

 Eskom	<b>Logical Architecture Definition for a Physical Application Component</b>	<b>Group IT</b>
---	---	-----------------

Title: **LAD PAC for Physical Security Information Management System (PSIM)**
 Unique Identifier: DEM2412993 & 2425114  
 Project Identifier:  
 Area of Applicability: **Eskom**  
 Documentation Type: **SP**  
 Disclosure Classification: **CONTROLLED DISCLOSURE**

### Project Stage Review

Lifecycle Phase	Lifecycle Stage	Stage Gate (after stage)	Deliverable	Appropriate Lifecycle Stage
<b>Pre-Project Planning</b>	Define Need		Project Statement of Work	
	Project Context	CRA	Statement of Architecture Work	
<b>Concept</b>	Feasibility			
	Concept Design	DRA	Conceptual Architecture Definition	
<b>Definition</b>	Logical (Basic) Design	ERA	Logical Architecture Definition	✓
<b>Execution</b>	Physical (Detailed) Design	IRA	Detailed Design	

**Compiled By**



.....  
**SJ Solomon**  
**Lead Architect**

Date: 11/14/20

**Approved By**



**P Nkosi**  
**ADR Chairman**  
 (A Fath - standing in for Patrick)

# Table of Contents

1. INTRODUCTION .....	4
2. SUPPORTING CLAUSES .....	4
2.1. SCOPE .....	4
2.2. APPLICABILITY .....	4
2.3. NORMATIVE / INFORMATIVE REFERENCES .....	4
2.3.1. Normative .....	4
2.3.2. Informative .....	4
3. SCOPE AND CONTEXT OF ARCHITECTURE DESIGN .....	5
3.1. WORK PACKAGE .....	5
3.1.1. Work Package Description .....	5
3.1.2. Work Package Rationale .....	5
3.2. WORK PACKAGE CATALOG .....	6
3.2.1. Target Work Package Catalog .....	6
3.3. REQUIREMENTS, CONSTRAINTS AND ASSUMPTIONS .....	7
3.3.1. Target Requirement Catalog .....	8
3.4. SECURITY ARCHITECTURE .....	15
3.5. RISKS AND ISSUES .....	16
3.5.1. Target Risk Catalog .....	16
4. PHYSICAL APPLICATION COMPONENT DESCRIPTION .....	17
5. APPLICATION ARCHITECTURE .....	20
5.1. APPLICATION ARCHITECTURE LANDSCAPE CONTEXT .....	20
5.1.1. Target Application Portfolio Catalog .....	20
5.2. APPLICATION INTERFACE CONTEXT .....	21
5.2.1. Target Application Communication Diagram .....	21
5.2.2. Target Application .....	23
5.3. APPLICATION STAKEHOLDERS .....	23
5.3.1. Target Stakeholder Analysis Diagram .....	23
5.4. INFORMATION SYSTEM/APPLICATION FUNCTIONS .....	24
5.4.1. Target Application Function Decomposition .....	24
6. DATA & INFORMATION ARCHITECTURE .....	27
6.1. LOGICAL DATA & INFORMATION .....	27
6.1.1. Target Data Catalog .....	27
7. TECHNOLOGY ARCHITECTURE .....	32
7.1. TECHNOLOGY SERVICES AND LOGICAL / PHYSICAL TECHNOLOGY COMPONENTS .....	32
7.1.1. Target Technology Portfolio Catalog .....	32
7.2. USER LOCATIONS .....	41
7.2.1. Target Application User Location Diagram .....	41
8. DELIVERABLE ACCEPTANCE .....	42

8.1. DOCUMENT GENERATED .....	42
8.2. SUPPORTING MODELS .....	42
8.3. ACCEPTANCE .....	43
9. APPENDIX .....	44
9.1. DEFINITIONS.....	44
9.2. ABBREVIATIONS.....	44
9.3. SYMBOL REFERENCE SHEET .....	46
10. INDEX .....	47
10.1. LIST OF FIGURES .....	47
10.2. LIST OF TABLES .....	47

## 1. INTRODUCTION

This Logical Architecture Definition for a Physical Application Component (LAD PAC) describes the logical design for the "Physical Security Information Management System (PSIM)" physical application component from an IT architecture perspective and will provide the foundation from which more detail designs can be applied. It presents a qualitative view of the solution and aims to communicate the design intent. This logical design definition generates the submission document for architecture review at the end of the logical design-stage.

The LAD PAC spans all relevant architecture domains (business, data & information, application and technology) and also examines all relevant states of the architecture (baseline, transition, and target).

The LAD PAC could contain content that is on a physical level of detail where it is needed for context purposes.

The content of the LAD PAC document is based on the TOGAF® Architecture Development Method (ADM). It is primarily documented using the standard modelling tool (ARIS) as a mechanism to capture the architecture content which is then output to this document.

## 2. SUPPORTING CLAUSES

### 2.1. SCOPE

This document scope covers the following:

- Applicability, normative/informative references, definitions, abbreviations and supporting documentation of this document
- Scope and context of architecture development work
- Architecture designs for the physical application component

### 2.2. APPLICABILITY

This document shall apply throughout Eskom Holdings Limited Divisions.

### 2.3. NORMATIVE / INFORMATIVE REFERENCES

#### 2.3.1. Normative

Normative documents that are indispensable for the application of this document are listed below:

List of References
Business Requirement Specification (BRS)
Statement of Architecture Work
Specification for integrated access control system (ACS) for Eskom Sites
Specification for CCTV Surveillance with Intruder Detection
Non-lethal fence
Integrated Security Alarm systems
Physical Security Integrated Standard

#### 2.3.2. Informative

1. Open Group Standard, TOGAF® Version 9.1.
2. 206-1461 Recipe - Statement of Architecture Work
3. 206-1462 Recipe - Conceptual Architecture Definition of an Application
4. 206-1513 Recipe - Logical Architecture Definition of an Application
5. 206-1630 Recipe - Logical Architecture Definition of a Data Interface
6. 206-1241 TOGAF® Architecture Content Framework
7. 206-1443 TOGAF® Content Metamodel

### **3. SCOPE AND CONTEXT OF ARCHITECTURE DESIGN**

The work package identifies the complete scope of architecture work necessary to realise the target architecture required by the Project Statement of Work and is shown in context of the portfolio of work packages.

#### **3.1. WORK PACKAGE**

##### **3.1.1. Work Package Description**

The aim of the required security monitoring solution is

1. To assess the security vulnerabilities of Eskom assets to physical security risks and to reduce these vulnerabilities to acceptable levels;
2. To empower the business to proactively predict and respond to physical security incidents;
3. To address the existing inadequate physical access control and CCTV systems, respectively through the availability of security incident logs and CCTV footages;
4. To assist the business to conduct comprehensive security incident investigations related to logged security breach occurrences;
5. To assist to mitigate against the significant increases in theft and vandalism at the various Eskom Telecommunications and Transmission sites, respectively where criminals have targeted and stolen copper cables, batteries and chargers

The design of the upgrade or replacement of the physical security systems will align to the desired level of physical security to provide protection against the identified risks.

Will be deployed in phases with a pilot site first then the same design will be rolled out to further sites once implemented successfully at the pilot site.

##### **3.1.2. Work Package Rationale**

The current business challenges / issues that need to be addressed are as follows -


1. Recently, concerns regarding Eskom's resilience to physical security threats became apparent.
2. Annual audits and assessments on physical security infrastructure, shows a clear deterioration.
3. The increasing high demand for non-ferrous metals has highlighted the vulnerability of Eskom infrastructure and facilities to vandalism and theft.
4. Increases in barrier intrusions have proven that current barriers are inadequate.
5. The existing barriers and perimeter lighting have mostly reached the end of their life span.
6. Inadequate physical access control and CCTV (Closed Circuit Television) systems resulted in incident logs and CCTV footage evidence being unavailable to assist in conducting incident investigations post the occurrence of physical security incidences. For example, at the Pieter both substation in the Central Grid, an employee died at the Eskom substation. However, not tracking physical access resulted in incident logs and CCTV evidence being available to assist the investigation. This resulted in a delay in concluding the incident investigation process due to a lack of information regarding the incident.
7. The physical location of substations makes substations vulnerable to criminal activities.
8. The lack of adequate physical security systems and measures poses a risk to security guards and employees, as they do not provide sufficient first line of defense.
9. Minimal refurbishment and replacement of physical security infrastructure over the past 25 years resulted in significant occurrences of physical security incidents.
10. Lack of an integrated physical security system across Eskom, which limits the collaboration of physical security systems to minimise physical security threats across the organisation.
11. Significant retrofitting of security capabilities, which results in excessive costs.

