**900103-000-00-KM-01, Cyber Defence Introduction, NQF Level 4, Credits 7**

**SUMMATIVE ASSESSMENT MEMO**

**MODULE ONE (1)**

|  |  |
| --- | --- |
| **Module #** | 900103-000-00-KM-01 |
| **NQF Level** | 4 |
| **Notional hours** | 70 |
| **Credit(s)** | 7 |
| **Occupational Code** | 900103-000-00-00 |
| **SAQA QUAL ID** | SP - 220330 |
| **Qualification Title** | Cybersecurity Defender |

|  |  |
| --- | --- |
| **Name** |  |
| **Contact Address** |  |
| **Telephone (H)** |  |
| **Telephone (W)** |  |
| **Facsimile** |  |
| **Cellular** |  |
| **E-mail** |  |

**Note to the learner**

This Learner Guide provides a comprehensive overview of the module. It is designed to improve the skills and knowledge of learners, and thus enabling them to effectively and efficiently complete specific tasks.

**Purpose of the Module**

The main focus of the learning in this knowledge module is to build an understanding of the basics of cybersecurity including definitions, concepts, terminology and the adverse effect of cyber vulnerabilities on the safety and security of company information, data and systems. They will also understand the importance of a safe cybersecurity and threat posture of a company

The learning will enable learners to demonstrate an understanding of:

* KM-01-KT01 : Introduction to cybersecurity 30%
* KM-01-KT02 : Cybersecurity basics 20%
* KM-01-KT03 : Cybersecurity governance fundamentals 20%
* KM-01-KT04 : A cyber secure organisation 15%
* KM-01-KT05 : Basics of threat intelligence 15%

**Entry Requirements**

NQF 3 (Gr 11) with Computer Literacy, English and Math Lit

**Provider Accreditation Requirements for the Knowledge Module**

*Physical Requirements:*

* The provider must have lesson plans and structured learning material or provide learners with access to structured learning material that addresses all the topics in all the knowledge modules as well as the applied knowledge in the application modules
* QCTO/ MICT SETA requirements

*Human Resource Requirements:*

* Lecturer/learner ratio of 1:20 (Maximum)
* Qualification of lecturer (SME):

NQF 5 qualified in industry recognised qualifications with 1 years’ experience in the IT industry

Cybersecurity vendor certification

* Assessors and moderators: accredited by the MICT SETA

*Legal Requirements:*

* Legal (product) licences to use the software for learning and training
* OHS compliance certificate
* Ethical clearance (where necessary)

AM

*Physical Requirements:*

* Valid licenses software and application, including OS.
* Internet connection and hardware availability.
* Examples and information specified in the scope statement and all the case studies, scenarios and access to hardware and software implied in the scope statements of the modules.
* Remote learners: Provider must provide business IT simulation system (e.g. invoice processing).

*Human Resource Requirements:*

* Qualification of lecturer (SME):  
  o NQF 5 industry recognised qualification with 1 year relevant experience
* Assessors and moderators: accredited by the MICT SETA

*Legal Requirements:*

* + Legal (product) licences to use the software for learning and training
  + OHS compliance certificate
  + Ethical clearance (where necessary)

**Venue, Date and Time:**

Consult your facilitator should there be any changes to the venue, date and/or time.

Refer to your timetable.

**Assessments**

**Associated Assessment Criteria (AACs)**

* Basic governance principles and concepts related to cybersecurity are understood.
* Basic concepts and principles of cybersecurity are understood.
* Basic concepts and principles of cyber threats and attacks are understood.
* Basic concepts and principles of cyber defence are understood.
* Ethical considerations in ethical hacking and penetration testing are understood.
* Procedures to respond to cybersecurity incidents are understood.

**Associated Assessment Criteria (AACs)**

* User and host identities are verified.
* Mechanisms are put in place to prevent system intrusions.
* Automated tools are used to guard against intrusions.
* Network confidentiality is ensured.
* The security posture is evaluated to detect vulnerabilities and to enhance resilience.

