Individual Assessment Coversheet

To be attached to the front of the assessment.

Campus: Midrand

Faculty: Information Technology

Module Code: ITNSA

Group: 2

Lecturer's Name: Miss Kangwa

Student Full Name: Asimdumise Zwane

Student Number: EDUV4935855

Indicate	Yes	No
Plagiarism report attached		

Declaration:

I declare that this assessment is my own original work except for source material explicitly acknowledged. I also declare that this assessment or any other of my original work related to it has not been previously, or is not being simultaneously, submitted for this or any other course. I am aware of the AI policy and acknowledge that I have not used any AI technology to generate or manipulate data, other than as permitted by the assessment instructions. I also declare that I am aware of the Institution's policy and regulations on honesty in academic work as set out in the Conditions of Enrolment, and of the disciplinary guidelines applicable to breaches of such policy and regulations.

Signature A.N Zwane	Date: 10 November 2025

Lecturer's Comments:

Marks Awarded: **%**

Signature	**Date**

Eduvos (Pty) Ltd. (formerly Pearson Institute of Higher Education) is registered with the Department of Higher Education and Training as a private higher education institution under the Higher Education Act, 101, of 1997. Registration Certificate number: 2001/HE07/008

Table of Contents

Question 1 3
Question 2 5
2.1. Best Practices. 5
2.2.a. Role of traffic monitoring. 5
b. Monitoring Strategy. 6
Question 3 6
Subnet Plan: 6
Network Segmentation Best Principles. 7
Question 4 10
4.1. Real-time visibility and threat detection plan 10
4.2. Site-to-site IPSec VPN Strategy. 12
Bibliography 16

Question 1

Eskom's cybersecurity incident reveals significant structural and operational vulnerabilities in its network security architecture, primarily due to deficient segmentation, weak access control, inadequate authentication practices, and outdated monitoring systems. These issues facilitated lateral movement, credential compromise, and possible exposure of sensitive systems, including SCADA and HR databases. (Editor, 2025)

Poor Network Segmentation.

Eskom's internal network lacks enough separation between important zones such as the billing, HR/payroll, and SCADA subnets. The least privilege principle is broken by the existence of any-to-any firewall rules between these segments, which permits uncontrolled east-west traffic. After the first intrusion, this misconfiguration allowed attackers to migrate laterally from the Billing subnet into the HR/Payroll systems. The possibility of spill-over attacks, in which an IT system compromise could interfere with operational control networks, is also increased by inadequate segmentation between IT and OT (SCADA) environments. Given SCADA's real-time control over generation and transmission processes, such exposure poses a threat to grid stability.

Weak Access Control and Authentication.

The enforcement of access control measures is inadequate. Only external contractors were given access to Multi-Factor Authentication (MFA), leaving internal staff accounts vulnerable to password-only authentication. Attackers were able to take advantage of brute-force login attempts against the billing site and access internal systems with compromised credentials because MFA was not in place. Staff accounts may have unneeded privileges, extending the blast radius of a breach. The use of weak internal credentials immediately jeopardises the confidentiality and integrity of sensitive customer and staff data held in billing and payroll databases.

Inadequate Monitoring and Incident Detection.

Eskom was unaware of changing attack trends since its intrusion detection and prevention systems (IDS/IPS) had not been upgraded in more than two years. A lack of efficient incident response culture and cooperation between the IT and OT departments is demonstrated by the delay in looking into anomalous SCADA traffic. The detection of brute-force assaults and lateral movement was delayed due to outdated signatures and inadequate log correlation, which decreased visibility into network anomalies. The organization's capacity to maintain the availability and resilience of its vital infrastructure is jeopardised by these flaws since possible threats may spread undetected into control systems. (Editor, 2025)

Risks Associated with the Misconfigured Public Wi-Fi Subnet.