12. Lack of physical security standardization across the organization, which results in misaligned physical security designs that potentially contradict the approved physical security standards.
13. Ineffective physical security monitoring and response capabilities across the organization.
14. Lack of maintenance and support for physical security systems.
15. The current physical security systems neither mitigate the on-going challenges of prevailing physical security threats, nor meet Eskom's statutory obligations as determined by the security threat and risk assessments.
16. In order to protect the critical Eskom infrastructure, the business seeks to pursue initiatives that will effectively manage risks affecting the critical Eskom infrastructure by adopting a technical, methodical and systematic approach to physical security.
17. This necessitates the need for Eskom to become more resilient to physical security threats by upgrading or replacing its existing physical security infrastructure to the same level of pervasiveness as the challenging physical security threats against its infrastructure.
18. A physical security infrastructure upgrade or replacement will positively contribute to both operational efficiency and realize financial savings for the organization.
19. This project carries the support of the OHS (Occupational Health and Safety) act, which is a legal compliance requirement for the safety of the Eskom employees and contractors.

### 3.2. WORK PACKAGE CATALOG

The work package structure in the diagram below identifies the included work packages of this architecture definition and that are necessary to realize the target architecture required by the Project Statement of Work. The identified work package is shown in context of the portfolio of work packages.

#### 3.2.1. Target Work Package Catalog

Name: DEV_D1_Tx & ET Security Monitoring System_Target_202008_V01  Type: Work package catalog Identifier: STD.25899894	Date review requested: 28 Feb 2014 Date of Next Revision: 28 Feb 2014 Date of Authorisation: 28 Feb 2014 QA Date: 10 Sep 2014 2:19:01 PM QA Status: Not Passed	Creator: system Time of generation: 12 Aug 2020 9:02:01 AM Last user: moatshh Last change: 31 Aug 2020 3:56:25 PM	 ARIS Model
---	--	--	---



**Figure 1: DEV\_D1\_Tx & ET Security Monitoring System\_Target\_202008\_V01 [Work Package Catalog]**

**Table 1: Work Package Descriptions**


Name	Description
Tx & ET Security Monitoring System	The aim of the required security monitoring solution is <ol style="list-style-type: none"> <li>1. to assess the security vulnerabilities of Eskom assets to physical security risks and to reduce these vulnerabilities to acceptable levels;</li> <li>2. to empower the business to proactively predict and respond to physical security incidents;</li> </ol>

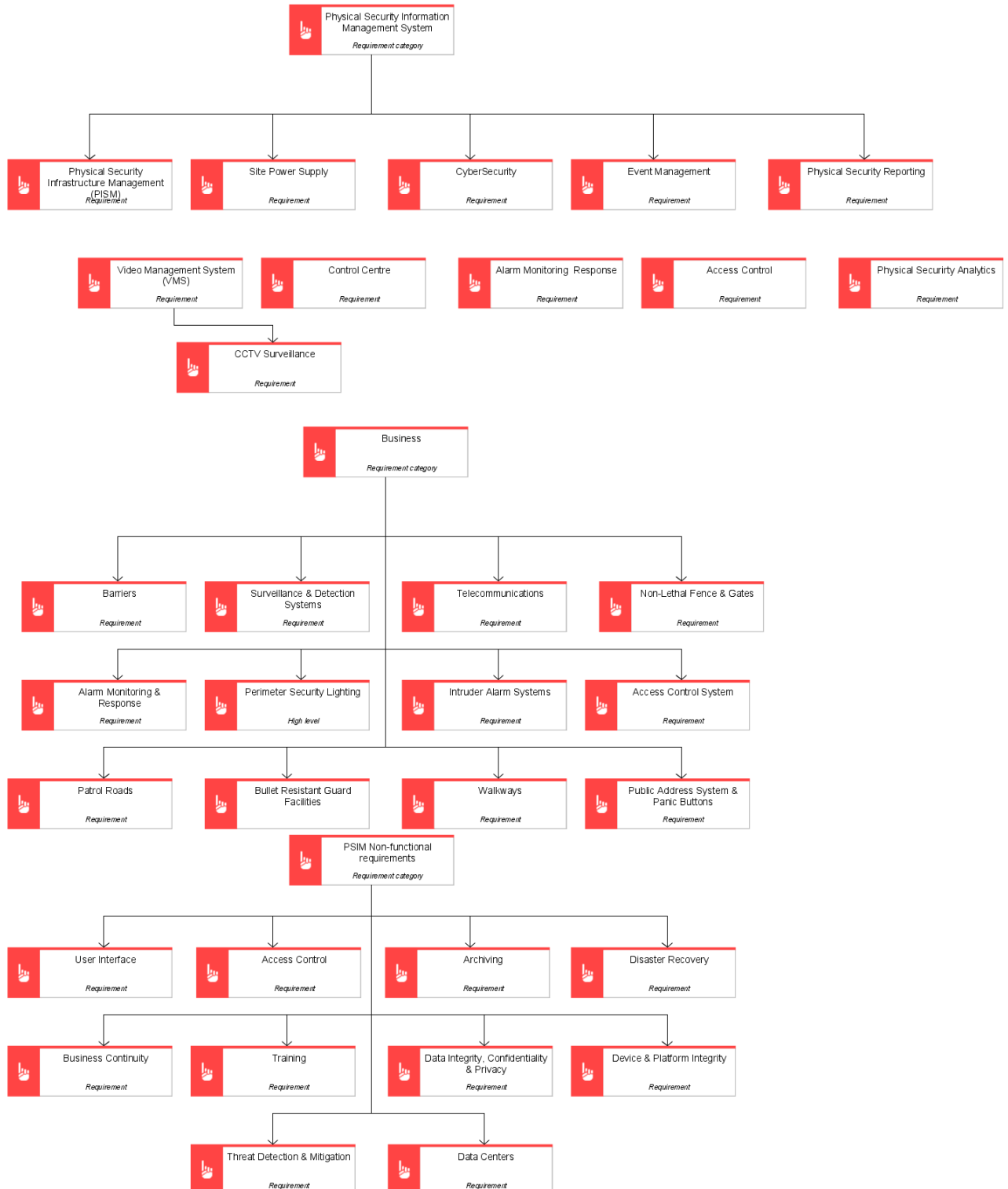
Name	Description
	<p>3. to address the existing inadequate physical access control and CCTV systems, respectively through the availability of security incident logs and CCTV footages;</p> <p>4. to assist the business to conduct comprehensive security incident investigations related to logged security breach occurrences;</p> <p>5. to assist to mitigate against the significant increases in theft and vandalism at the various Eskom Telecommunications and Transmission sites, respectively where criminals have targeted and stolen copper cables, batteries and chargers; and</p> <p>The design of the upgrade or replacement of the physical security systems will align to the desired level of physical security to provide protection against the identified risks.</p> <p>Will be deployed in phases with a pilot site first then the same design will be rolled out to further sites once implemented successfully at the pilot site.</p>

### 3.3. REQUIREMENTS, CONSTRAINTS AND ASSUMPTIONS

The requirements are quantitative statements of business needs that are to be fulfilled by the architecture design. Constraints and assumptions, which by their very nature are beyond the control of the enterprise, can produce changes in these requirements in an unforeseen manner. The requirements, constraints and assumptions are represented in the requirements catalog.

