and practices in the organisation.
2. How to handle confidential information.
3. How to establish constructive relationships.
4. Why it is important to integrate own work with that of other persons.
5. What are the ways of identifying development needs.
6. How self-development objectives are set.
7. What are development opportunities and their resource implications.
8. What are the ways of assessing own performance and progress.
9. How to maintain good working relationships, even when disagreeing with others.
10. What are the scope and limit of own authority for taking corrective action.
11. How to use different styles of approach in different circumstances.
12. How to set targets, prioritise and organise work and inform and consult with others about work methods.
13. How to use scheduling techniques and aids and plan work.
14. How to manage time, deadlines and timescales, work as a team and seek and exchange information, advice and support.
15. How to handle disagreements and conflict and what procedures exist to deal with conflict and poor working relationships.
16. How to show commitment and motivation towards own work.
17. How to deal with changed priorities and unforeseen situations.
18. How to negotiate the assistance of others.
19. How to coordinate resources and tasks.
20. What are the organisational and departmental structures.
21. What are your own and colleagues' work roles and responsibilities.
22. What are the organisational reporting procedures.
23. Where to access information that will assist in learning, including formal training courses.
24. Who are the persons able to assist with planning and implementing own required learning.

EVIDENCE GUIDE

For assessment purposes:

(1) Critical Aspects of Evidence

Candidates must prove that they can carry out **all** the elements, meeting **all** of the performance criteria, range and underpinning knowledge **on more than one occasion.** This evidence must come from a real working environment.

(2) Methods of Assessment

Assessors should gather a range of evidence that is valid, sufficient, current and authentic.

Evidence may be collected in a variety of ways including:

- Observation
- Written/oral questioning
- Witness testimony
- Written evidence (work records, reports)
- Simulations

(3) Context of Assessment

This unit may be assessed on the job, off the job or a combination of both. Where assessment occurs off the job, that is, the candidate is not in productive work, then an appropriate simulation must be used where the range of conditions reflects realistic workplace situations. The competencies covered by this unit would be demonstrated by a candidate working alone or as part of a team. The assessment environment should not disadvantage the candidate.

The candidate must have access to all tools, equipment, materials and documentation required. The candidate must be permitted to refer to any relevant workplace procedures, products and manufacturing specifications, codes, standards, manuals and reference materials.

Simulation **may be used**.

U78103 Communicate to develop and maintain networks and relationships

Unit Descriptor:

This unit deals with the knowledge, skills and attitudes required to collect, analyse and communicate information and to use that information to develop and maintain effective working relationships and networks. The unit emphasises communication and representation.

ELEMENT	PERFORMANCE CRITERIA
Candidates must be able to:	
1. Communicate ideas and information	1.1 Collect relevant information from appropriate sources and analyse and share with colleagues to improve performance.
	1.2 **Communicate** ideas and information in a manner appropriate to the recipient and specific needs.
	1.3 Exchange **information** and resources with colleagues to make sure that all parties can work in an effective manner.
	1.4 Implement **consultation processes** to encourage colleagues to contribute to issues related to their work and relay feedback to the team with regards to outcomes.
	1.5 Implement **processes** to ensure that issues raised are referred to **relevant personnel** as required.
2. Develop trust and confidence	2.1 Identify, agree on and respect the roles and responsibilities of colleagues.
	2.2 Obtain and maintain the trust and confidence of colleagues through competent performance.
	2.3 Fulfil and **communicate** agreements made with colleagues.
	2.4 Advise colleagues of difficulties and where agreements cannot be fulfilled in accordance with organisational procedures.

3. Develop and maintain networks and relationships	3.1 Establish working relationships with persons relevant to the work being carried out.
	3.2 Use **networks** to identify and build relationships.
4. Manage difficulties into positive outcomes	4.1 Identify and analyse difficulties, conflicts of interest and disagreements and take action to resolve the situation in ways that minimise damage to the work being carried out.
	4.2 Provide feedback to colleagues on their performance and solicit feedback from colleagues on own performance to identify areas for improvement.
	4.3 Guide and support colleagues to resolve work difficulties.
	4.4 Review and improve **workplace outcomes** in consultation with **relevant personnel**.

RANGE STATEMENT

All range statements must be assessed:

1. **Communicate** may include but not limited to:

    - Written
    - Verbal
    - Non-verbal

2. **Information** may include but not limited to:

    - Data appropriate to work roles and organisational policies that is shared and retrieved in writing or verbally, electronically or manually such as:

        - archived, filed and historical background data
        - individual and team performance data
        - marketing and customer related data
        - planning and organisational documents, including the outcomes of continuous improvement and quality assurance
        - policies and procedures

3. **Consultation processes** may include but not limited to:

    - Feedback to the work team and relevant personnel in relation to outcomes of the consultation process
    - Opportunities for all employees to contribute to ideas and information about organisational issues

4. **Processes** may include but not limited to:

    - Conducting informal meetings
    - Coordinating surveys or questionnaires
    - Distributing newsletters or reports
    - Exchanging informal dialogue with relevant personnel