The Public Wi-Fi subnet (192.168.10.0/24) poses a serious security concern since it can bridge a guest network with internal infrastructure by performing internal DNS lookups. Attackers can map internal hostnames, perform network reconnaissance, and find possible targets like billing servers or HR systems thanks to this vulnerability. From this position, a malevolent actor may use collected internal data to social-engineer employees or exploit additional vulnerabilities. Deeper access could allow attackers to alter employee payroll data (impairing integrity), exfiltrate or manipulate customer billing records (breaching confidentiality), or introduce malicious traffic into the SCADA network, potentially disrupting operations or triggering power outages. Beyond data loss, national service continuity and public confidence in Eskom's dependability are at danger. (Systems, 2025)

Eskom is at risk on all fronts of the CIA Triad if identified weaknesses are not addressed: customer billing and employee data could be compromised (Confidentiality); financial and operational data may be manipulated, resulting in fraud or grid mismanagement (Integrity); and electricity supply could be disrupted due to potential SCADA operations interference (Availability).

(Management, 2025)

Question 2

2.1. Best Practices.

Firewall policies should be updated to enforce granular, least-privilege rules that limit traffic by source, destination, and service. These rules should be backed by frequent audits and centralised management to improve ASISA's network security management. Strong encryption (such as AES-256 with IPSec or SSL/TLS) and multi-factor authentication are required for VPN connections to protect remote access, and user groups must be divided and watched for questionable activity. With inter-VLAN firewalls or ACLs to regulate data flow and separate important compliance datasets, the existing flat LAN should be divided into several VLANs that divide departments and regional offices. Role-based and zero-trust principles should guide access control, guaranteeing that users and consultants can only access authorised systems following identity verification via a central directory like Azure AD or Active Directory. Together, these steps would preserve ASISA's hybrid architecture, secure private investment and savings information, and uphold confidence in its digital regulatory activities.

2.2.a. Role of traffic monitoring.

Traffic monitoring and logging are critical to improving ASISA's cybersecurity posture because they provide continuous visibility into network activity, allowing for early detection of aberrant or malicious behaviour that could jeopardise sensitive financial and regulatory data. ASISA may monitor access attempts, identify policy violations, and assist forensic investigations in the event of breaches by methodically gathering logs from firewalls, servers, VPNs, and endpoints. By centralising these logs in a Security Information and Event Management (SIEM) system, incident response efficiency would be increased by real-time correlation and alerting. (Busch, 2024)

By studying network traffic patterns and spotting signatures or anomalies that point to cyberattacks like malware infections, data exfiltration, or unauthorised access attempts, the deployment of Intrusion Detection and Prevention Systems (IDS/IPS) will significantly improve threat visibility. The IPS actively stops or quarantines

harmful traffic before it reaches important systems. IDS/IPS would ensure the security and integrity of financial data by protecting regulatory data flows between regional offices and cloud platforms in ASISA's hybrid environment, which combines on-premises and cloud systems. ASISA's capacity to identify, address, and prevent cybersecurity issues is strengthened by the layered defence that traffic monitoring, logging, and IDS/IPS together provide.

b. Monitoring Strategy.

For ASISA's hybrid architecture, a good monitoring plan would integrate cloud and on-site monitoring into a single solution. While cloud platforms should employ tools like Azure Security Centre or AWS CloudWatch to monitor access and configuration changes, on-site networks can use IDS/IPS and firewall log analysis to find suspect behaviour. For real-time warnings and threat correlation, every log should be sent into a central SIEM. Continuous visibility, quick incident response, and robust protection of ASISA's critical financial and regulatory data are all ensured by this unified approach. (Sharif, 2023)

Question 3

Subnet Plan:

VLAN	Name	Site	Network (CIDR)	Netmask	Network Range	Usable IP Range
10	Administration	Cape Town	10.20.0.0/26	255.255.255.192	10.20.0.0 – 10.20.0.63	10.20.0.2 – 10.20.0.62
11	Licensing and Compliance	Cape Town	10.20.0.64/26	255.255.255.192	10.20.0.64 – 10.20.0.127	10.20.0.66 – 10.20.0.126
12	Fisheries Monitoring	Cape Town	10.20.0.128/26	255.255.255.192	10.20.0.128 – 10.20.0.191	10.20.0.130 – 10.20.0.190
13	HR & Finance	Cape Town	10.20.0.192/27	255.255.255.224	10.20.0.192 – 10.20.0.223	10.20.0.194 – 10.20.0.222

