Eskom	Standard	Technology

Title: **INFORMATION AND COMMUNICATIONS TECHNOLOGY NETWORK SECURITY FRAMEWORK**

Unique Identifier:	**240-146054527**
Alternative Reference Number:	**N/A**
Area of Applicability:	**Engineering**
Documentation Type:	**Standard**
Revision:	**1**
Total Pages:	**28**
Next Review Date:	**January 2025**
Disclosure Classification:	**Controlled Disclosure**

Compiled by	Approved by	Authorized by
Matthew Taljaard	Richard McCurrach	Karen Pillay
Engineer Telecommunications T&S	Senior Manager PTM&C	General Manager Security (Acting)
Date: 30/09/2019	Date: 30/9/2019	Date: 7/11/2019

Authorized by	Authorized by	Supported by SCOT/SC
Titus Mathe	Nico Harris	Kgomotso Setlhapelo
General Manager Group Technology	General Manager IT (Acting)	Telecommunications SCOT SC Chairperson
Date: 12/11/2019	Date: 5/12/2019	Date: 14/11/2019

PCM Reference: **240-53458797 PCM for Perform PTM&C Systems Engineering**
SCOT Study Committee Number/Name: **Telecommunications Study Committee**

Content

ESKOM COPYRIGHT PROTECTED

When downloaded from the WEB, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the WEB.

Figures

Tables

ESKOM COPYRIGHT PROTECTED

When downloaded from the WEB, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the WEB.

1. Introduction

Information and Communications Technology (ICT) is essential to ensuring a business is able to operate across vast locations and systems.

The need for interconnectivity is now being embraced by the business as a whole, which requires these different networks and providers to communicate and collaborate with each other.

An interconnected network brings both advantages and disadvantages. A network security framework is required to provide guidelines, processes and standards to manage communications, controls, connections and collaboration amongst the different network providers in Eskom.

There are three main types of network providers to Eskom; these are Group IT (which provides Corporate LAN and MPLS WAN country-wide links), Eskom Telecommunications (ET) (which provides Operational Technology LAN and MPLS WAN country-wide links), and other 3rd Party Telecommunications Service Providers (which provide LAN/WAN/APN/Radio/Satellite/Internet links to both Group IT and Eskom Telecommunications). Some networks in the Eskom environment are segregated with no interconnectivity, and are known as “air-gapped” or “islanded" networks. These networks may also require connectivity in the near future.

The future Eskom network should incorporate the confidentiality, integrity and availability (CIA) requirements for all of Eskom’s services. It is therefore important that cybersecurity principles are embedded in the framework, architecture and design of future ICT security networks.

2. Supporting clauses

2.1 Scope

This document gives the high-level framework of the proposed future Eskom ICT network security estate. The framework will assist Eskom in aligning to relevant legislative acts. The document covers the intended use of the Eskom’s ICT network security and how it aims to achieve the challenges Eskom experiences.

Network aspects will be included in relevant network frameworks, roadmaps, architecture and/or other documents.

2.1.1 Purpose

The purpose of this document is to give a high-level understanding on the following:

1) Define a Network Security Framework for all Eskom ICT environments.
2) Assist in addressing current and future demands and challenges of the electric power utility network.
3) Alignment of ICT Network Security Framework with Cybersecurity requirements
4) Identify the key role players for Eskom ICT network security and their responsibility to the business.
5) Provide direction of secure interconnectivity between the key role players in Eskom (IT, ET, 3rd Party),

2.1.2 Applicability

This document shall apply throughout Eskom Holdings Limited Divisions.

2.2 Normative/informative references

Parties using this document shall apply the most recent edition of the documents listed in the following paragraphs.

ESKOM COPYRIGHT PROTECTED

When downloaded from the WEB, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the WEB.

2.2.1 Normative

[1] 32-85 Information Security Policy

[2] 32-373 IT OT Third Party Remote Access Standard

[3] 32-377 Information Security – Firewall Standard

[4] 32-729 System Operator Minimum Telecommunications Requirements

[5] 32-1203 Eskom Telecommunications User Requirement Specifications

[6] 240-4620188 Fibre Optic Roadmap

[7] 240-50201762 Information Security - Network Security Standard

[8] 240-55410927 Cyber Security Standard for Operational Technology Rev. 2

[9] 240-55863502 Definition of Operational Technology (OT) and OT / IT Collaboration Accountabilities

[10] 240-56927206 Corporate Plan

[11] 240-606480018 Terms of Reference for Design Review Teams Presiding Over Transmission and Distribution Infrastructure Designs in Eskom

[12] 240-61268959 Substation Automation - Network Architecture Standard for Transmission Substations

[13] 240-79669677 Demilitarised Designs for Operational Technology Systems

[14] 240-81321219 Substation Automation - Network Architecture Standard for Distribution Substations

[15] 240-91714320 Telecommunications Network Cybersecurity Architecture

2.2.2 Informative

[16] SABS Standards Division, SANS 62443-2-1:2016 “Part 2-1: Establishing an Industrial Automation and Control System Security Program”, Pretoria, June 2016.

[17] Homeland Security, “Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies”, September 2016.

[18] National Institute of Standards and Technology, Special Publication 800-82 “Guide to Industrial Control Systems (ICS) Security”, May 2015.

[19] Y. Zhu, B. Wang, S. Zhang, “The Analysis and Design of Network and Information Security of Electric Power System”, IEEE Transmission and Distribution Conference, China, 2005.

[20] A. Conklin, “IT vs OT Security: A Time to consider a Change in CIA to include Resilience” 49th Hawaii International Conference on System Sciences, 2016.

[21] National Institute of Standard and Technology, “Guidelines for Smart Grid Cybersecurity”, 7628 Rev.1, September 2014.

[22] National Institute of Standard and Technology, “Framework for Improving Critical Infrastructure Cybersecurity”, Rev. 1, February 2014.

[23] ITU-T, “Overview of Cybersecurity”, X.1205 Rev. 1, April 2008.

[24] System Administration, Networking, and Security Institute, “Infrastructure Security Architecture for Effective Security Monitoring”, Rev. 1, December 2015.

[25] Republic of South Africa, “National Ley Points Act”, Act No. 102, 25 July 1980, [On-line]. Available: https://www.gov.za/sites/default/files/Act%20102%20of%201980.pdf [June 15, 2018].

[26] Republic of South Africa, “Critical Infrastructure Bill”, B22-2017, [On-line]. Available: https://www.saps.gov.za/resource_centre/bills/downloads/infrastructure_protection_bill_2017.pdf [June 15, 2018].

ESKOM COPYRIGHT PROTECTED

When downloaded from the WEB, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the WEB.

[27] Republic of South Africa, "Cybercrimes and Cybersecurity Bill", B6-2017, Gazette No. 40487, 9 December 2016 [On-line]. Available: http://www.justice.gov.za/legislation/bills/CyberCrimesBill2017.pdf [June 15, 2018].

2.3 Definitions

2.3.1 General

Definition	Description
Critical Asset	Facilities, systems, and equipment which if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the electric power utility network. Criteria for a critical asset is defined in 240-55410927 "Cyber Security Standard for Operational Technology".
Cybersecurity	Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and user's assets. Organisation and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organisation and user's assets against relevant security risks in the cyber environment. The general security objectives comprise of Availability, Integrity, which includes authenticity and non-repudiation and Confidentiality
Data Centre	A data centre is a repository that houses computing facilities like servers, routers, switches, and firewalls, as well as supporting components like backup equipment, fire suppression facilities, and air conditioning. A data centre may be a dedicated building or a room known as a data room. A data centre may be private or shared.
Electronic Security Perimeter	An electronic security perimeter (ESP) is a logical fencing of a system. The term ESP is introduced when a system has multiple secure zones. An example is a data centre with geographical separate sites for redundancy. At a minimum, this data centre will have two secure zones (one for site A and one for site B) but collectively they will reside together under one ESP (e.g. data centre X ESP) to create a high availability data centre.
Hardening	The process of securing a system by reducing its surface of vulnerability.
Information and Communication Technology	The Information and Communication Technology (ICT) is an umbrella term to describe the collective Eskom Telecommunications and Group Information Technology network.
Information Technology	Information Technology (IT) is a common term used to describe the entire spectrum of technologies used for corporate information processing including software, hardware and related services. It involves the electronic representation of business information that is processed by a computer or sent over digital communications (e.g. IP network). In Eskom, the Group Information Technology (GIT) business unit represents IT.