### 3.3.1. Target Requirement Catalog

Name: DEV_D1_Tx & ET Security Monitoring System_Target_202008_V01		Creator: system Time of generation: 12 Aug 2020 9:02:01 AM Last user: solomosj Last change: 10 Nov 2020 12:33:30 PM	 ARIS Model
Type: Requirement catalog Identifier: STD.25899896	QA Date: 10 Jul 2014 1:02:21 PM QA Status: Passed		



**Figure 2: DEV\_D1\_Tx & ET Security Monitoring System\_Target\_202008\_V01 [Requirement Catalog]**



**Table 3: Requirement Descriptions**

Name	Description	Requirement Priority
Access Control	<p>* The fundamental element of access control is to have strong identity mechanisms for all grid elements—users, devices and applications. * It is equally important to perform mutual authentication of both nodes involved in the communications for it to be considered secure. * The FAR (false acceptance rate) should have a X.509-based digital certificate that can be used to bootstrap the device and install our own digital certificate. * Such an identity forms the basis of AAA (Authentication, Authorization and Accounting) services performed by the router with other entities, i.e. aggregation routers, network management systems and authentication servers. * . It is recommended to use an X.509 certificate-based identity for the Security Endpoints / Devices as it is secure for authentication and scalable cryptographic key management. * . Strong authentication of nodes can be achieved by taking full advantage of a set of open standards such as IEEE 802.1x, EAP (Extensible Authentication Protocol) and RADIUS. * Every Security Endpoint / Device and remote worker joining the mesh network should be authenticated before being allowed access to the network (the technician's credentials could be a username and password or a X.509 digital certificate). * The FARs pass on the Security Endpoint / Device's credentials to the centralized AAA server.</p>	High
Access Control System	<p>1. Controlling access to buildings, facilities and sites via the IACS (Integrated Access Control System). Deploy MFA (Multi-Factor Authentication) and Certificate-based authentication. Refer to Section 13 for the IACS specification. 2. Obtain approval from the Grid in line with HV (High Voltage) Regulations for access to any Eskom Transmission or Eskom Telecommunications sites.</p>	High
Alarm Monitoring & Response	<p>1. Detected alarms at the Control Centres are necessary to support the response plan and action by the security operators. 2. Mimic panels with demarcated zones need to be available in guardhouses for guards to respond to the exact location of the alarms. 3. Send Eskom Telecommunication site alarms to Zero Control and NMC (Network Management Center) to alert them of events and incidents. 4. Send alert SMS's to the relevant security response teams when security incidents occur. 5. If it is a positive intrusion, the controller will deploy the armed response company to respond to the security alarms. Zero control will contact armed response company. 6. Provide feedback to the security control centre to inform them of workflow progress. 7. Armed response contracts to be established.</p>	High
Archiving	<p>The solution needs to adhere to the Standard for records retention periods. Refer to Section 13 details CCTV Footage minimum archiving requirements: * Video streams shall be stored for a minimum of 32 days, irrespective of size. * Alarm archives shall be</p>	High

Name	Description	Requirement Priority
	stored for a minimum of 5 years. * All video stream data shall be time and data stamped via a central Eskom server. * Alarm archives shall be stored for a minimum of 5 years	
Barriers	The outer barrier security measures shall comprise of: 1. A concrete wall with an intrusion detection system; or 2. A high tensile steel fence with an intrusion detection system. 3. Outer barriers to consist of a concrete anti-tunneling feature. 4. Double v overhang with razor coils. 5. The inner barrier security measures shall comprise of: 6. An inner fence consisting of welded mesh. 7. Single overhang.	High
Bullet Resistant Guard Facilities	Eskom Transmission Substations shall have a permanent guardhouse/ security control room built close to the entrance to the primary entry point to the substation. The guardhouse / security control room will be equipped with the following: 1. Kitchen. 2. Ablution facilities. 3. Equipment room. 4. Mimic panels. 5. Bulletproof windows. 6. Hardened doors. 7. Air conditioning for the equipment. 8. Panic buttons. 9. Firearm safe. The Firearm safe shall integrate to the Eskom Arsenal Register. 10. Firearm safe making area (bullet catch).	High
Business Continuity	By implementing as a minimum of a Production environment with DR as a fail-over, would imply that BCP is addressed.	
Control Centre	1. To function as a nerve centre with monitoring, analysis and control functions. 2. To maintain, sustain and improve reliable security operations effectively. 3. Serve Eskom Transmission and Eskom Telecommunication's sites. 4. Shall be self-sufficient regarding services (i.e. backup power and HVAC). 5. Shall present site-relevant information in a GIS (Geographical Information System) format to enhance situational awareness. 6. The PSIM shall manage the information flow between the security control centre and its associated physical security systems. 7. Different SCC's (Security Control Centres) will exist, i.e. RSCCs (Regional Security Control Centres) and NSCCs (National Security Control Centres). 8. These Control Centres will make use of Eskom-owned Data Centre Facilities and connect via Eskom-owned Telecommunications infrastructure. 9. The SCCs will be responsible for monitoring and responding to its own site occurrences and incidents as well as generate notifications and alarms. The Security control centre shall have the following general functional requirements: 1. Responsible for monitoring access control to the sites. 2. Classify incidents, apply the appropriate response and create alarms and notifications. 3. Manage incident response and escalate to the level of response needed. 4. Continuous monitoring of site perimeters. 5. Monitor general surveillance and anti-tampering/ sabotage observations. 6. Control of PTZ cameras to verify an incident as being a nuisance alarm or a real threat. 7. Monitor of all detection incidents. 8. Use the PA system to deter any threat. 9. Investigate user security	High

Name	Description	Requirement Priority
	profiles and behaviours. 10. Respond to emergency/ evacuation notifications. 11. Maintain the ELB (Electronic Incident Logbook) continuously during a shift handover and generate daily/ weekly reports. 12. Support regulatory compliance in all spheres of the Eskom business.	
CyberSecurity	1. Segregate/ separate the security data from the conventional OT (Operational Technology) and IT (Information Technology) data; ideally physical segregation, where security has its own physical communication infrastructure and security DMZ (Demilitarised Zone) is recommended. 2. Certificate-based authentication supported by an Eskom HSM (Hardware Security Module). 3. Eskom-owned Data Centre facilities to house the physical security management platforms.	High
Data Centers	PSIM will be housed in an Eskom-owned Data Centre which will form part of the Core Data Network	High
Data Integrity, Confidentiality & Privacy	<p>* Consistency - There must be no differences in data between users i.e. If a number of users request the same data, there should be no discrepancy from user to user. * Completeness of information is vital to ensure proper investigation of incidents. * Accuracy of data is vital to assist the business to make informed decisions based on the availability of data. * The systems should deliver the data in real-time (performance) * The FAN (Field Area Network) should ensure data integrity and confidentiality for data from the Security Endpoint / Devices when it traverses the public or private WAN (Wide Area Network) * Data confidentiality uses encryption mechanisms available at various layers of the communication stack, e.g. an IPv6 node in the last mile can encrypt data using AES (Advanced Encryption Standard) at:</p> <ul style="list-style-type: none"> <li>* 1. Layer 2 (IEEE (Institute of Electrical and Electronics Engineers) 802.15.4g or IEEE P1901.2)</li> <li>2. Layer 3 IPsec (IP Security)</li> <li>3. Layer 4 DTLS (Datagram Transport Layer Settings)</li> <li>4. Layer 7 (ANSI C12.22 or DLMS (Device Language Messaging Specification)/COSEM (Companion Specification for Energy Metering))</li> </ul> <p>* IPsec ensures data integrity and confidentiality for all traffic (can even have site-site VPN between the FAR (False Acceptance Rate) and the WAN). * It is recommended to use network-layer encryption (AES with IPsec) in the WAN and link-layer encryption in the mesh (AES on IEEE 802.15.4g or IEEE P1901.2). * This design provides network visibility into the traffic at the FAR and helps enables the use of IP-based techniques of multicast, network segmentation and QoS (Quality of Service). * It also allows the Security Endpoint / Device to only perform link-layer encryption while the FAR does both L2 and L3. * L2 and L3 encryption can be supplemented by use of L7 techniques that verify message integrity and proof of origin (digitally signed firmware images or digitally signed commands as part of C12.22 or DLMS/COSEM).</p>	High