20	IT & Logistics	Durban	10.20.0.224/27	255.255.255.224	10.20.0.224 – 10.20.0.255	10.20.0.226 – 10.20.0.254
21	Vessel Tracking & Surveillance	Durban	10.20.1.0/27	255.255.255.224	10.20.1.0 – 10.20.1.31	10.20.1.1 – 10.20.1.30
30	Environmental Monitoring	Port Elizabeth	10.20.1.32/28	255.255.255.240	10.20.1.32 – 10.20.1.47	10.20.1.33 – 10.20.1.46
40	DMZ (Web, Mail, reverse proxy, WAF)	Any/ Central	10.20.1.48/28	255.255.255.240	10.20.1.48 – 10.20.1.63	10.20.1.49 – 10.20.1.62
41	Management & Monitoring	Any/ Central	10.20.1.64/28	255.255.255.240	10.20.1.64 – 10.20.1.79	10.20.1.65 – 10.20.1.78
42	VPN client pool (remote inspectors)	Any/ Central	10.20.1.80/27	255.255.255.224	10.20.1.80 – 10.20.1.111	10.20.1.81 – 10.20.1.110
-	Reserved for future services	-	10.20.1.112 – 10.20.1.255	-	10.20.1.112 – 10.20.1.255	-

Network Segmentation Best Principles.

The Fisheries Department's network should be segmented to isolate crucial operations while allowing authorized connectivity between vital systems to guarantee security and operational effectiveness. To provide logical separation that stops needless traffic flow and restricts the spread of security incidents like malware or unauthorized access, each department and functional area should have its own VLAN and subnet. (Chin, 2025)

1. **Apply the Principle of Least Privilege:**

Access Control Lists (ACLs) on routers or the Cisco ASA firewall must be used to strictly regulate access between VLANs. Every department should only have the minimal network rights needed to carry out its responsibilities. For instance, unless certain shared programs (like the payroll or ERP system) need it, the HR & Finance subnet shouldn't have direct access to the Fisheries Monitoring subnet.

2. **Employ Layered Security (Defence in Depth):**

One device should not be the exclusive source of security. Apply several levels of security instead, such as firewall filtering, endpoint protection, intrusion detection/prevention (IDS/IPS), and VLAN segmentation. All traffic between internal subnets and external networks should be inspected by the ASA firewall, and interdepartmental communication should go through controlled routing points that enforce filtering and monitoring.

3. **Isolate Sensitive and Public Zones:**

The DMZ and public internet must be completely cut off from vital internal systems including HR databases, compliance data, and fishery monitoring tools. Only public-facing services, such as web and email servers, which interact with internal systems via a proxy or particular application gateway rather than directly, should be housed in the DMZ. This lessens the possibility that sensitive research or personnel data will be compromised by outside threats.

4. **Establish Dedicated Management and Monitoring Networks:**

Every network equipment, including servers, switches, firewalls, and routers, should be controlled by a different Management VLAN that is only accessible by authorized administrators. This VLAN should only be accessible via secure channels like SSH or VPN, and it shouldn't handle regular user traffic. To centralize control over network health and security events, monitoring tools such as SNMP collectors, NMS platforms, and Syslog servers should also be in this VLAN.

5. **Turn on Role-Based Access Control (RBAC):**

Roles should be used to control user access to network resources. The ASA firewall or authentication server (such as Active Directory or RADIUS) should impose different access controls for researchers, inspectors, and administrators. This guarantees that data access is still managed in accordance with job functions even inside the same subnet. (Wickramasinghe, 2024)

6. **Use Secure Inter-Site Connectivity:**

An IPsec Site-to-Site VPN should be used for communication between Cape Town, Durban, and Port Elizabeth because the department operates in several places. This guarantees that information moving over the public internet is encrypted and shielded from eavesdropping. To reduce the attack surface, VPN tunnels should be set up to only permit communication between authorized subnets.