ESKOM COPYRIGHT PROTECTED

When downloaded from the WEB, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the WEB.

Definition	Description
IT-OT Convergence	The trend that: The underlying platforms and technologies used in IT and OT are increasingly the same; The underlying platforms are increasingly using some shared infrastructure, standard and approaches; The shifting from proprietary and hardware-based technology to open and software-based technology; The evolution of new risks due to the above; Those companies are increasingly leveraging these trends for increased business value and efficient monetary spending.
Jump Server	A jump server is a device that spans two dissimilar security zones (such as a DMZ and a zone residing in a secure area) and provides a controlled means of access between them. A hardened jump server can be used for critical areas of the business such as connections into Secure Area 1.
Open Systems Interconnection Model	Open System Interconnection (OSI) model is a conceptual model that standardises the communication functions of a telecommunication or computing system without regard to the underlying internal structure and technology. The model uses layers and defined as such: Physical Layer – Transmission and reception of raw bit streams over a physical medium. Data Link Layer – Reliable transmission of data frames between two nodes connected by a physical layer. Network Layer – Structuring and managing a multi-node network, including addressing routing and traffic control. Transport Layer – Reliable transmission of data segments between points on a network including segmentation, acknowledgement and multiplexing. Session Layer – Managing communication sessions. Presentation Layer – Translation of data between a networking service and an application. Application Layer – High-level application programming interface.
Operational Technology	Technology used to control, monitor or operate the electrical grid are considered Operational Technology (OT).This is considered Eskom's core business.
Secure Area	A secure area is a term used to secure a service both on site and in transport. Secure areas are setup in a manner that prevents propagation of a threat from one secure area to another. When a secure area is defined in an organisation, those classed services must be segregated from services outside that secure area. Segregation can be in the following: Physical insulation, protocol insulation and firewall insulation.
Security Zone	A security zone is defined as a grouping of logical or physical assets that share common security requirements. A security zone is a segregate zone in a network. A security zone is limited to the physical infrastructure that creates that zone. Once the data leaves that segregation device (e.g. firewall), it is in another zone. Examples can be a control zone for production equipment, a demilitarised zone for sharing information between networks, an enterprise zone for the corporate side of the business, etc.

ESKOM COPYRIGHT PROTECTED

When downloaded from the WEB, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the WEB.

2.3.2 Disclosure classification

Controlled disclosure: controlled disclosure to external parties (either enforced by law, or discretionary).

2.4 Abbreviations

Abbreviation	Description
ADR	Architecture and Design Review Committee
CCA	Critical Cyber Assets
CIA	Confidentiality, Integrity and Availability
CSMS	Cybersecurity Management Systems
DMZ	Demilitarized Zone
EAB	Enterprise Architecture Board
ESP	Electronic Security Perimeter
ET	Eskom Telecommunications
LAN/WAN	Local Area Network / Wide Area Network
HMI	Human Machine Interface
ICT	Information and Communications Technology
IP/MPLS	Internet Protocol / Multiprotocol Label Switching
IS	Information Security
IT	Information Technology
OSI	Open System Interconnection
OT	Operational Technology
PLC	Programmable Logic Controller
PSP	Physical Security Perimeter
SCADA	Supervisory Control and Data Acquisition
SCOT	Steering Committee of Technologies
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network

2.5 Roles and responsibilities

The following are roles and responsibilities for the implementation of this document:

1) ICT Network Security – Responsible for the secure implementation, operation and maintenance of all ICT Network Systems (Systems including Signalling, Voice and Data across any medium including Wired, Wireless, Optical, Radio, Satellite). (Members/Committees/Group to be confirmed)

2) ICT Network System Planners are responsible for assessing the requirements on a per site basis and perform the detailed design based on the site-specific requirements. (Members/Committees/Group to be confirmed)

ESKOM COPYRIGHT PROTECTED

When downloaded from the WEB, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the WEB.

3) ICT Network System Owners shall participate in the standards and process development through approved committees and architecture forums and project implementation through design review governance. (Members/Committees/Group to be confirmed)

2.6 Process for monitoring

The framework is to provide guidance for key role players to update their documentation and designs going forward.

The relevant committees as per the roles and responsibilities above shall review this framework.

The framework should provide the ability to measure risk and improve security.

The framework should map back to COBIT, ISO, NIST, CIS etc.

2.7 Related/supporting documents

Not applicable.

3. Eskom Information and Communication Technology

Eskom ICT currently has two units which are:

1) Operational Technology (OT): Technology used to control, monitor and operate the electrical grid is considered OT. OT's availability, integrity and confidentiality requirements have led to Eskom constructing an internal telecommunications network known as Eskom Telecommunications (ET).

2) Information Technology (IT): Term used to describe the entire spectrum of technologies used for corporate information processing including software, hardware and related services. It involves the electronic representation of business information that is processed by a computer or sent over digital communications.

ET provides majority of the operational telecommunications network links and where it cannot, third party network service providers are sourced to ensure connectivity. IT has leveraged some of ET's existing communications infrastructure where possible but mostly utilises connections from third party network service providers.

Therefore, multiple networks, both internal and external, currently provide communications for both IT and OT sites and systems across Eskom.

The concerns with this are:

1) No common Network Security Framework in place between IT ,ET and OT

2) Limited number of accepted Network Security Communications Standards between IT, OT and ET

3) No documented Network Security Processes between IT, ET and OT

The framework needs to be established based on existing standards, guidelines, and practices – for reducing cyber risks to all infrastructures especially to critical assets.

4. Information and Communication Technology Network Security Framework

NIST Cybersecurity Frameworks provides guidance on Functions and Categories for Cybersecurity, this existing framework can be adapted for the Network Security framework and serve as a guideline.

The NIST functions are Identify, Protect, Detect, Respond and Recover:

- Identify: Develop an organizational understanding to manage network security risk to systems, people, assets, data, and capabilities

ESKOM COPYRIGHT PROTECTED

When downloaded from the WEB, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the WEB.

a) Document critical assets and business environments

b) Identify required Governance

c) Understand the need for Risk assessment

d) Identify required Risk Management strategies

- Protect: Develop and implement appropriate safeguards to ensure delivery of critical services

a) Develop, document and implement access control with monitoring, reporting and alerting.

b) Create Awareness and conduct Training in the environment

c) Enforce data security controls

d) Create information protection processes and processes

e) Perform regular maintenance

f) Research and implement protective technologies

- Detect: Develop and implement appropriate activities to identify the occurrence of a network security event

a) Implement Systems to Detect Anomalies and highlight/alert on Security Events

b) Perform Security Continuous Monitoring

c) Implement and Improve on Detection Processes

- Respond: Develop and implement appropriate activities to take action regarding a detected network security incident

a) Have Response plans in place

b) Have communications channels and mechanisms in place

c) Ability to be able to perform Analysis, Implement Mitigation and Implement Improvements

- Recover: Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a network security incident

a) Recovery Planning for minor/major system/environmental/network security service related disasters

b) Improvements and maintenance of all recovery planning with regular tests of the plans

c) Accepted trusted communication channels during recovery processes

4.1 ICT Network Security Focus Areas

Table 1: ICT Network Security Focus Areas

Category	Current State	To Be
Network Security Analysis and Planning	Done in silos for each environment/provider.	Combined planning will lead to effective security analysis.
Network Security Architecture	Current focus is on point solutions to be able to quickly deliver on a project request.	Point solution view should be expanded to include the bigger picture for the entire landscape. Focus needs to include the end-state of the network security estate.

ESKOM COPYRIGHT PROTECTED

When downloaded from the WEB, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the WEB.