**Associated Assessment Criteria (AACs)**

* Threats to the cybersecurity of the company are detected.
* Adversary techniques, tactics and practices (TTPs) are emulated
* using an emulation platform.
* Network traffic is monitored and analysed using a suitable platform.
* Incidents are identified, responded to and reported.

**Associated Assessment Criteria (AACs)**

* Foot-printing tools are used against a target and intelligence is gathered.
* Vulnerabilities are identified using penetration testing tools.
* Servers and devices are attacked to build better defences.
* Clients are manipulated to uncover internal threats.
* Targets are exploited to increase cybersecurity.

Antivirus and intruder detection systems (IDS) are tested

# PURPOSE OF THE QUALIFICATION

Cybersecurity Defenders are responsible for proactively protecting organisations’ systems from attacks, they are the first line of defence against cyberattacks, the first responders to cybersecurity breaches and are responsible for the hardening of the information systems of organisations ensuring compliance with legislation

# QUALIFICATION RULES

This Skills Programme consist of two components namely Knowledge/Theory component and Application component. The following are compulsory modules in each of the two components:

**Knowledge/Theory Component:**

The following Modules are compulsory:

* 900103-000-00-KM-01, Cyber Defence Introduction, NQF Level 4, Credits 7
* 900103-000-00-KM-02, Cyber Threats and Attacks, NQF Level 4, Credits 7
* 900103-000-00-KM-03, Cybersecurity, NQF Level 4, Credits 7
* 900103-000-00-KM-04, Responding to Cybersecurity Incidents, NQF Level 4, Credits 5

Total number of credits for Knowledge Component: 26

**Application Component:**

* 900103-000-00-PM-01, Protect against cybersecurity threats, intrusions and attacks, NQF Level 4, Credits 11
* 900103-000-00-PM-02, Detect cybersecurity threats, intrusions and attacks, NQF Level 4, Credits 11
* 900103-000-00-PM-03, Conduct Penetration Testing Techniques to Determine Security, NQF Level 4, Credits 12

Total number of credits for Application Component: 34

# EXIT LEVEL OUTCOMES

**Exit Level Outcomes (ELO) 1**

Demonstrate knowledge and understanding of cybersecurity, cyber

threats and attacks and cyber defence

**Exit Level Outcomes (ELO) 2**

Protect against cybersecurity intrusions and attacks

**Exit Level Outcomes (ELO) 3**

Detect cybersecurity threats and attacks

**Exit Level Outcomes (ELO) 4**

Use different penetration testing tools to identify vulnerabilities in the security posture of an organisation

# KM-01-KT01: Introduction to cybersecurity 30%

1. **IAC0103 Analyse the impact of cyberattacks, incidents and data breaches on companies.**
2. **Cyberattacks**:

Cyberattacks are deliberate, malicious actions taken by individuals or groups to exploit vulnerabilities in computer systems, networks, or digital devices. The objective of a cyberattack is to compromise the security of the target and cause harm or gain unauthorized access to sensitive information. Cyberattacks can take various forms and may include:

* **Malware**: The deployment of malicious software, such as viruses, worms, Trojans, ransomware, or spyware, to disrupt, steal data, or gain unauthorized access.
* **Phishing**: The use of deceptive emails, messages, or websites to trick individuals into revealing sensitive information, such as login credentials or financial details.

1. **IAC0104 Give reasons for attacking specific targets.**

Cyberattacks can target various entities, including individuals, groups, organizations, and governments. The motives behind cyberattacks can vary widely, ranging from financial gain and data theft to political activism and espionage. Here's how each of these entities can be the target of cyberattacks:

1. **Individuals**: Individual users are often targeted through techniques like phishing, social engineering, or the use of malicious software (malware). Cybercriminals may try to steal personal information, financial data, login credentials, or even gain access to personal devices and accounts.
2. **Groups and Organizations**: Businesses, non-profit organizations, and other groups can be targets of cyberattacks. These attacks can aim to steal sensitive business data, disrupt operations, extort money through ransomware attacks, or gain a competitive advantage through corporate espionage.