7. **Track and Log Inter-VLAN Traffic:**

All traffic between sites and VLANs should be tracked and examined for odd activity. The department can identify trends like illegal access attempts or data exfiltration by using a centralized SIEM (Security Information and Event Management) technology. To guarantee compliance and early threat detection, logs from firewalls, VPNs, and IDS/IPS systems should be routinely examined.

8. **Implement Quality of Service (QoS) and Network Policies:**

To guarantee performance and dependability, critical applications like the Fisheries ERP, vessel tracking systems, and VoIP communications should be given higher bandwidth priority. Large data transfers or guest Wi-Fi are examples of bandwidth-intensive but less important traffic that should be restricted or scheduled for off-peak times.

9. **Frequently Audit and Update Segmentation Policies:**

To ensure that network segmentation rules continue to meet operational needs, they should be examined on a regular basis. Additional subnets or exceptions may be needed for new departments, systems, or research projects; they should be established using a structured change control procedure. To have a clean, safe configuration, out-of-date or unnecessary rules must be eliminated.

Conclusion

510 usable addresses give room for growth, simpler ACLs, clean per-site + per-service subnets and a reasonable VPN pool without squeezing the DMZ/management ranges. The default gateway for each subnet is the first useable IP address (e.g., 10.20.0.1 for the Administration VLAN). This facilitates the identification and uniform management of gateway addresses across all sites. While keeping administrative, operational, and public-facing systems clearly separated, this subnetting structure promotes efficiency, scalability, and security. Additionally, it makes monitoring, policy enforcement, and troubleshooting easier across all Fisheries Department locations. (Ballejos, 2025)

Question 4

4.1. Real-time visibility and threat detection plan

In my capacity as the security consultant, I suggest a real-time network visibility and threat-detection strategy that incorporates Intrusion Detection and Prevention Systems (IDS/IPS) throughout the DMZ housing public-facing services as well as the Fisheries Department's locations in Cape Town, Durban, and Port Elizabeth.

1. **IDS/IPS Placement and Architecture:**

To actively block malicious traffic, each site will install inline IPS at the network perimeter, which is situated between the internal LAN and the Cisco ASA firewall. To track internal east-west traffic, a passive IDS sensor will be installed on important internal network segments, such as those connecting departmental VLANs to the core switch. All incoming and outgoing traffic to and from public web and email servers will be inspected by a dedicated IDS/IPS sensor in the DMZ, which will identify web application and email-based threats before they get to vital systems.

2. **Traffic Inspection Scope: The IDS/IPS ought to examine:**

The incoming internet traffic that enters the DMZ in search of malware, exploits, and brute-force login attempts. Inter-site VPN traffic between Port Elizabeth, Durban, and Cape Town for attempts at data exfiltration or policy violations. Internal communication between departmental VLANs to identify insider risks or lateral mobility. Also look for unusual data transfers in outbound traffic that might point to compromised sites or command-and-control communication.

3. **Detection and Tuning:**

The systems will be adjusted to identify a variety of dangers, such as:

- Assaults that rely on signatures (malware, phishing payloads, SQL injection, and cross-site scripting).
- Unusual login times, massive data uploads, or access to servers that are prohibited are examples of anomalous behaviour.
- Research databases and HR systems are the target of port scans and reconnaissance attempts.
- Infractions of the policy, include using external file-sharing services or VPN tunnels without authorization.
- Accurate detection will be ensured, and false positives will be minimized with regular signature updates and baseline behaviour modelling.

4. **Centralized Log Analysis and SIEM Correlation:**

A centralized Security Information and Event Management (SIEM) platform at the Cape Town headquarters will receive all IDS/IPS alarms, firewall logs, and VPN connection records. To provide a cohesive picture of network activity and enable security analysts to identify multi-stage assaults that span several locations, the SIEM will correlate data from all three sites. Critical occurrences, such repeated unsuccessful login attempts or data transfers to unidentified locations, will trigger automated alarms.