Category	Current State	To Be
Network Security Design	Primary focus is protecting assets/devices and the information stored on or transmitted among these assets.	Secured by Design; all assets/components to should be protected and authenticated/validated as trusted. Defence-in-depth with clear separation of components in a solution will simplify designs for easy understanding, deployment and troubleshooting.
Network Security Implementation	Zero trust and vague understanding between environments and role players result in duplication or services and devices.	Document current ICT network security architectures for both IT and OT, list the best practices/methodologies from each environment and adopt a rollout project to align the remaining ICT network security environments to a common security standard.
Network Security Support	Support functions performed by both in house technical teams and 3rd party vendors, 3rd party vendors benefit from this methodology (limited skills and knowledge transfer to in house teams).	Support functions should only be performed by in house technical teams and escalations for additional support to 3rd party vendors, where possible.
Network Security Availability and Resilience	Availability and resilience of systems, applications, and network environments ensures productivity of the Eskom business as a whole. Network security devices require regular updates and maintenance software to ensure that they are up-to-date against current threats and vulnerabilities. Some networks are being maintained regularly and some networks have little or no maintenance being done due to availability requirements.	Network security devices need to be deployed in highly available configurations to reduce/minimise downtime and impact. Single points of failure in the environment need to documented and optimised to reduce impact. Where unplanned downtime is experienced, the current design deployment needs to be documented, optimised and re-tested for improvements in availability uptimes.
Secure Communications	Current communications across wired and wireless LAN and WAN networks is currently done via both encrypted and clear text protocols, these risks needs to be highlighted, logged in a risk register and tracked until resolution thereof. Failure of resolution will trigger a risk letter being issued for the risk being accepted as known.	All communications should be secured by encryption to mitigate attacks by tampering of data as it is passed from one environment or system to another. This must include local LAN segment communications between systems and devices.
Network Security Appliance Lifetime	Network Security appliance lifetime is generally between 3-5 years, as determined by the Vendor/Supplier. Once an appliance reaches end of life/support/maintenance/sale, the service offering of the appliances is no longer guaranteed	Network security appliances need periodic replacement and with hardware/software and maintenance support to provide a level of acceptable service level.
Network Security Standards(Technology Specific)	Missing and duplicated standards.	Create standards for each technology within the network security environment: • Firewalls • VPN • IPS • Antibot • Antivirus • Data Leakage Protection • Application Filtering

ESKOM COPYRIGHT PROTECTED

When downloaded from the WEB, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the WEB.

Category	Current State	To Be
		• URL Filtering • DNS • NTP • DDOS • WAF • Load Balancing(with techniques/algorithms) • Reverse/Forward Proxy • Routers (including access control lists usage schemas, protocols authentication and key requirements etc.) • Switches (including VLAN, port/mac security, filtering etc. • Wireless Technologies and WIFI • APN's • Satellite Services • Radio Links(RF) • Management Zones • Internet Service Provider and Edge Minimum Network Security Requirements • Guest WIFI • Cross Functional Network and Network Security Services • Other components not included in the above list
Network Security Product Specific Configuration Standard (Technical Document)	Missing and duplicated technical standards	• Cisco Firewall Standard • Checkpoint Firewall Standard • Cisco Switch Standard • Cisco Router Standard • Cisco WIFI Controller Standard • Other Vendors related Standards
Network Security Hardware and Software Baselines	Strive to Achieve Software Vendor release versions of N-1 Mix of 100/1000MB Appliances in the environments	All Device release versions to be N-1 Minimum standard of device capabilities should be 1Gig interfaces copper or fibre with sufficient memory and processing capabilities
Network Security Toolsets	Ad-hoc, in-house, freeware, unregistered software toolsets used for support. Support Hardware(Laptops) not for technical operations use	Standardise on required toolsets and software/hardware to perform support, monitoring, maintenance.
Network Security Guidelines, Patterns, Best Practices		• SCADA Segmentation Pattern (Reference Levels 0 – 5) • DMZ Generic Patterns (Web, App, DB etc.) • Best Practice guides for appliances, configurations • Generic Guideline Network Security Documents

ESKOM COPYRIGHT PROTECTED

When downloaded from the WEB, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the WEB.

4.2 Secure Areas, Security Zones and Electronic Security Perimeters

A secure area is a term used to secure a service both on site and in transport. Secure areas are setup in a manner that prevents propagation of a threat from one secure area to the next.

Segregation can be in the following:

1) Physical insulation – Systems can be isolated from each other physically. This can be done by having separate networks. A time delay of transfer of data can also be seen as physical insulation. If data was transferred from one network to another through a medium such as a hard disk, this can be seen as physical insulation.

2) Protocol insulation – Insulation can be accomplished with the use of a different communication language between networks and systems. A converter is required to enable different networks or systems from exchanging data.

3) Data insulation – Data can be isolated on a logical level. Data can be controlled and only authorised connections will allow data to pass such as firewall segregation. Physical equipment can be virtualised to create isolation such as virtual local area networks (VLANs).

In Eskom IT, a common practice to segregate data or cyber assets based on their security requirement is with one or more demilitarized security zones (DMZ). A security zone (DMZ) is a grouping of logical or physical assets that share common security requirements. This is commonly done with firewalls to create different security zones (DMZ's). A similar concept is applied in Eskom OT but is called an electronic security perimeter (ESP). An ESP is defined as the logical perimeter of the system. For a generic OT site, the ESP usually correlates with the physical security perimeter (PSP) of the site. Because of this definition, there may be further ESPs or security zones inside the main ESP.

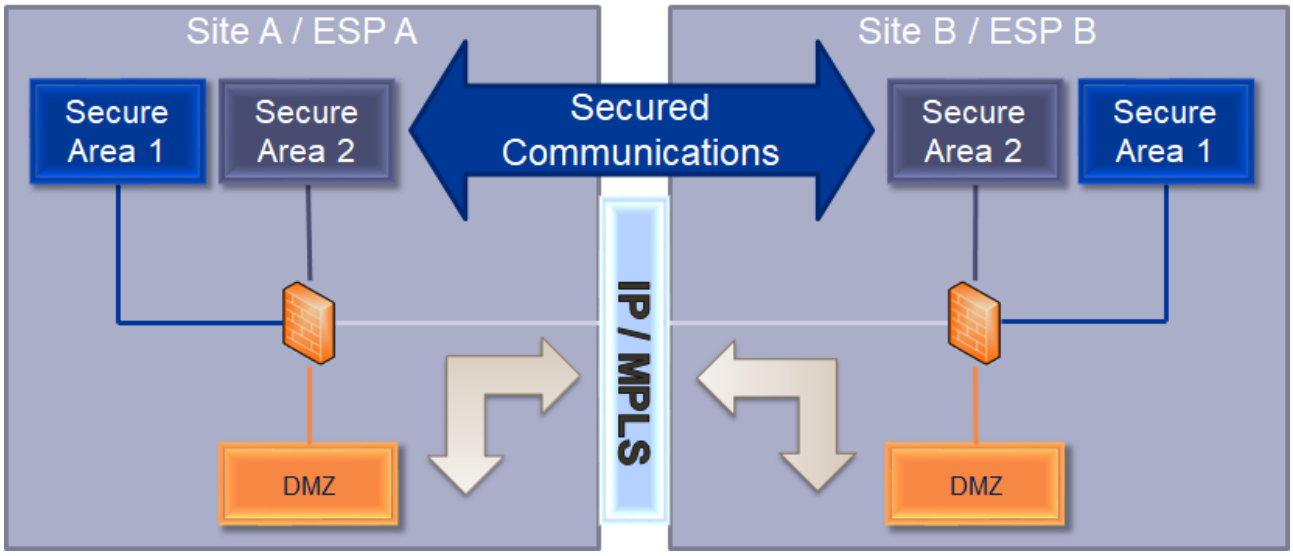

Figure 1: Security Zone / Electronic Security Perimeter and Secure Areas

Figure 1 shows how an ESP or security zone with DMZ integrates with a secure area. It is important to note that secure areas are not localised. Security zones can be seen as logical perimeters usually implemented with firewalls and other data segregation technologies. Data between two sites will hit a DMZ and then go to the allocated secure area. A secure area however, aims to secure the data flow. This means the source location; its travel paths and destination all make up the secure area for the data. The secure area therefore, allows segregated ESPs or security zones (DMZ's) to share information securely over an untrusted network. Encryption technologies (e.g. SSL\TLS\SFTP\VPN) can be used to further enhance the security of the communications over the untrusted networks.

ESKOM COPYRIGHT PROTECTED

When downloaded from the WEB, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the WEB.