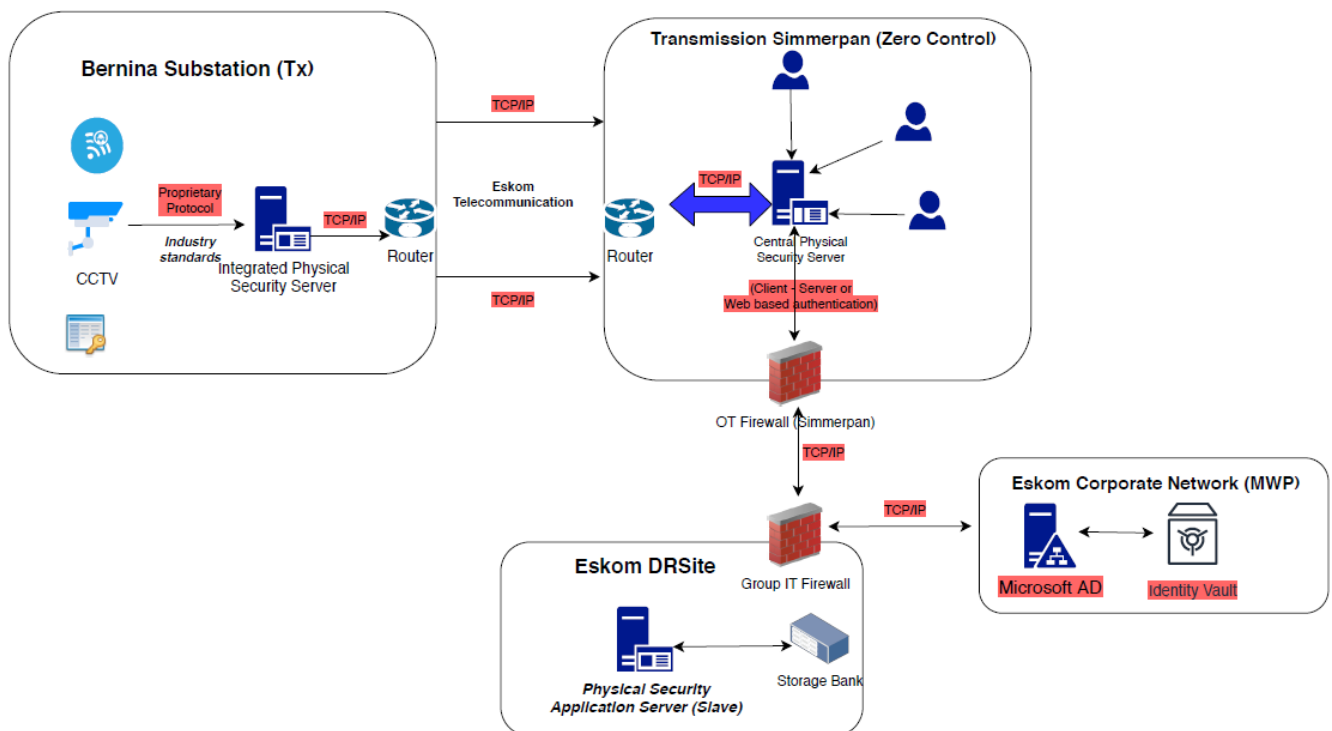
Name	Description	Requirement Priority
Device & Platform Integrity	<p>* A basic tenet of security design is to ensure that devices, endpoints, and applications cannot be compromised easily and are resistant to cyber-attacks.</p> <p>* The routers we choose should therefore be tamper-resistant mechanical designs and use IE (Industrial Ethernet).</p> <p>* Routers should even have if possible a physical lock and key mechanism as well as be ruggedized where necessary.</p> <p>* This makes it extremely difficult for any rogue entity to open or uninstall the device.</p> <p>* Platforms should generate software and NMS alerts if the router door or chassis is opened.</p> <p>* Additionally, each router motherboard should be equipped with a dedicated security chip where possible that provides:</p> <ol style="list-style-type: none"> <li>1. Secure unique device identifier (802.1AR)</li> <li>2. Immutable identity and certifiable cryptography</li> <li>3. Entropy source with true randomisation</li> <li>4. Memory protection and image signing and validation</li> <li>5. Tamper-proof secure storage of configuration and data</li> </ol>	High
Disaster Recovery	<p>* This depends on who will be responsible for implementing, operating and maintaining the physical technology platforms, i.e. it could be either Tx or ET or GIT. The business requires both "Production" and "Disaster Recovery" (DR) environments, respectively and/ or a "High-Availability" configuration.</p> <p>* Traditionally GIT run Production and DR as a backup, but the future is High-Availability configurations.</p> <p>* New Simmerpan Data Centre is recommended for Production Site and MegaWatt Park for DR site.</p>	High
Event Management	Ability to replay any event or incident from the stored database for further investigation.	High
Intruder Alarm Systems	<p>The use of intruder alarm systems for areas that require protection is necessary. The hazard, the risk exposure and the pre-determined level of protection required determines the type of system, in particular where such alarms will transmit signals to a control room.</p> <ol style="list-style-type: none"> <li>1. Internal alarm systems to monitor entry into the control rooms or other critical building or identified area.</li> <li>2. Optimisation of the current Eskom Telecommunications alarm systems as well as integration into the new systems. Refer to Section 13 for the Security Alarm System Specification.</li> </ol>	High
Non-Lethal Fence & Gates	<ol style="list-style-type: none"> <li>1. Must comprise of a minimum of 5 joules throughout. Refer to section 13 for Non-Lethal Fence Specification.</li> <li>2. Access gates control consisting of 3 automated sliding gates; and</li> <li>3. Emergency exits need to have the same characteristic continuous flow throughout the security measures to ensure that the integrity of the perimeter is maintained.</li> <li>4. There will be sufficient distance between the internal and external security perimeter fence to effect maintenance.</li> <li>5. The construction of a concrete plinth will prevent vegetation encroaching onto the electric fence.</li> </ol>	High
PSIM Non-functional requirements		

Name	Description	Requirement Priority
Patrol Roads	1. Patrol roads shall consist of 3-meter gravel roads on the inside and outside of the outer perimeter barrier.	High
Perimeter Security Lighting	1. Provision of lighting to provide visibility for observation and optimum CCTV functionality. Refer to section 13 for CCTV specification. 2. The perimeter security lighting will be zoned. Refer to section 13 for the Security Lighting Specification. 3. Activation of the perimeter security lighting zones by means of a signal. Refer to section 13 for the Security Lighting Specification. 4. Manual activation of individual zones for testing and security purposes from the main gate security control room.	
Physical Security Analytics	Ability to analyze trends in security events and incidents and report on the same	Medium
Physical Security Information Management System		
Physical Security Infrastructure Management (PISM)	1. Ensure enterprise-wide integration of physical security systems. 2. Collect and correlate data from multiple unconnected or diverse security subsystems and components. 3. Manage incidents in real time. 4. Proactively resolve situations by empowering the security personnel. 5. Creates real-time dashboards and reports.	High
Physical Security Reporting	Provisioning of standard and customized reports	Medium
Public Address System & Panic Buttons	1. Substations shall be equipped with an automated PA (Public Address) system. The PA system will support local control on site and remote control from the control centre. This will allow the controllers to warn the intruder/s and serve as an evacuation system. Refer to Section 13 for the security PA systems specification. 2. Deploy panic buttons at strategic areas in the substation control room. The panic button alarm must be clearly distinguished as a panic alarm. Refer to Section 13 for the Security Alarm System Specification.	High
Site Power Supply	1. Supply power from a central point to all physical security elements. 2. Backup power is required to power the physical security equipment in the event of an unplanned power failure.	High
Surveillance & Detection Systems	The surveillance systems shall comprise of the following (Refer to section 13 for the Security Lighting Specification): 1. A CCTV system with static cameras on the perimeter of the substation, with PTZ (Pan, Tilt and Zoom) capability at strategic points. 2. Cameras installed at key points (i.e. substation buildings and entrances) to identify both vehicles and persons. 3. This system should support video analytics to detect unauthorised activities. 4. Stream real-time video footage to Eskom Zero Control for remote monitoring. 5. Passive infrared beams to assist with detection of security threats to critical assets. 6. Capable of operating in adverse weather conditions and function effectively at day and night. 7. An audible siren activated during any security event triggered by any deployed physical security sensor. 8. Security	High