5. **Relevant personnel** may include but not limited to:

    - Managers
    - Occupational health and safety committee and other people with specialist responsibilities
    - Other employees
    - Supervisors

6. **Networks** may include but not limited to:

    - Established structures or unstructured arrangements and may include business or professional associations
    - Informal or formal and with individuals or groups
    - Internal and/or external

7. **Workplace outcomes** may include but not limited to:

    - Occupational health and safety processes and procedures
    - Performance of the work team

UNDERPINNING KNOWLEDGE AND SKILLS

Candidates must know and understand:

1. How to use coaching and mentoring skills to provide support to colleagues.
2. What information should be collected and how to analyse and share this information.
3. What are the methods of communication in regard to the recipient.
4. What consultation methods can be used within the team.
5. How to network to identify and build relationships.
6. How to identify and analyse conflicts of interest and disagreements.
7. How to provide constructive feedback.
8. What methods can be used to provide guidance and support to colleagues.
9. What literacy skills are required to research, analyse, interpret and report information.
10. What relationship, management and communication skills are required to:
    - deal with people openly and fairly
    - forge effective relationships with internal and/or external persons and develop and maintain these networks
    - gain the trust and confidence of colleagues
    - respond to unexpected demands from a range of people
    - utilise supportive and consultative processes effectively
    - demonstrate respect for colleagues and their work
11. What is the relevant legislation and industry practice that affects business operations, especially with regards to occupational health and safety (OHS), environmental issues, industrial relations and anti-discrimination.
12. What theories are associated with managing work relationships to achieve planned outcomes:
    - developing trust and confidence
    - maintaining fair and consistent behaviour in work relationships
    - understanding the cultural and social environment
    - identifying and assessing interpersonal styles
    - establishing, building and maintaining networks
    - identifying and resolving problems
    - resolving conflict
    - managing poor work performance
    - monitoring, analysing and introducing ways to improve work relationships.

EVIDENCE GUIDE

For assessment purposes:

(1) Critical Aspects of Evidence

Candidates must prove that they can carry out **all** the elements, meeting **all** of the performance criteria, range and underpinning knowledge **on more than one occasion.** This evidence must come from a real working environment.

(2) Methods of Assessment

Assessors should gather a range of evidence that is valid, sufficient, current and authentic.

Evidence may be collected in a variety of ways including:

- Observation
- Written/oral questioning
- Written evidence
- Witness testimony
- Professional discussion

Questioning techniques should not require language, literacy or numeracy skills beyond those required in this unit of competency.

(3) Context of Assessment

This unit may be assessed on the job, off the job or a combination of both. Where assessment occurs off the job, that is the candidate is not in productive work, then an appropriate simulation must be used where the range of conditions reflects realistic workplace situations. The competencies covered by this unit would be demonstrated by a candidate working alone or as part of a team. The assessment environment should not disadvantage the candidate.

The candidate must have access to all tools, equipment, materials and documentation required. The candidate must be permitted to refer to any relevant workplace procedures, products and manufacturing specifications, codes, standards, manuals and reference materials.

Simulation **should not be used**, except in exceptional circumstances where natural work evidence is unlikely to occur.

Level 3 Glossary of Terms

Assessment methods

The methods which can be used to determine competence in performance and underpinning knowledge.

Assessors

The Assessor's role is to determine whether evidence presented by a candidate for assessment within the programme meets the required standard of competence in the relevant unit or element. The Assessor needs to be competent to assess to national standards in the area under assessment.

Approved Centre

Organisation/Centre approved by the TVET Council to offer full National Vocational Qualifications.

Case Studies

In situations where it is difficult for workplace assessment to take place, case studies can offer the candidate an opportunity to demonstrate potential competence.

A case study is a description of an actual or imaginary situation presented in some detail. The way the case study is presented will vary depending upon the qualification, but the most usual methods are written, taped or filmed.

The main advantage of a case study is the amount of evidence of underpinning knowledge they can generate and the specific nature of the evidence produced.

Competence

In the context of vocational qualifications, competence means: the ability to carry out prescribed activities to nationally pre-determined standards in an occupation. The definition embraces cognitive, practical and behavioural skills, underpinning knowledge and understanding and the ability to react appropriately in contingency situations.

Element

An element is a description of an activity which a person should be able to do. It is a description of an action, behaviour or outcome which a person should be able to demonstrate.

Explanation of NVQ Levels

NVQs cover five (5) levels of competence, from entry level staff at Level 1 through to senior management at Level 5.

Appendix 2

Level 3 Glossary of Terms

Level 1 - Entry Level

Recognises competence in a range of varied work activities performed in a variety of contexts. Most work activities are simple and routine. Collaboration with others through work groups or teams may often be a requirement. Substantial supervision is required especially during the early months evolving into more autonomy with time.

Level 2 - Skilled Occupations:

Recognises competence in a broad range of diverse work activities performed in a variety of contexts. Some of these may be complex and non-routine and involve some responsibility and autonomy. Collaboration with others through work groups or teams and guidance of others may be required.