5. Future ICT Network Security Framework

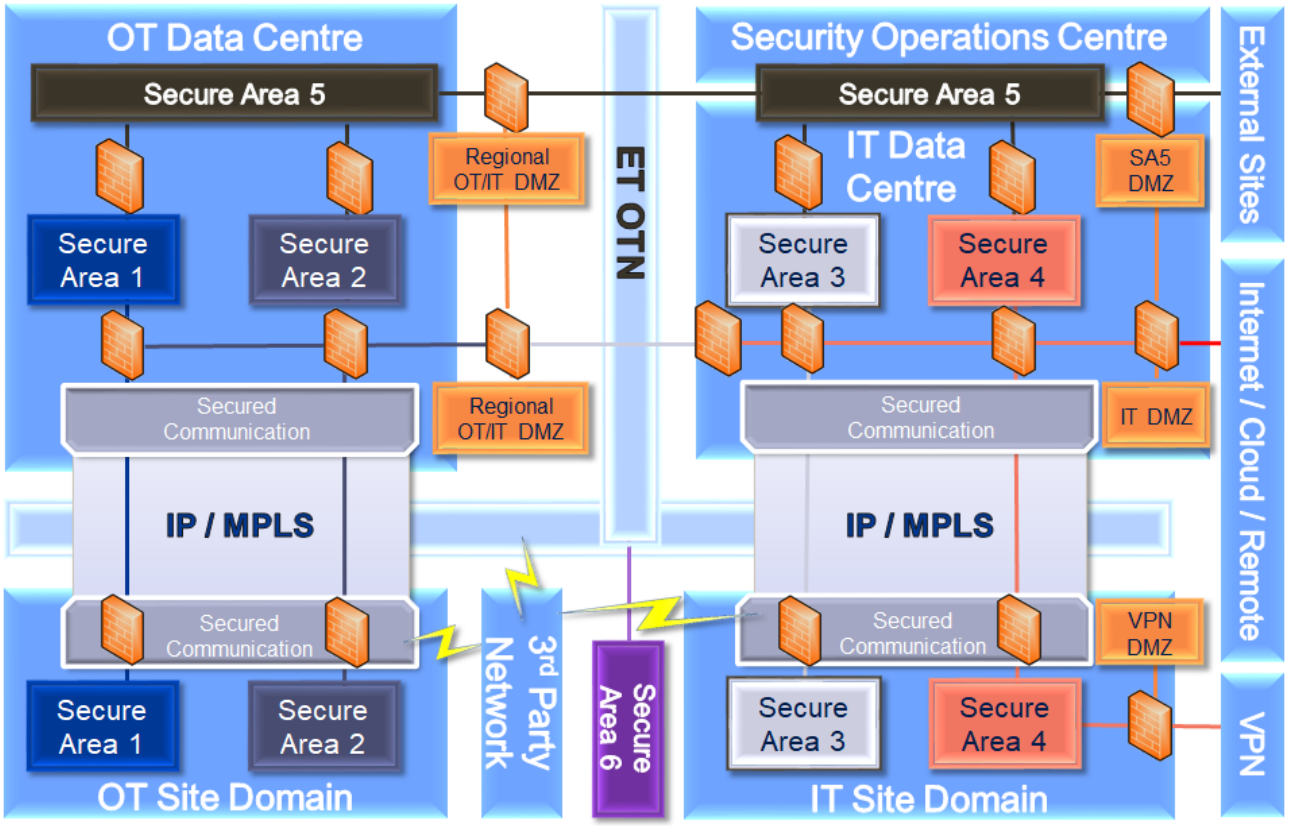

Figure 2: Future ICT Network Security Strategy Framework

Figure 2 above shows how the secure areas will be applied to secure the services of Eskom. Merging the OT environment with the IT environment allows for interconnectivity and to share resources across the business. This however, also opens the systems to vulnerabilities that could propagate from one area to another and hence the requirement for secure areas. The framework is to apply a defence-in-depth approach to exchanging data. Figure 2 above shows firewalls, which represent the use of a security insulation technique such as, but not limited to, firewalls. Next generation firewall enhancements like IPS, Application Control, AntiBot, Network Antivirus, URL Filtering etc. can increase the network security insulation.

The secure area should prevent propagation of threats from one secure area to another. The other advantage of having secure areas is different governance can occur in each area. This allows multiple entities (OT, IT) in the organisation to govern how data is respected in their domain.

5.1 Secure Areas Allocation

5.1.1 Operational Technology Areas (Area 1 and Area 2)

The OT environment can be broken down into two main groupings, this being a data centre or a site. Sites will report to a local, and if required, a national data centre. OT secure areas allow data to flow securely between sites and data centres.

ESKOM COPYRIGHT PROTECTED

When downloaded from the WEB, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the WEB.

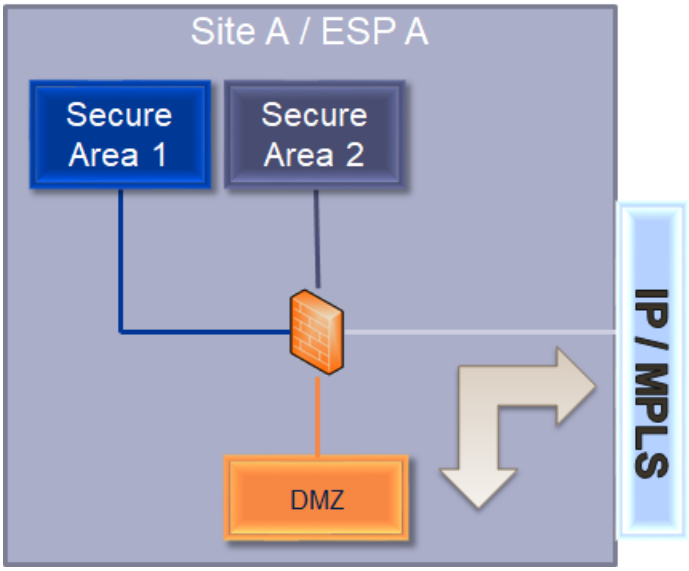

Figure 3: Logical Connection of Secure Area 1, Secure Area 2, Regional OT/IT DMZ and WAN.

Figure 3 above shows that data from the regional OT/IT demilitarized zone (DMZ) will either go to Secure Area 1 or Secure Area 2. The amount of firewalls will align to the DMZ Standard. The figure above is the recommended approach to protecting critical cyber assets (CCA).

5.1.2 Secure Area 1

Secure Area 1 will be segregated over OSI Layer 3 between sites providing a similar setup to Time Division Multiplexing (TDM). For services that are not ready for IP, TDM will be used to facilitate these communications until the transition to a TCP/IP service is reliable. Secure Area 1 is segregated from Secure Area 2 with a DMZ. It is important to note that a service attempting to get to Secure Area 1 (e.g. remote access) will not go through Secure Area 2 first but directly to Secure Area 1 (from jump server in DMZ to Secure Area 1).

5.1.3 Secure Area 2

Secure Area 2 will be segregated over layer 3 between sites. Most services that require connection outside the ESP of the site will reside here. Introducing Secure Area 2 will mitigate the risk of exposure to Critical Cyber Assets in the event of a cyber-breach occurring in this secure area.

5.1.4 Centralised Regional IT / OT Demilitarised Zone

A regional DMZ shall be used to bridge the IT and OT areas together. Having a central point ensures assurance that security is maintained in the flow of traffic between IT and OT. This allows greater use of financial and human resources to secure the DMZ. A high-level example is shown in Figure 4.

ESKOM COPYRIGHT PROTECTED

When downloaded from the WEB, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the WEB.