5. **Proactive Monitoring and Security Benefits:**

Real-time, proactive monitoring will improve service dependability and security. Early intrusion detection prevents data breaches involving sensitive research or compliance data by enabling the department to isolate impacted systems before damage is done. Network performance is further enhanced by continuous visibility since anomalous traffic patterns can be fixed before they result in congestion or poor service. Through the integration of IDS/IPS with automated reporting and central log analysis, the Fisheries Department will be able to create a network infrastructure that is more secure, flexible, and robust throughout all of its operational locations.

4.2. Site-to-site IPSec VPN Strategy.

1. **Key exchange options and protocols**

IKE version: IKEv2; more reliable, quicker rekeying, improved NAT-Traversal, and easier setup for contemporary devices.

IKE (Phase-1/IKE SA) plan:

Encryption: AES-GCM-256 (AEAD offers integrity and secrecy in a single primitive).

PRF/Integrity (IKE auth): SHA-384 (used, when necessary, in IKE PRF/HMAC).

DH/Key exchange: group 19 (P-256) serves as a backup, while group 20 (P-384) is the primary.

The lifespan of the IKE SA is 86,400s (24 hours), a balance between stability and security.

Recommended primary IPsec (Phase-2/Child SA) proposal:

ESP: ECDH group 19 (P-256) with AES-GCM-256 (AEAD cipher) and PFS enabled.

Rekeying can be planned for periods of low traffic; the child SA lifetime is 28,800s (8hours) or the data volume threshold.

Why these choices: IKEv2 enhances stability/DPD and NAT traversal; ECDH groups minimize compute compared to big MODP groups while delivering strong PFS; AES-GCM offers good security and typically hardware acceleration (AES-NI) on newer devices. (Heintzkill, 2023)

2. **Credential management and peer authentication**

Certificate-based authentication using a small PKI (internal CA or enterprise PKI) is the main solution. For IKE authentication, use ECDSA certificates (P-256/P-384).

Advantages:

- Teams do not disclose a secret.
- Simpler to rotate and revoke (CRL/OCSP).
- More robust defence than PSK (resists offline brute force).
- Use high-entropy pre-shared keys (PSKs) safely stored in configuration vaults in conjunction with peer IP limitations and frequent rotation as a fallback or operational option if PKI is not accessible.

Operational items include setting expiration and CRL/OCSP checks, issuing site certificates to each ASA/firewall, and upholding a safe cert-revocation procedure.

3. **Routing policies with the tunnel model**

The suggested approach is route-based VPNs with dynamic routing (OSPF) over the tunnel or tunnels utilizing Virtual Tunnel Interfaces (VTI) or something similar.

Why route-based: VTIs facilitate the execution of routing protocols, provide multipoint, and streamline failover and ACLs.

Routing protocol: OSPFv2 between sites via VTIs; limit OSPF areas to site interconnect only and enable OSPF authentication. If policy simplicity is necessary, use static routes instead; however, dynamic routing is advised for scalability and resiliency.

Route advertisement policy: Don't disseminate the internet default route into the tunnel; instead, only promote the internal networks of the local site.

Selectors of traffic: Set up crypto selectors or ACLs to match just the precise site networks:

- Cape Town to Durban: 10.20.0.0/22 – 192.16.8.0/22
- Cape Town to Port Elizabeth: 10.20.0.0/22 – 192.168.50.0/24
- Durban to Port Elizabeth: 172.16.8.0/22 – 192.168.50.0/24

Every site uses local internet transit; do not send general internet traffic across the tunnels. The VPN is only traversed by the specified inter-site prefixes. (Editor, 2025)

4. **Traffic limitation and access control**

- Only authorized inter-site subnets must be strictly matched by crypto ACLs and selectors. Any traffic that tries to match other selectors should be dropped by devices.

- Firewall rules on ASA: by default, deny all other ports and only permit necessary services between sites (such as DB replication ports, management, vessel telemetry ports, and OSPF).