Name	Description	Requirement Priority
	managers/ management to view CCTV visuals via a remote location. 9. Upon a triggered alarm, the PTZ shall zoom into that affected area. Upon the detection of a person or animal, the PTZ shall follow the motion of that person or animal. The control signals from an operator shall take preference over the tracking functions.	
Telecommunications	1. Telecommunication infrastructure shall be in place to transfer all security information from the physical security systems to the remote control center.	High
Threat Detection & Mitigation	<ul style="list-style-type: none"> <li>* A simple but powerful network security technique is to logically separate different functional elements that should never be communicating with each other (e.g. OT, IT and Security Traffic).</li> <li>* The security architecture should support VLANs (Virtual Local Area Networks), VRF's (Virtual Routing and Forwarding) or GRE (Generic Routing Encapsulation) to achieve network segmentation.</li> <li>* To build on top of that, access lists and firewall features can be configured on FAR's and substation routers respectively, to filter and control access in the Eskom Transmission Substations and Eskom Telecommunications High-Sites.</li> <li>* All traffic originating from the FAN should be aggregated at the control-center tier and needs to be passed through a Next-Generation firewall, especially if it has traversed through a public network. This firewall should implement zone-based policies as well as intrusion prevention signatures to detect and mitigate threats.</li> <li>* Different applications in the control center tier should be part of a layered design based on stricter restrictions with increasing security levels (e.g. apply the Eskom ICT Network Security Framework and Web Application Pattern rules).</li> <li>* An important aspect of threat detection is the use of syslog and netflow information from network devices.</li> <li>• Event logs from firewalls, routers, NMS (Network Management Systems) and head-end systems, meters and other end-points need to be collected and passed on to a SIEM (Security Incident and Event Manager tool. Such an application can correlate events occurring in different parts of the grid to identify few security incidents, enabling a quicker and more coordinated response.</li> </ul>	High
Training	Training for System Users is required and the supplier will come and do the on-site training for all the identified users.	Medium
User Interface	<ul style="list-style-type: none"> <li>* Graphical user interface to be user friendly and have different overlays / layers to display different system data on one screen.</li> <li>* User should not need to move between screens to get a status overview of all integrated systems</li> <li>* All new systems will have to be evaluated by super users of current system on this functionality.</li> </ul>	High
Video Management System (VMS)	1. Support 'black screen monitoring': No active video is visible in normal state. A triggered site alarm will activate the video and the controller will see a series of still images or a short video clip of the zone of the triggered alarm. The controller can then choose to	High

Name	Description	Requirement Priority
	stream the video from the site. 2. Support an event queue to allow the management and acknowledgment of multiple alarm events. 3. It shall be possible to look at a new event without having acknowledged a previous event. 4. Support PTZ control including PTZ pre-set positions. 5. Allow the transmission of voice from the controller to the PA system on site. 6. Allow for the controller to control lights at the site. 7. Allow controller to view the location of alarms and cameras on a site layout 8. Allow controller to view the location and status of all sites on a map 9. Link comments from the controller to an event. 10. Enable the escalation of incidents to another workstation running the client software (e.g. another controller). 11. Log events and actions for auditing purposes. 12. Track movement and highlight which area of the camera field of view has triggered an alarm (this could be software based or a feature of the cameras or video analytics on site).	
Walkways	1. Provision an unobstructed walkway on the inside of the inner perimeter fence of the site to allow security guards to patrol the entire circumference by foot.	High

### 3.4. SECURITY ARCHITECTURE



The security architecture, as per the above diagram illustrates the following: -


- The solution shall use Microsoft AD as the main identification and authorization system
- The Bernina and central server infrastructure shall use a client – server architecture

- Where the PSIM will need to provide automated alarms and alerts to outsourced suppliers such as armed response or security companies, the data shall be interfaced from the OT firewall
- The supplier is required to prove their disaster recovery capability as part of the proof of concept design, although the physical infrastructure may not necessarily be located at Eskom's IT data center

### 3.5. RISKS AND ISSUES

This section provides the description of any risks and issues that are known at this time and are likely to affect the successful completion of the target architecture definition (excluding project management specific risks).

#### 3.5.1. Target Risk Catalog

Name: DEV_D1_Tx & ET Security Monitoring System_Target_202008_V01  Type: Risk catalog Identifier: STD.25899895	Creator: system Time of generation: 12 Aug 2020 9:02:01 AM Last user: moatshh Last change: 31 Aug 2020 3:56:10 PM	
---	--	---



**Figure 3: DEV\_D1\_Tx & ET Security Monitoring System\_Target\_202008\_V01 [Risk Catalog]**

**Table 5: Risk Descriptions**

Name	Risk Rating
Inadequate physical access control and CCTV (Closed Circuit Television) systems	High
Increases in barrier intrusions have proven that current barriers are inadequate.	High
Monitoring and response capability	High
Lack of an integrated physical security system across Eskom, which limits the collaboration of physical security systems to minimize physical security threats across the organization.	High
Lack of maintenance and support for physical security systems.	High
Lack of physical security standardization across the organization, which results in misaligned physical security designs that potentially contradict the approved physical security standards.	High



Name	Risk Rating
Minimal refurbishment and replacement of physical security infrastructure over the past 25 years resulted in significant occurrences of physical security incidents.	High
Significant retrofitting of security capabilities, which results in excessive costs.	High
The current physical security systems neither mitigate the on-going challenges of prevailing physical security threats, nor meet Eskom's statutory obligations as determined by the security threat and risk assessments.	High
The existing barriers and perimeter lighting have mostly reached the end of their life span.	High
The lack of adequate physical security systems and measures poses a risk to security guards and employees, as they do not provide sufficient first line of defense.	High

#### 4. PHYSICAL APPLICATION COMPONENT DESCRIPTION

The table below provides the attributes that describes the physical application component.

**Table 7: Physical Application Component Attributes**

Attribute	Value
Name	Physical Security Information Management System (PSIM)
Application Level	Client – Server
Full Name	N/A
Abbreviation	PSIM
Version	Unknown
Description	This is for the IT components of the solution only - the OT side has separate infrastructure and systems that will integrate into the IT systems.
Restriction On Usage Terms & Conditions	Unknown
Rationale	To provision a solution that manages security incidents and events from the Benina Substation
Primary Application Purpose	To manage physical security risks from Benina Substation
Standard Approval Date	To be determined
Used By: Division (Obsolete)	Group Security; Transmission
Standardization Status	In evaluation
Evaluation (Start)	To be determined, following RFP process
Phase-In Phase (Start)	To be determined, following RFP process
Phase-In Phase (End)	To be determined, following RFP process
Standard (Start)	To be determined, following RFP process
Standard (End)	To be determined, following RFP process
Phase-Out Phase (Start)	To be determined, following RFP process
Phase-Out Phase (End)	To be determined, following RFP process
Criticality	High
Number Of Users	20 – 30 (POC – Benina)
Repository Notes	None
Last Upgrade (Year)	N/A