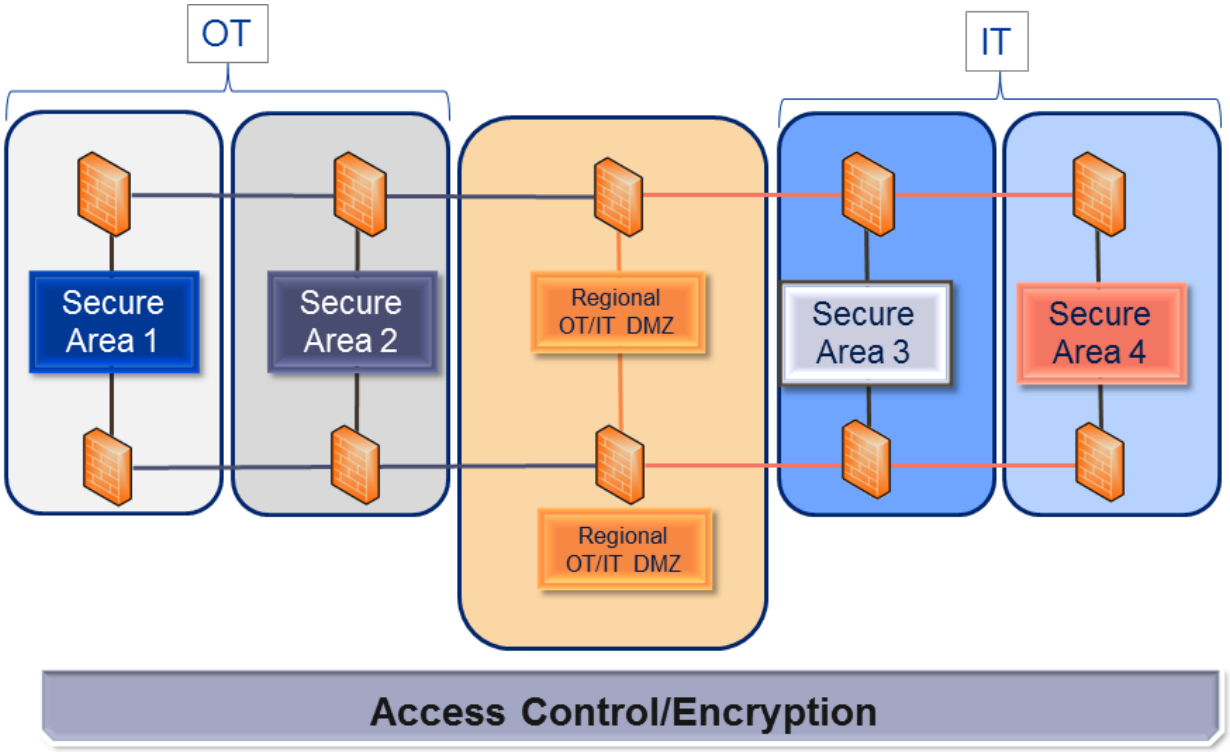

Figure 4: IT / OT exchanging data over a Central DMZ

5.2 Function and Purpose of Operational Technology Secure Areas

The OT area will be separated into two secure areas. One secure area will be designated for critical services and the other secure area for non-critical services. This will allow OT system owners to focus their efforts on securing critical cyber assets that are essential to their operations.

5.2.1 Secure Area 1 – Critical Operational Technology Services

Secure Area 1 is dedicated to services that directly impact the control, monitoring and operations of the power system. A dedicated secure area for control is essential to the reliable operation of the power network. Systems that meet the definition for an essential service will reside in secure area 1. The creation of secure area 1 will allow OT system owners to focus their efforts on protecting essential systems.

5.2.2 Secure Area 2 – Non-Critical Operational Technology Services

Secure Area 2 is dedicated to services that support the critical operational environment (Secure Area 1). Services that are hosted by OT but do not meet the essential services definition will reside in secure area 2.

5.3 Information Technology Secure Areas (Area 3 and Area 4)

The IT Network security environment should also cater for two areas, one to host OT Services and another for IT Services.

5.3.1 Secure Area 3 – Production Services

Secure Area 3 is dedicated for OT services hosted by IT. The reliance for OT on IT makes a requirement that OT hosted applications on IT systems be segregated from the rest of the IT enterprise network. The OT systems hosted by IT will follow an agreed upon governance between IT and OT. Secure Area 3 may also be used to host IT Services pertaining to the site requirements, these services should not be mixed with OT services.

ESKOM COPYRIGHT PROTECTED

When downloaded from the WEB, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the WEB.

5.3.2 Secure Area 4 – Enterprise Services

Secure Area 4 is dedicated to enterprise services maintained by IT that have no impact to OT operations. Enterprise services follow IT governance. OT governance has no influence to these systems. Secure Area 4 may comprise different service offerings, for e.g. Internet Access, VPN, etc.

5.4 Function of Information Technology Secure Areas

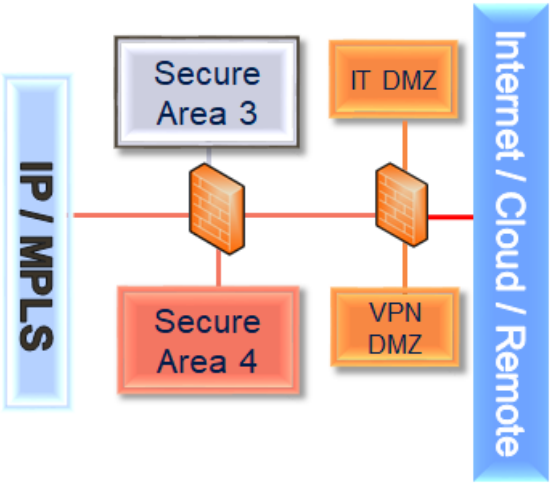

Figure 5: Logical Connection of the IT Secure Areas

Figure 5 show that when data enters the business, the data will go to the relevant secure area requesting that data. In cases such as a remote connection, once authenticated, will only be configured to go to the relative IT / OT DMZ.

5.4.1 Secure Area 3

Secure Area 3 will be segregated over layer 3 between sites. Important to note that all services have to pass through Secure Area 4 to get to Secure Area 3. This access is statically configured on all firewalls that the connection traverses.

5.4.2 Secure Area 4

Secure Area 4 will be segregated over layer 3 between sites. IT services will remain in the area unless it serves an operational purpose and then will move to higher secure area.

5.4.3 IT Segregation and Site VPN

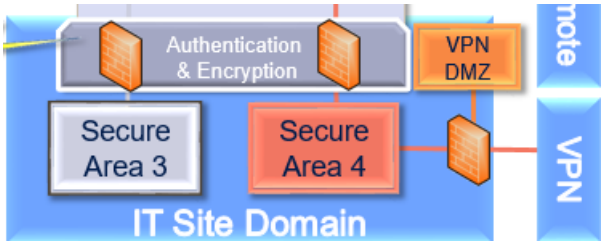

Figure 6: Information Technology Site-to-site Virtual Private Network

IT also segregates Secure Area 3 services from Secure Area 4 services. IT may also setup site-to-site VPNs where required. This is shown in Figure 6. If these sites require internet access, they will break out at the IT data centre, which is the central logical entrance of the Eskom business.

ESKOM COPYRIGHT PROTECTED

When downloaded from the WEB, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the WEB.

5.4.4 Information Technology Centralised Demilitarised Zone

The IT centralised DMZ will be the breaking in and out point for all communications to the internet. For OT services requiring internet and remote access, it is important that all communications go through this central point. This will allow other areas of the business to benefit from IT's security control measures for remote access.

5.5 Secure Area 5 – Integrated Security Operations Centre (ISOC)

Secure Area 5 is dedicated to services controlled by an Integrated Security Operations Centre (ISOC) Unit.

5.6 Function of Secure Area 5 – ISOC

Secure Area 5 will reside in both IT and OT environments. Security incidents will be fed from Secure Area 1-6 to Secure Area 5 directly. This information can have confidentiality rating or higher. Declassified information from Secure Area 5 will be shared back to the secure areas via their respective DMZ connections.

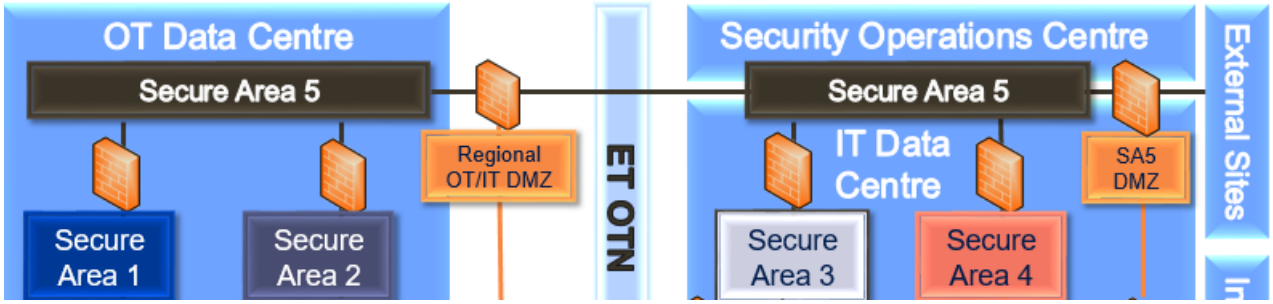

Figure 7: Secure Area 5

Secure Area 5 is reserved for the ISOC unit and shown in Figure 7. The unit will look at cyber and physical threats across the business by taking data sent by the different areas of the business and processing this to identify the threats.