- Least privilege routing: Inadvertently advertising internal-only segments into the VPN should be prevented by network ACLs and route filters. If BGP is being utilized, employ prefix/route filters.

5. Availability, performance, and resilience

Dual tunnels per peer: Establish two IPsec tunnels, either to separate public IP addresses on the same site or to separate ISP links, between each site (main and backup). For automatic failover, use routing metrics (OSPF cost or static route preferences).

Device HA: To ensure that tunnels are maintained during failover, set up the ASA/edge firewall in active/standby (stateful failover).

DPD/Keepalive: To preserve availability, activate Dead Peer Detection (DPD) and aggressive re-establishment.

IP SLA/WAN failover: Use IP SLA probes to swiftly identify failover links and WAN outages.

Performance

Hardware acceleration: Make use of devices that have AES-NI or IPsec offload (ASA with hardware crypto module, or dedicated VPN equipment).

Crypto selections adjusted for CPU: For robust security and effective CPU utilization, choose AES-GCM + ECDH.

MTU tuning and fragmentation: To prevent fragmentation, lower the tunnel MTU (for example, 1400) and allow path MTU discovery.

Rekey policy: Plan rekeys at sensible intervals, refrain from rekeying every tunnel at once, and rekey during periods of low traffic if throughput is high.

6. **Protection against common attacks.**

ACLs and rate-limiting lessen brute-force and DoS attacks; certificate-based authentication with ECDH and Perfect Forward Secrecy (PFS) protects against man-in-the-middle attacks and guarantees session confidentiality; and replay protection in ESP blocks duplicate packets. Access to approved subnets is restricted by strict traffic selectors, and fragmentation problems are avoided by NAT-Traversal and Path MTU Discovery. Frequent firmware updates provide a strong and secure VPN environment by guarding against protocol-level vulnerabilities.

7. **Monitoring, logging, and key lifecycle management**

Centralized logging and real-time monitoring improve security and performance. For correlation and anomaly detection, a central SIEM receives all VPN events, including tunnel formation, rekeying, and connection dropouts. Early threat detection is aided by alerts for recurring failures or anomalous data transfers. To guarantee service stability, tunnel performance indicators including latency and packet loss are tracked. To prevent unwanted access, keys and certificates are routinely cycled, and OCSP or CRL are used to verify the authenticity of certificates. The VPN is kept dependable, secure, and compliant through ongoing monitoring and appropriate key management. (Editor, 2025)

Bibliography

Ballejos, L., 2025. *NinjaOne.* [Online]
Available at: https://www.ninjaone.com
[Accessed 21 October 2025].

Busch, Z., 2024. *G2 Learning Hub.* [Online]
Available at: https://learn.g2.com
[Accessed 30 October 2025].

Chin, K., 2025. *UpGuard.* [Online]
Available at: https://www.upguard.com
[Accessed 3 November 2025].

Editor, 2025. *Threats to Information Security.* [Online]
Available at: https://www.geeksforgeeks.org
[Accessed 30 October 2025].

Editor, 2025. *V2 Cloud.* [Online]
Available at: https://v2cloud.com
[Accessed 3 November 2025].

Editor, N. S., 2025. *Network security threats and vulnerabilities.* [Online]
Available at: https://nordlayer.com
[Accessed 31 October 2025].

Editor, O., 2025. *Oracle Help Center.* [Online]
Available at: https://docs.oracle.com
[Accessed 30 October 2025].

Heintzkill, R., 2023. *CBT Nuggets.* [Online]
Available at: https://www.cbtnuggets.com
[Accessed 1 November 2025].

Management, N., 2025. *What is network security?.* [Online]
Available at: https://www.imperva.com
[Accessed 31 October 2025].

Sharif, A., 2023. *CrowdStrike.* [Online]
Available at: https://www.crowdstrike.com
[Accessed 29 October 2025].

Systems, C., 2025. *Network and data protection.* [Online]
Available at: https://www.cisco.com
[Accessed 31 October 2025].

Wickramasinghe, S., 2024. *Splunk.* [Online]
Available at: https://www.splunk.com
[Accessed 4 November 2025].