Attribute	Value
IT/OT	OT and IT
Date Market Tested	Unknown
Vendor Details	Unknown
Vendor Number	Unknown
Contract Number	Unknown
Contract Start Date	To be determined, following RFP process
Contract End Date	To be determined, following RFP process
Licence Required	20 – 30 (POC – Benina)
Licences Allocated	20 – 30
Licences Acquired	None
Software Licence Category	Subscription
Licence Model (As-Is)	N/A
Licence Model (To-Be)	Subscription
Enterprise IT Services Classification	Line of Business – Tx
System Strategy/Roadmap	Unknown
System Pace Layer	Persistent
Cloud Candidate (Obsolete)	N/A
Service Model (As-Is)	Unknown
Service Model (To-Be)	Unknown
Deployment Model (As-Is)	Unknown
Deployment Model (To-Be)	Client - Server
System Type	Application
Cloud Hosting Location (As-Is)	N/A
Cloud Hosting Location (To-Be)	N/A
UID	Unknown
Identifier	STD.25922683
Bespoke	No
Software Licence	Subscription
Product Name*	Unknown
Business Impact Assessment Link	TBC
Business Impact Assessment Date	TBC
Disaster Recovery Plan Link	N/A for POC
Disaster Recovery Tested Date	N/A for POC
Black Start – Needed During Black Start	No
Black Start – Critical For Black Start	No
Black Start Impact – Financial (Revenue)	No
Black Start Impact – Core Operations/Productivity	No

Attribute	Value
Black Start Impact – Customer Satisfaction	No
Black Start Impact – Employee (Well-Being/Safety)	No
Cloud Candidate	No
RFx Number	Unknown

5. APPLICATION ARCHITECTURE

5.1. APPLICATION ARCHITECTURE LANDSCAPE CONTEXT

The application portfolio catalog provides a contextual perspective of the Information systems (IS) and/or the applications for this architectural definition. It could also show the decomposition of the IS/application.

5.1.1. Target Application Portfolio Catalog


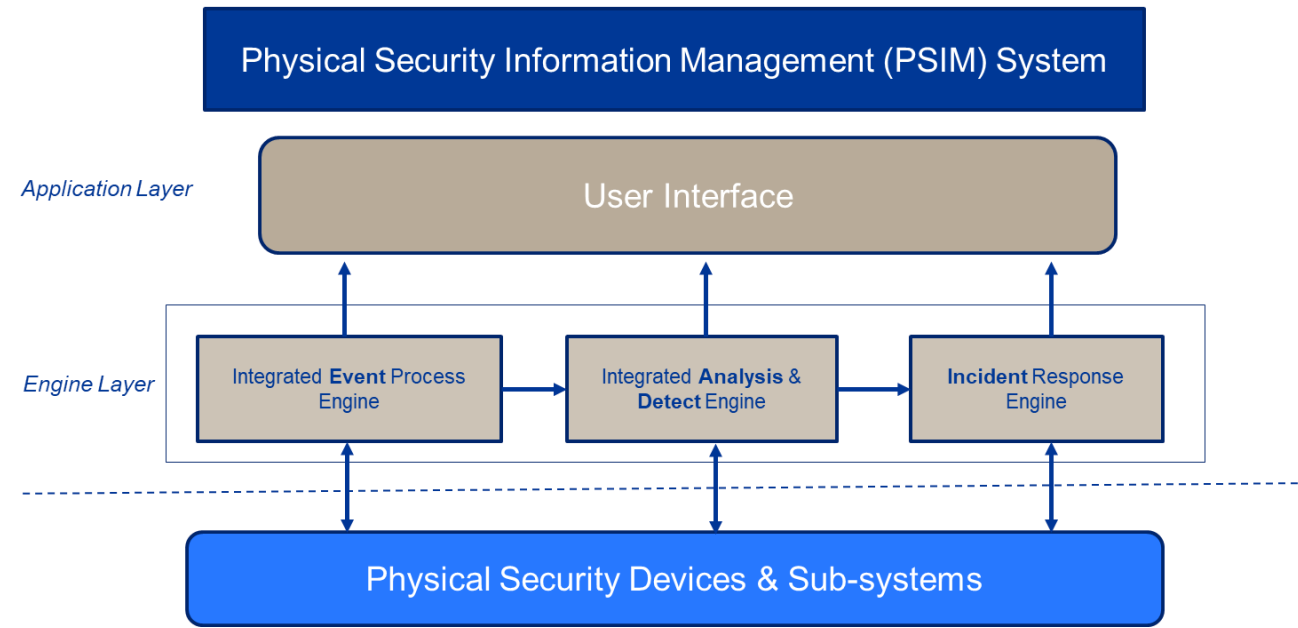
Name: DEV_D3_Tx & ET Security Monitoring System_Target_202008_V01		Creator: solomosj Time of generation: 10 Nov 2020 8:44:38 PM Last user: solomosj Last change: 10 Nov 2020 8:56:06 PM	 ARIS Model
Type: Application portfolio catalog Identifier: STD.26019260			



Figure 4: DEV\_D3\_Tx & ET Security Monitoring System\_Target\_202008\_V01 [Application Portfolio Catalog]

Table 8: Information System Descriptions

Name	Description
Security Incident and Event Management	An information system that integrates all security devices and provides a response to operators on how to direct the response strategy.



The above diagram illustrates that the solution shall follow an event driven approach, to ensure cost effectiveness.


Table 9: Physical Application Component Descriptions

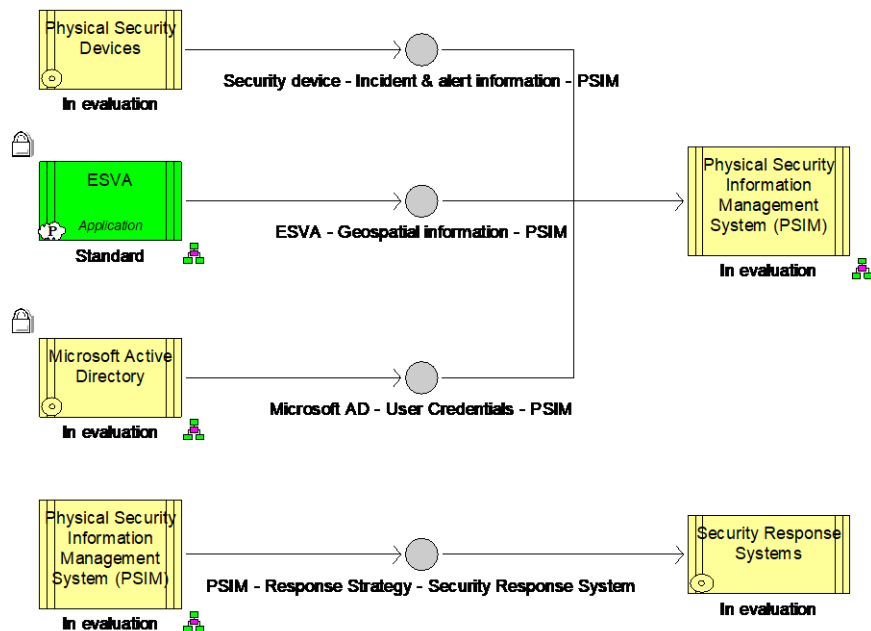
Name	Description	Attributes
Physical Security Information Management System (PSIM)	This is for the IT components of the solution only - the OT side has separate infrastructure and systems that will integrate into the IT systems.	Standardization Status: In evaluation

## 5.2. APPLICATION INTERFACE CONTEXT

The application interface context provides a description of the flow of data between the ISs or applications.

### 5.2.1. Target Application Communication Diagram

Name: DEV_D3_Tx & ET Security Monitoring System_Target_202008_V01  Type: Application communication diagram Identifier: STD.26022360	Creator: solomosj Time of generation: 12 Nov 2020 9:48:40 PM Last user: system Last change: 17 Nov 2020 5:48:15 PM	 Eskom ARIS Model
--	---	--



**Figure 5: DEV\_D3\_Tx & ET Security Monitoring System\_Target\_202008\_V01 [Application Communication Diagram]**

**Table 11: Interface Descriptions**

Name	Description
ESVA - Geospatial information - PSIM	Ability to interface with Eskom's GIS Platform with the primary purpose to locate substations in the event of a security incident and / or event. The current geospatial system (ESVA) is being reviewed and will be assessed. Eskom will provision a suitable solution in order to meet the needs of the physical security information management system
Microsoft AD - User Credentials - PSIM	Eskom's identification and authorization system, where users are granted access to applications
PSIM - Response Strategy - Security Response System	Interface where in the event of an incident, the system is required to alert external systems such as armed response systems for a response plan

Name	Description
Security device - Incident & alert information - PSIM	Interface between security devices and the PSIM, where a common interface is used to facilitate all related incidents and events.