The data sent from Secure Area 1 - 6 is of a highly sensitive nature. Declassified information is returned back to the relevant secure area and system owners can review the results.

Secure Area 5 also has communications to external sites referred to as trusted collaboration partner. These external sites are used in the collaboration of combating cyber threats which include but not limited to:

1) Agreed upon commitments with Cyber Response Committees.

2) Government organisation such as the South African Police Service.

This unit will deploy their own technology in the different domains to collect information securely and will have their own data centre.

Figure 8 shows the roll of the ISOC unit as an integrated security operations centre.

ESKOM COPYRIGHT PROTECTED

When downloaded from the WEB, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the WEB.

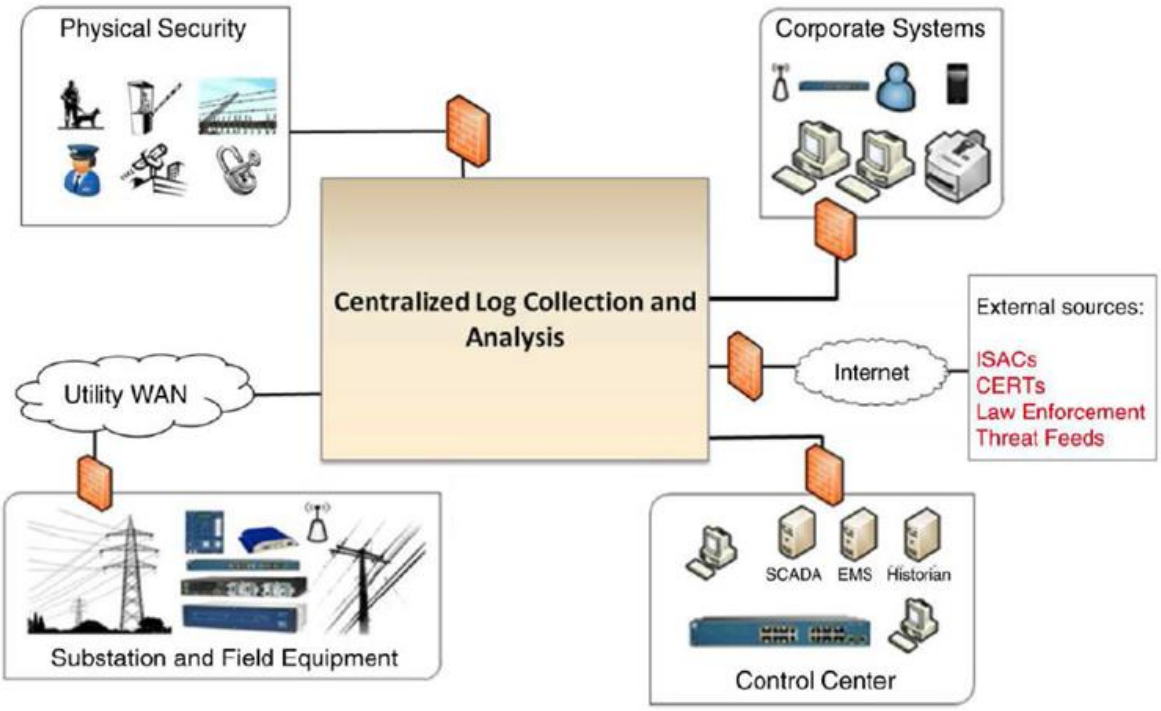

Figure 8: Guidelines for Planning an Integrated Security Operations Center, by G. Rasche, December 2013, EPRI

5.7 Secure Area 6 – External Service

Secure Area 6 is reserved for external services on the Eskom network.

5.8 Function of External Service – Area 6

In the event that Eskom would like to lease excess bandwidth, a secure area is established to accommodate the service. This secure area will only exist on the shared transport infrastructure and will not interact with the rest of the secure areas and thus, Eskom data.

5.9 Secure Area Attributes and Flow Diagram

Annex A shows a flow diagram to correctly allocate a service to a secure area based on its attributes.

Table 2 shows a summary of the attributes for each secure area.

ESKOM COPYRIGHT PROTECTED

When downloaded from the WEB, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the WEB.

Table 2: Secure Area Attributes

Attribute	Secure Area 1	Secure Area 2	Secure Area 3	Secure Area 4	Secure Area 5	Secure Area 6
Purpose	Critical network infrastructure (e.g. SCADA), monitoring and Protection. Critical work force enablement. Synchronisation Distribution.	Non-real time OT monitoring. Physical Security. Work force enablement.	OT systems hosted by IT.	Enterprise business systems.	Integrated Security Operations Centre (ISOC)	External Services
Confidentiality	Confidential (default)	Confidential (default)	Confidential (default)	Confidential (default)	Secret (default)	Confidential (default)
Data flow control between secure areas	All connections entering or leaving the secure area shall be through a DMZ. Data leaving the secure area must be pushed to a DMZ (unidirectional data flow). Data entering the secure area must come through a hardened jump server from the DMZ. Connections must be verified (e.g. multi-factor authentication) and monitored.	All connections entering or leaving the secure area shall be through a DMZ. Data entering the secure area must come through a jump server from the DMZ.	All connections entering or leaving the secure area shall be through a DMZ. Data entering the secure area must come through a jump server from the DMZ.	All connections entering or leaving the secure area shall be through a DMZ. Data entering the secure area must come through a jump server from the DMZ.	All connections entering or leaving the secure area shall be through a DMZ. Data leaving the secure area must be pushed to a DMZ (unidirectional data flow). Data entering the secure area must come through a hardened jump server from the DMZ. Connections must be verified (e.g. multi-factor authentication) monitored.	Data in this secure area shall not have connectivity with other secure areas.
Governance	OT	OT	IT and OT	IT	ISOC and supplemented with IT and OT.	IT and OT

ESKOM COPYRIGHT PROTECTED

When downloaded from the WEB, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the WEB.

Attribute	Secure Area 1	Secure Area 2	Secure Area 3	Secure Area 4	Secure Area 5	Secure Area 6
Connections between a secure area	Data in transport between this secure area shall be segregated from other data in a different secure area. Encryption and authentication should be applied where possible.	Data in transport between this secure area shall be segregated from other data in a different secure area.	Data in transport between this secure area shall be segregated from other data in a different secure area.	Data in transport between this secure area shall be segregated from other data in a different secure area.	Data in transport between this secure area shall be segregated from other data in a different secure area.	Data in transport between this secure area shall be segregated from other data in a different secure area. Encryption and authentication should be applied where possible.
Data storage	Data stored shall be segregated from other data in a different secure area.	Data stored shall be segregated from other data in a different secure area.	Data stored shall be segregated from other data in a different secure area.	Data stored shall be segregated from other data in a different secure area.	Data stored shall be segregated from other data in a different secure area.	Data stored shall be segregated from other data in a different secure area.
System Owner	OT system owner.	OT system owner	IT system owner	IT system owner	ISOC system owner	IT and OT system owners
Centralisation	Centralised OT service hosted by OT. Only centralise for OT. Cannot provide services for IT or ESD. Possible for centralised server of secure area 2 service to reside in secure area 1.	Possible to centralise non-essential services.	Centralised OT service hosted by IT. Service is provided for OT only.	Centralised IT service hosted by IT. Can provide service for entire business.	Centralised service hosted by Monitoring and Reporting Unit. Can provide service for entire business.	Possible to centralise non-essential services. Can provide service for entire business.
Third party networks	Third party networks should be avoided where possible.	Third party networks are acceptable.	Third party networks are acceptable.	Third party networks are acceptable.	Third party networks should be avoided where possible.	Third party networks should be avoided where possible, but may be acceptable depending on service requirements
*The confidential data classification may have more glandular categories (functional classes of data) pertaining to segregate medical, financial, engineering, etc. in the future of implementing this document.						