# KM-01-KT02 : Cybersecurity basics 20%

1. **IAC0201 Discuss the cybersecurity as an escalating global pandemic.**

Cyber threats are potential risks or vulnerabilities that exist in computer systems, networks, or digital environments. When these threats are exploited or leveraged by malicious actors, they materialize into cyber attacks. In other words, an attack occurs when a threat is realized and exploited by an individual, group, or automated system with malicious intent.

For example, a common threat is the existence of a software vulnerability, such as an unpatched security flaw in a web application. If a hacker identifies this vulnerability and uses it to gain unauthorized access to the application or compromise its data, it becomes a cyber attack. The hacker exploits the existing threat (the unpatched vulnerability) to launch the attack.

Threats can come from various sources, including external attackers, insiders (such as disgruntled employees or contractors), or even accidental actions by users. Different cyber attack techniques are used to exploit different types of threats, aiming to achieve specific objectives such as data theft, service disruption, financial gain, or espionage.

# KM-01-KT03 : Cybersecurity governance fundamentals 20%

1. **IAC0301 Describe the compliance with legislation.**

As of my last update in September 2021, there is no specific "Cybercrimes Act" that applies universally across all countries. However, many countries have enacted laws and regulations that address cybercrimes and cybersecurity issues. These laws are designed to combat various forms of cybercriminal activities and protect individuals, organizations, and governments from cyber threats.

The content and scope of cybercrime legislation can vary significantly from one country to another, but some common elements found in such laws include:

1. **Definition of Cybercrimes**: Cybercrime laws typically define various cyber offenses, such as unauthorized access to computer systems, data theft, hacking, identity theft, online fraud, cyberbullying, distribution of malicious software, and denial-of-service attacks.
2. **Penalties and Punishments**: Cybercrime laws prescribe penalties and punishments for offenders found guilty of committing cybercrimes. These penalties may include fines, imprisonment, asset forfeiture, or other appropriate legal actions.
3. **IAC0302 Describe the aim and function of various governance tools.**

A cyber security policy is a fundamental and essential document that serves as the foundation of protection for an organization's digital assets, data, systems, and networks. It outlines the guidelines, principles, and rules that govern the organization's approach to managing and mitigating cyber risks. A well-crafted cyber security policy provides a framework for safeguarding against cyber threats, ensuring data confidentiality, integrity, and availability, and promoting a culture of security awareness within the organization.

Here are some key aspects of how a cyber security policy serves as the foundation of protection:

1. **Risk Management**: The policy defines the organization's risk appetite and risk management strategies. It identifies potential cyber threats and vulnerabilities, assesses their impact, and establishes measures to mitigate risks effectively.

# KM-01-KT04 : A cyber secure organisation 15%

1. **IAC0402 Discuss the importance of a resilient cybersecurity posture.**

Installation weaknesses and vulnerabilities in the context of cybersecurity refer to security gaps and flaws that can be exploited during the setup or deployment of software, applications, systems, or networks. These weaknesses can expose organizations to potential cyber threats and increase the risk of unauthorized access, data breaches, or system compromise. Identifying and addressing installation vulnerabilities is crucial for maintaining a strong cybersecurity posture. Some common installation weaknesses and vulnerabilities include:

1. **Default Settings**: Many software and hardware products come with default settings that are not secure or appropriate for specific environments. Failure to change default passwords or configurations can leave systems vulnerable to unauthorized access.
2. **Outdated Software**: Installing outdated or unpatched software can expose systems to known vulnerabilities that have been addressed in newer versions. Regularly updating software with security patches is essential to mitigate such risks.
3. **IAC0403 Justify the importance of ethics in cybersecurity.**

Ethical considerations related to different types of software licenses are essential for both software developers and users. Various software licenses govern the terms and conditions under which software can be used, distributed, and modified. Understanding the ethical implications of these licenses helps promote responsible and fair use of software and fosters a collaborative and respectful software development community. Here are some ethical considerations related to different types of software licenses:

1. **Open Source Licenses**:
   * **Sharing and Collaboration**: Open-source licenses promote the sharing of software source code and encourage collaborative development. Ethical considerations here involve giving proper credit to original authors and contributing back improvements to the community.