**Table 12: Physical Application Component Descriptions**

Name	Description	Attributes
ESVA	Enterprise spatial viewer and analysis. Built on ESRI technology. Should replace TxSIS and TxSIS2	Criticality: Normal Standardization Status: Phased out
Physical Security Information Management System (PSIM)	This is for the IT components of the solution only - the OT side has separate infrastructure and systems that will integrate into the IT systems.	Standardization Status: In evaluation

**Table 13: Physical Software Technology Component Descriptions**

Name	Description	Attributes
Microsoft Active Directory	Provides authentication and authorisation and other related services. It authenticates and authorises all users and computers in a Windows domain type network, assigning and enforcing security policies for all computers and installing or updating software. Active Directory allows administrators to organize objects of a network (such as users, computers, and devices) into a logical hierarchical collection of containers, irrespective of the physical location or hierarchy of the objects.	Criticality: Normal Standardization Status: In evaluation
Physical Security Devices	Devices that are used to detect intruders into the Eskom property	Standardization Status: In evaluation
Security Response Systems	A system that is used to manage and mitigate the security risk or incident	Standardization Status: In evaluation

## 5.2.2. Target Application

## 5.3. APPLICATION STAKEHOLDERS

The stakeholder analysis describes the stakeholders for the architecture, their influence over the engagement, their key interests and concerns that must be addressed by the target architecture. It includes those organizational units, business roles and persons with an interest in the architecture design(s), and that are likely to be affected by it.

### 5.3.1. Target Stakeholder Analysis Diagram

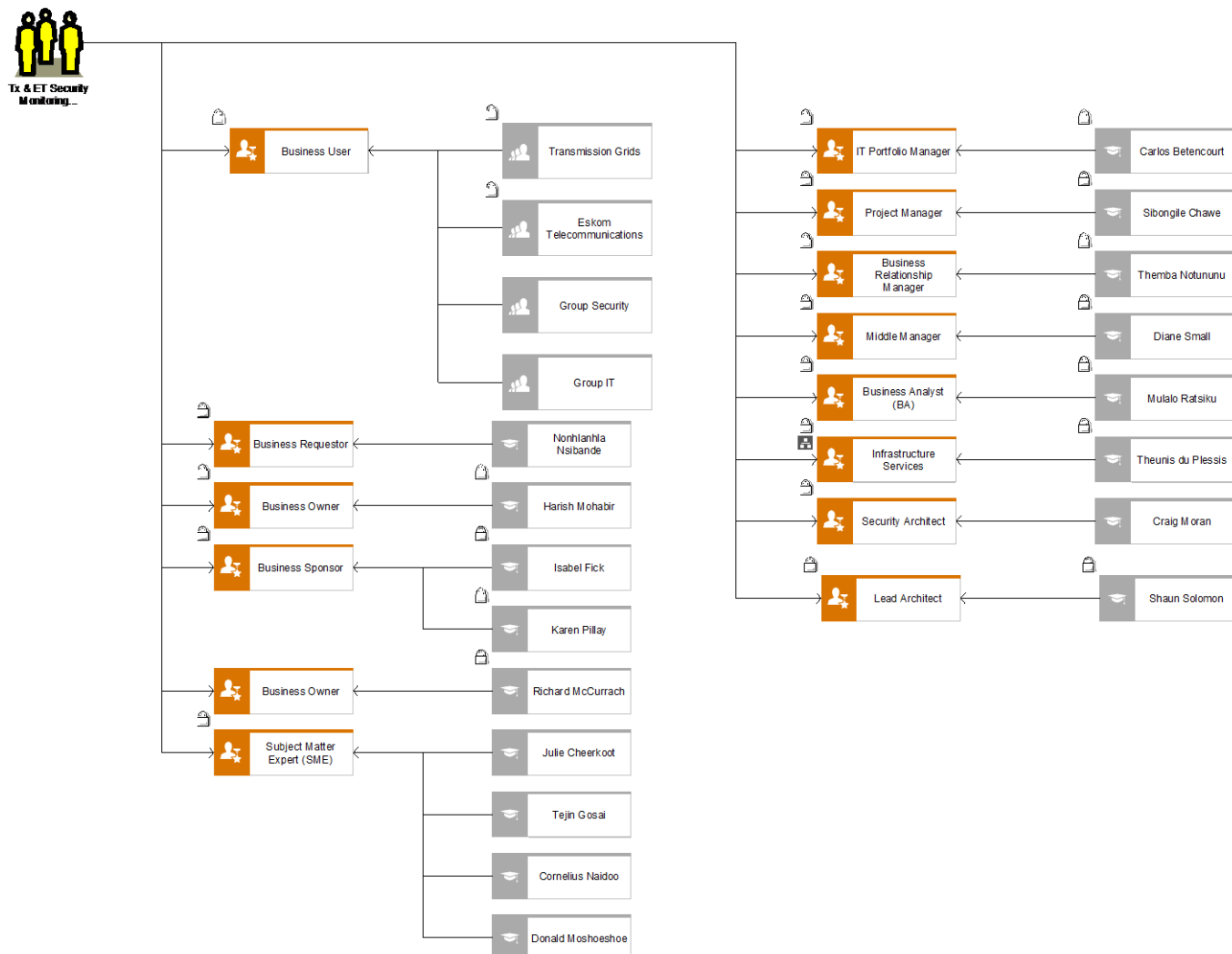
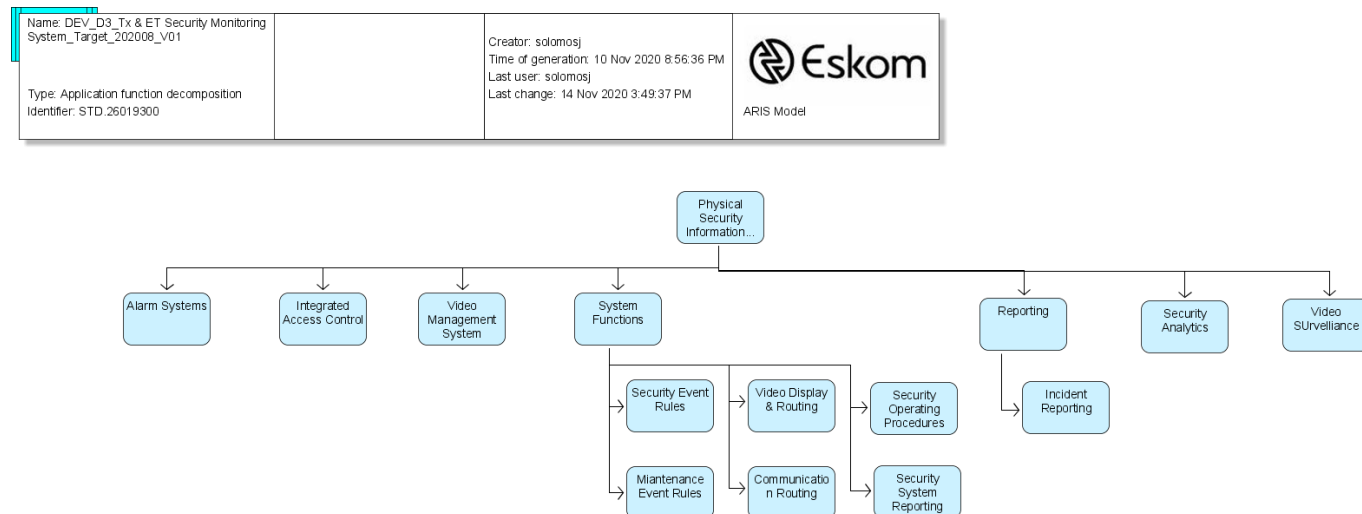


Figure 6: DEV\_D3\_Tx & ET Security Monitoring System\_Target\_202008\_V01 [Stakeholder Analysis Diagram]

## 5.4. INFORMATION SYSTEM/APPLICATION FUNCTIONS

The function decomposition view provides a representation of the functions of the IS or application in scope for the application architecture. The functions imply a partial or full automation of the business process they are intended to support.