ESKOM COPYRIGHT PROTECTED

When downloaded from the WEB, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the WEB.

6. Authorization

This document has been seen and accepted by:

Name and surname	Designation
Phil Khumalo	General Manager Regions Distribution
Comfort Masike	Senior Manager National Control
Danie Du Plessis	Senior Manager Grids
Isabel Fick	Senior Manager Eskom Telecommunications
Karen Pillay	Senior Manager Security Solution (Physical)
Lloyd Chego	Senior Manager Security Solutions (Cyber)
Nhlanhla Tshabalala	Senior Manager ITSO TSG (Acting)
Prudence Madiba	Senior Manager Generation
Richard McCurrach	Senior Manager PTM&C
Sikelela Mkhabela	Senior Manager Distribution
Mmabatho Thipe	Middle Manager Information Security (Acting)
Mervin Mottian	Middle Manager Network Operations
Amelia Mtshali	Middle Manager PTM&C
Cornelius Naidoo	Middle Manager PTM&C
Deon Van Rooi	Middle Manager PTM&C
Nombuso Msibi	Middle Manager PTM&C
Steve Papadopoulos	Middle Manager PTM&C
Tony Sheerin	Middle Manager PTM&C
Anthea Solomon	Middle Manager Transmission Secondary Plant
Rob Stephen	SCOT Chairperson
Sham Dhrampal	IT/OT Chairperson
Thabo Mashegoane	Enterprise Architecture Board Chairperson
Sham Dhrampal	Enterprise Architecture Review Committee Chairperson
Lloyd Chego	Cybersecurity Committee Chairperson
Ezzard De Lange	Security Architecture Authority Chairperson
Prathaban Moodley	Smart Grid Study Committee Chairperson
Kgomotso Setlhapelo	Telecommunication Study Committee Chairperson
Marlini Sukhnandan	Telecontrol Study Committee Chairperson
Andre De La Guerre	PTM&C Design and Review Team Chairperson
Reshin Moodley	Cybersecurity Care Group Chairperson
Tejin Gosai	Teleprotection Care Group Chairperson

ESKOM COPYRIGHT PROTECTED

When downloaded from the WEB, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the WEB.

7. Revisions

Date	Rev	Compiler	Remarks
Jan 2020	1	M Taljaard	Final Document for Authorisation and Publication

8. Development team

The following people were involved in the development of this document:

- Matthew Taljaard
- Sarish Amrithlall
- Vanessa Naidu
- Kgomotso Setlhapelo
- Tejin Gosai
- Ziyaad Gydien
- Bongani Shezi
- Cornelius Naidoo
- Zwelandile Mbebe
- Dan Panday
- Beresford Jelliman
- Simon Higgins
- Craig Boesack
- Ken Hales
- Mahendra Balipursad
- Rishi Hariram
- Billy Petzer
- Michelle Govender

9. Acknowledgements

This document is supported by the following committees:

- Enterprise Architecture Board Committee
- Enterprise Architecture Review
- Cybersecurity Committee
- ET Engineering Forum
- IT/OT Collaboration Committee
- PTM&C Design Review Team
- SCOT Committee
- Security Architecture Authority
- Smart Grid Study Committee
- Telecommunication Study Committee
- Cybersecurity Care Group

ESKOM COPYRIGHT PROTECTED

When downloaded from the WEB, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the WEB.

- Telecontrol Study Committee
- Teleprotection Care Group

ESKOM COPYRIGHT PROTECTED

When downloaded from the WEB, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the WEB.

Annex A – Secure Area Attributes

Definition Based on Attributes

Secure Area 1	Service that is essential to the operations of Eskom's core business (OT) that affects a single or decentralized portion of the operations Network.
Secure Area 2	Service that is not essential to the operations of Eskom's core business (OT) that affects a single or decentralized portion of the operations Network.
Secure Area 3	Service that is not essential to the operations of Eskom's core business (OT) that can be centralized and hosted in the IT environment.
Secure Area 4	Service that is not part of Eskom's core business (OT) but provides corporate information processing to enhance the efficiency of the business (IT).
Secure Area 5	Service that provides centralised cyber or physical security technology services on behalf of the business.
Secure Area 6	Services that are external to Eskom that shares the same physical transport infrastructure as internal Eskom data.

Figure A.1: Definition for Secure Areas Based on Attributes

ESKOM COPYRIGHT PROTECTED

When downloaded from the WEB, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the WEB.

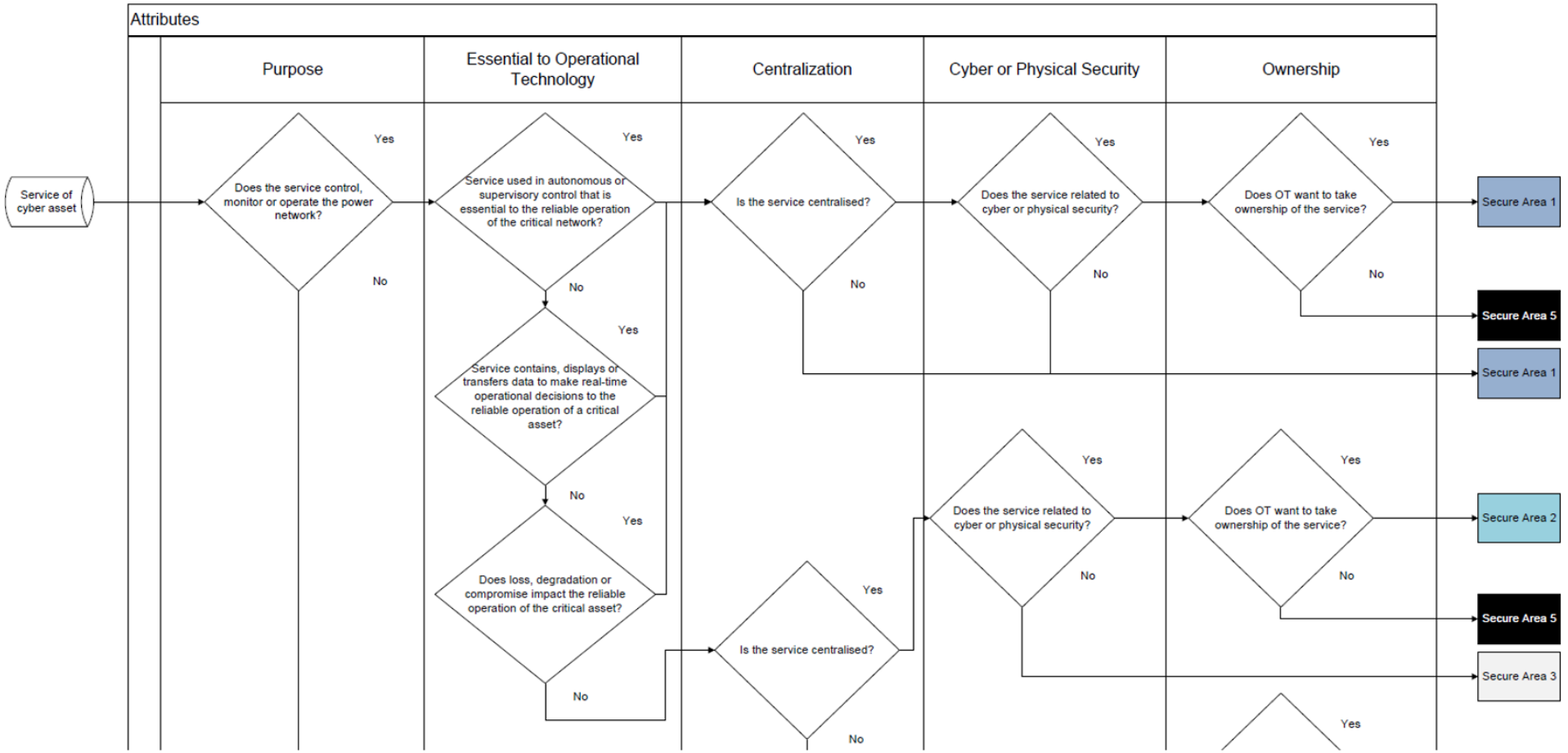

Figure A.2: Secure Area Attribute Flow Diagram (part 1 of 3)

ESKOM COPYRIGHT PROTECTED

When downloaded from the WEB, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the WEB.

