MICTSETA | Media, Information And Communication Technologies Sector Education And Training Authority

SHAPING SKILLS, PIONEERING INDUSTRIES, EMPOWERING FUTURES

EXTERNAL INTEGRATED SUMMATIVE ASSESSMENT - EXEMPLAR

Computer-Based

STUDENT NAME & SURNAME	
ID NUMBER	
EISA REGISTRATION NUMBER	
ASSESSMENT CENTRE	
ASSESSMENT CENTRE ACCREDITATION NUMBER	
QUALIFICATION	
SAQA ID	
CREDITS	
PAPER	
DATE OF EISA	
DURATION	
TOTAL MARKS	

EISA Practical Assessment: Cybersecurity (3 Hours)

This External Integrated Summative Assessment (EISA) evaluates competencies across ELOs 1-5 from the Cybersecurity qualification. Candidates demonstrate practical skills in risk analysis, threat protection, monitoring, response, and recovery in simulated scenarios.[1]

Assessment Instructions

- Duration: 3 hours (180 minutes).
- Resources: Computer with internet access (simulated environment), provided tools (e.g., Wireshark, firewall software, backup utilities).
- Tasks: 4 integrated practical tasks building on a central scenario of a mid-sized South African company (TechSecure Ltd) facing escalating cyber threats.
- Submission: Screenshots, reports, and configurations saved in a zipped folder labeled with candidate ID.
- Marking: Total 100 marks; pass mark 60%.[2]

[1] Cybersecurity-QAS-Addendum-and-Grid.know.csv

[2] Cybersecurity-QAS-Addendum-and-Grid.know.csv

Central Scenario Context

TechSecure Ltd, a Johannesburg-based fintech firm, manages sensitive client data under POPIA compliance. Recent indicators show phishing emails, unusual network traffic, ransomware encryption on servers, and backup integrity issues. You are the cybersecurity analyst tasked with hands-on intervention.[3]

Task 1: Risk Analysis and Vulnerability Scan (45 minutes, 25 marks)

Scenario Expansion: Network logs reveal reconnaissance scans from IP 192.168.1.100 targeting ports 22 (SSH) and 3389 (RDP). Employee reports clicking phishing links mimicking bank alerts, potentially exposing credentials. Database server shows unpatched vulnerabilities (e.g., CVE-2023-1234 in MySQL).

Requirements:

- Scan the simulated network using Nmap or OpenVAS; identify top 5 risks.
- Document vulnerabilities with CVSS scores and potential impacts (e.g., data breach leading to R5 million fine).
- Recommend patches and configurations (e.g., disable RDP if unused).

Evidence: Scan report PDF with analysis (10 marks), risk register table (15 marks).[4]

[3] Cybersecurity-QAS-Addendum-and-Grid.know.csv

[4] Cybersecurity-QAS-Addendum-and-Grid.know.csv

Task 2: Threat Protection and Mitigation (45 minutes, 25 marks)

Scenario Expansion: Firewall logs indicate inbound SYN floods (DoS attack) and malware signatures matching identity theft trojans. Internal user "admin" attempted unauthorized access to HR database, violating ethics policy. Assets at risk: Customer PII and intellectual property code repositories.

Requirements:

- Configure a virtual firewall (e.g., pfSense) to block malicious IPs and enable IDS rules.
- Implement endpoint protection: Encrypt sample data files with AES-256 and set up multi-factor authentication simulation.
- Test and verify mitigation effectiveness.

Evidence: Configuration screenshots (12 marks), test logs showing blocked attempts (13 marks).[5]

[5] Cybersecurity-QAS-Addendum-and-Grid.know.csv

Task 3: Monitoring and Incident Response (45 minutes, 25 marks)

Scenario Expansion: Real-time alerts from SIEM tool show lateral movement post-phishing: Ransomware encrypts /data/share folder (binary logic exploit via weak passwords). Ethical monitoring must balance CIA triad—confidentiality breached, integrity compromised, availability at 50%.

Requirements:

- Set up monitoring with Wireshark or Snort; capture and analyze traffic for anomalies.
- Execute incident response: Isolate affected systems, notify stakeholders per policy.
- Log actions aligning with cybersecurity ethics and governance (e.g., no data tampering).

Evidence: Packet capture analysis report (10 marks), response playbook execution log (15 marks).[6]

[6] Cybersecurity-QAS-Addendum-and-Grid.know.csv

Task 4: Recovery Protocols (45 minutes, 25 marks)

Scenario Expansion: Post-ransomware, backups from last 24 hours are corrupted due to incomplete incremental strategy. Assets include databases and VM images; recovery must restore to RPO of 4 hours while verifying integrity against known hashes.

Requirements:

- Restore from offsite backup using tools like Veeam or rsync; compare pre/post hashes.
- Differentiate backup (proactive copies) vs. recovery (restoration process); document steps.
- Validate system functionality and update recovery plan for future (e.g., 3-2-1 rule).

Evidence: Recovery log with timestamps (12 marks), verification report and plan updates (13 marks).[7]

[7] Cybersecurity-QAS-Addendum-and-Grid.know.csv

Assessment Grid Alignment

Task	ELO Focus	Cognitive Levels (K:C:A:CE %)	Modules
1	ELO 1	20:60:20:0	KM01-KM08[8]
2	ELO 2-3	20:40:30:10	KM02-KM04[9]
3	ELO 3-4	10:30:40:20	KM03-KM07[10]
4	ELO 5	30:40:20:10	KM08[11]

⁂

[8] Cybersecurity-QAS-Addendum-and-Grid.know.csv

[9] Cybersecurity-QAS-Addendum-and-Grid.know.csv

[10] Cybersecurity-QAS-Addendum-and-Grid.know.csv

[11] Cybersecurity-QAS-Addendum-and-Grid.know.csv