Level 3 - Technician and Supervisory Occupations:

Recognises competence in a broad range of complex, technical or professional work activities performed in a wide variety of contexts, with a substantial degree of personal responsibility and autonomy. Responsibility for the work of others and the allocation of resources are often a requirement. The individual is capable of self-directed application, exhibits problem solving, planning, designing and supervisory capabilities.

Level 4 - Technical Specialist and Middle Management Occupations:

Recognises competence involving the application of a range of fundamental principles and complex techniques across a wide and unpredictable variety of contexts. Requires very substantial personal autonomy and often significant responsibility for the work of others, the allocation of resources, as well as personal accountability for analysis, diagnosis, design, planning, execution and evaluation.

Level 5 - Chartered, Professional and Senior Management Occupations:

Recognises the ability to exercise personal professional responsibility for the design, development or improvement of a product, process, system or service. Recognises technical and management competencies at the highest level and includes those who have occupied positions of the highest responsibility and made outstanding contribution to the promotion and practice of their occupation.

External Verifier

The External Verifier is trained and appointed by the TVET Council and is competent to approve and ensure an approved Centre's quality of provision.

Internal Verifier

The Internal Verifier acts in a supporting role for Assessors to ensure consistent quality of assessment and competence. They need to be competent to assess to national standards in the area under assessment.

Appendix 2

Level 3 Glossary of Terms

VQ

National Vocational Qualifications (NVQs) are work-based qualifications that assess an individual's competence in a work situation and certify that the individual can perform the work role to the standards expected in employment.

NVQs are based on national occupational standards of competence drawn up by standards-setting bodies known as Industry Lead Bodies. The standards describe the level and breadth of performance that is expected of persons working in the industry or sector which the NVQ covers.

NVQ Coordinator

Within each approved Centre offering NVQs, there is a centre contact who has overall responsibility for the operation and administration of the NVQ system.

Observation

Observation of the candidate carrying out his/her job in the workplace is the assessment method recommended in the vast majority of units and elements. Observation of staff carrying out their duties is something that most supervisors and managers do every day.

Performance criteria

Performance criteria indicate what is required for the successful achievement of an element. They are descriptions of what you would expect to see in competent performance.

Product of Work

This could be items produced during the normal course of work which can be used for evidence purposes such as reports, menus, promotional literature, training plans, etc.

Questioning

Questioning is one of the most appropriate ways to collect evidence to assess a candidate's underpinning knowledge and understanding.

Questioning can also be used to assess a candidate in those areas of work listed in the range which cannot be assessed by observation. Guidance on when this assessment method can be used is given in the assessment guidance of each individual element.

As an assessment method, questioning ensures you have all of the evidence about a candidate's performance. It also allows you to clarify situations.

Appendix 2

Level 3 Glossary of Terms

Range statements

The range puts the element of competence into context. A range statement is a description of the range of situations to which an element and its performance criteria is intended to apply.

Range statements are prescriptive; therefore each category must be assessed.

Role-plays

Role-plays are simulations where the candidate is asked to act out a situation in the way he/she considers "real" people would behave. By using role-play situations to assess a candidate you are able to collect evidence and make a judgment about how the candidate is most likely to perform. This may be necessary if the range specified includes a situation in which the candidate is unlikely to find himself/herself in the normal course of their work, or where the candidate needs to develop competence before being judged competently, for example, in a disciplinary situation,

Simulations

Where possible, assessment should always be carried out by observing **natural performance** in the workplace. **Simulated performance,** however, can be used where specified to collect evidence about an aspect of the candidate's work which occurs infrequently or is potentially hazardous, for example, dealing with fires.

By designing the simulated situation, briefing the candidate and observing his/her performance, you will be able to elicit evidence which will help you judge how a candidate is **most likely** to perform in real life.

Supplementary evidence

Supplementary evidence can be used to confirm and support performance evidence. Types of supplementary evidence include witness testimonies, reports, journals or diaries, records of activities, personal statements, simulation (see note in glossary).

Underpinning knowledge

Underpinning knowledge indicates what knowledge is <u>essential</u> for a person to possess in order to successfully achieve an element and prove total competence.

Units

A unit of competence describes one or more activities which form a significant part of an individual's work. Units are accredited separately but in combination can make up a vocational qualification. There are three categories of units:

Appendix 2

Level 3 Glossary of Terms

Mandatory units - are core to a qualification and must be completed.

Optional units - candidates must choose the required number of individual units, specified in the qualification structure, to achieve the qualification.

Work-based projects

Work-based projects are a useful way for you to collect evidence to support any decision you make about a candidate's performance. They are particularly appropriate in determining the level of a candidate's underpinning knowledge and understanding where it may be insufficient to rely only on questioning observation.

A project often involves the identification of a solution to a specific problem identified by you and/or the candidate (such as looking at ways to redress a recent drop in sales), or may be a structured programme of work built around a central situation or idea (such as the introduction of a new job rostering process).