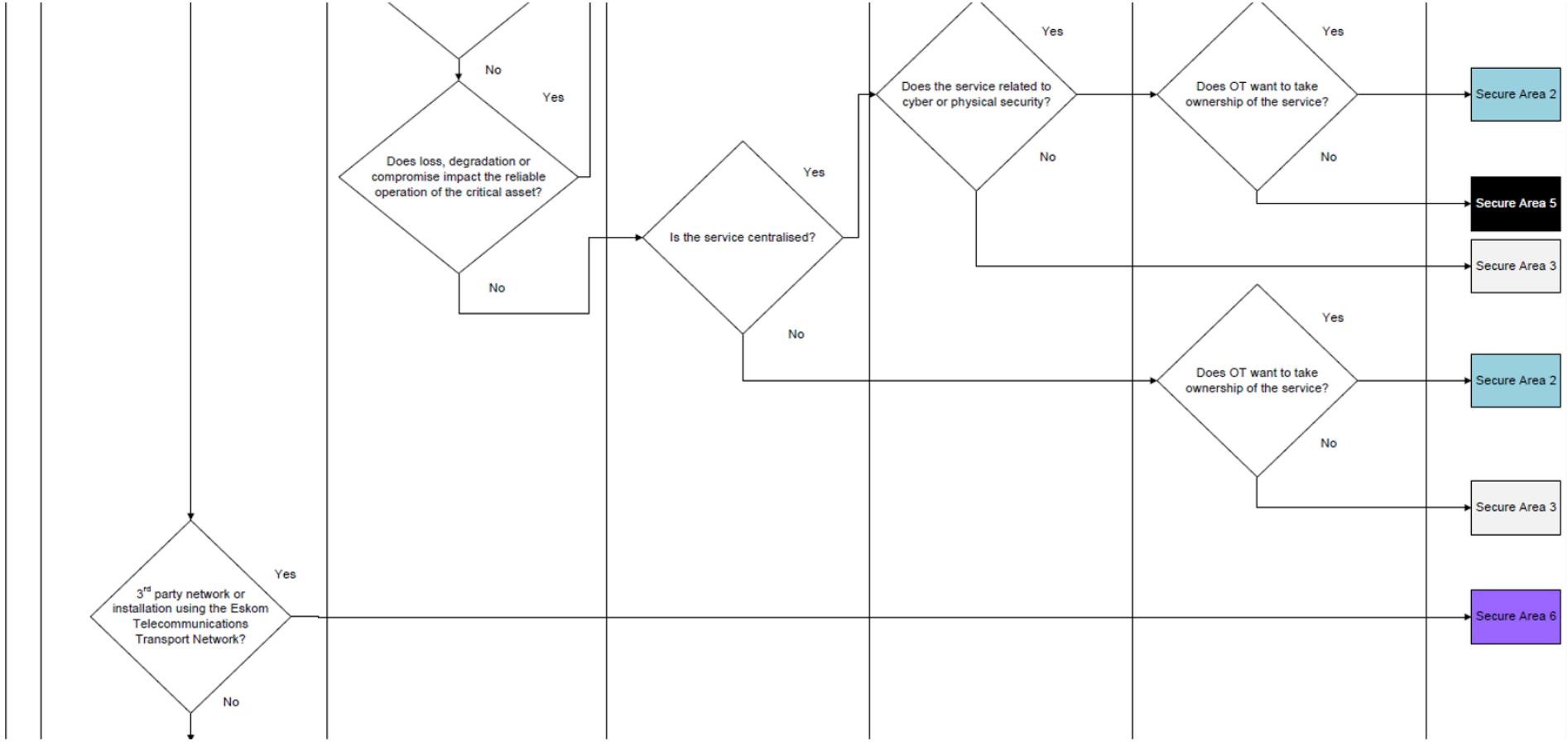

Figure A.3: Secure Area Attribute Flow Diagram (part 2 of 3)

ESKOM COPYRIGHT PROTECTED

When downloaded from the WEB, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the WEB.

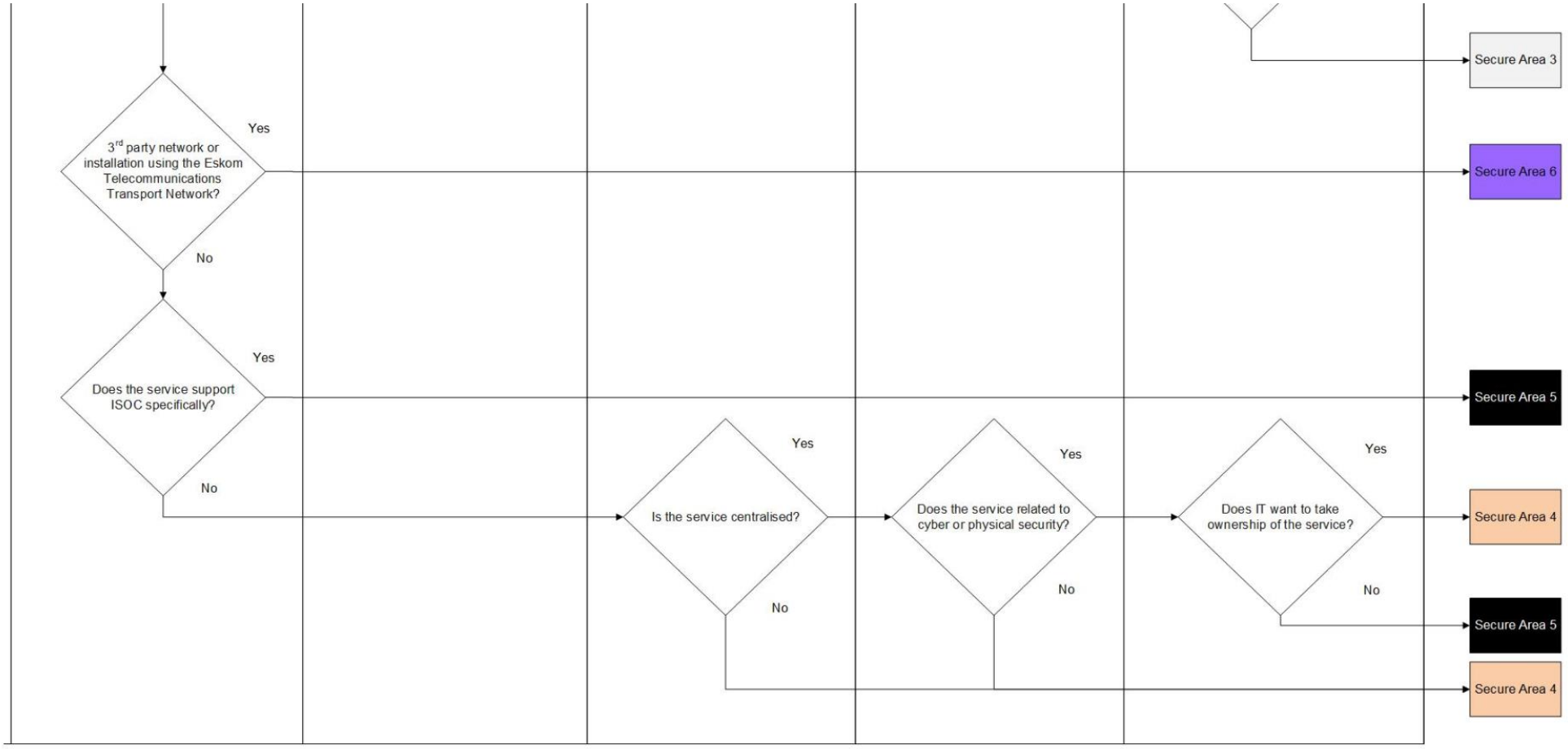

Figure A.4: Secure Area Attribute Flow Diagram (part 3 of 3)

ESKOM COPYRIGHT PROTECTED

When downloaded from the WEB, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the WEB.