### 5.4.1. Target Application Function Decomposition



**Figure 7: DEV\_D3\_Tx & ET Security Monitoring System\_Target\_202008\_V01 [Application Function Decomposition]**

**Table 16: Application Function\* Descriptions**

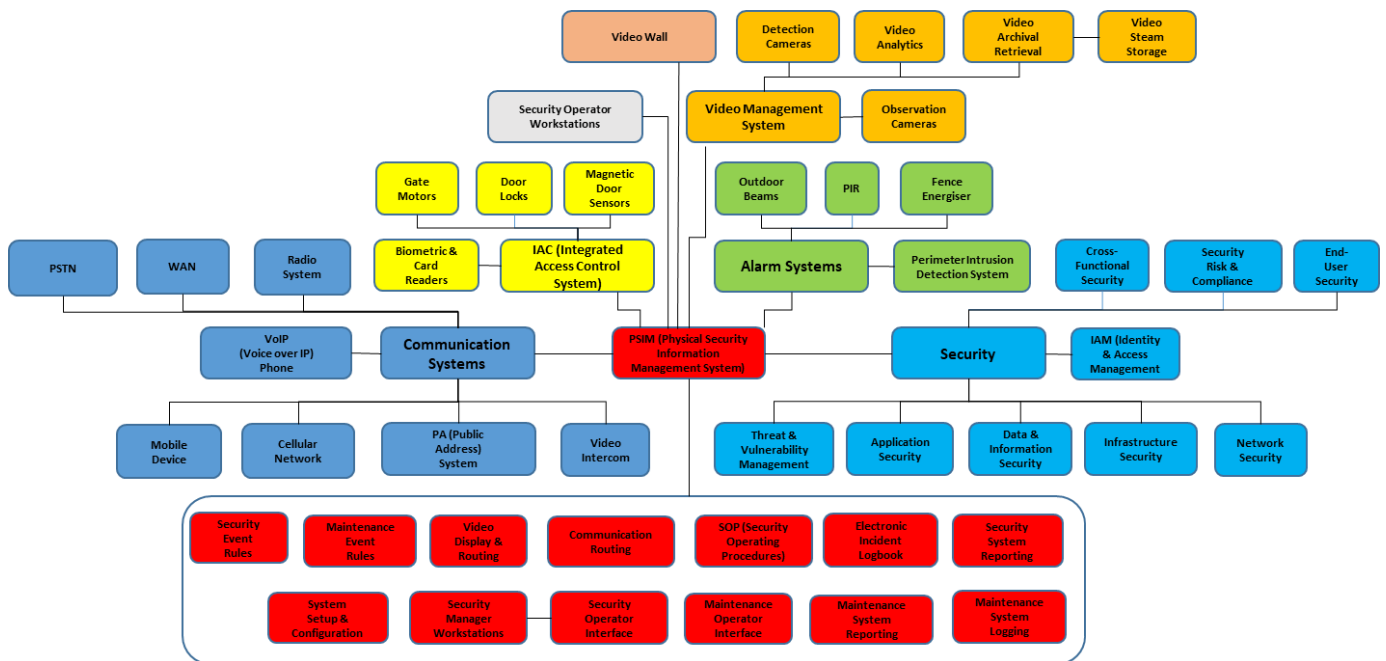
Name	Description
Alarm Systems	A system which provides the operator with an alert, so that the necessary response strategy may be taken
Communication Routing	A network routing that provides systems and application to route and direct network traffic to their destination
Incident Reporting	A report that provides a list of incidents and events so that end users may analyze and take tactical and management action, to mitigate the risk of physical assets
Integrated Access Control	Solution that provides logical and physical access to end users so that they may access resources
Maintenance Event Rules	Rules that are logically configured into systems to direct security events and incidents, with a view to mitigate management risks
Reporting	A capability that consolidates data into a single and recognizable format which can be used by multiple users, who have access to read the report
Security Analytics	A capability that is used to analyze data based on trends not normally available in standard reporting functions
Security Event Rules	System configuration that is pre-designed in order to assist operators based on simple and advanced logic
Security Operating Procedures	Procedures that are logically automated in the system in order to achieve specific risk mitigation objectives
Security System Reporting	Reporting that provides a record of all system related events such as access control and system health
System Functions	Product features that have been pre-configured by the OEM for ease of use by end users
Video Display & Routing	Display configuration and navigation for end users

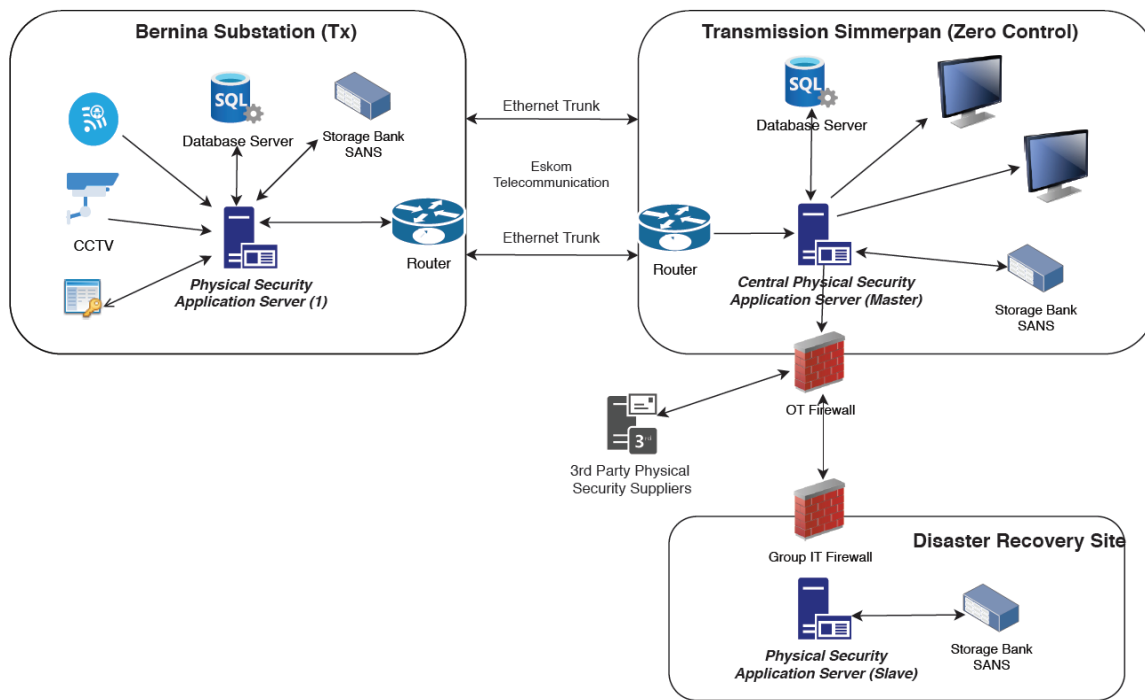


Name	Description
Video Management System	A sophisticated video management which provides end users with the capability to view system functions
Video SURveillance	Capability to record video footage based on demand or in the event of an incident

**Table 17: Physical Application Component Descriptions**

Name	Description	Attributes
Physical Security Information Management System (PSIM)	This is for the IT components of the solution only - the OT side has separate infrastructure and systems that will integrate into the IT systems.	Standardization Status: In evaluation





## SYSTEM ARCHITECTURE

The proof of concept is envisaged that the system architecture comprise of the following as a minimum: -

1. A client – server architecture which consists of a local integration server located at Bernina Substation which integrates all security devices using an industry protocol/s
2. A database server which may be logically configured on the application server which manages all incoming events and incidents and other configuration data where required
3. A storage device which is used as a back-up device for the application server and primarily used to record video surveillance from camera's
4. The end user may access the local integration server upon request primarily for configuration and maintenance / support purposes
5. The solution architecture is designed based on an event driven engine and users may access the solution upon demand. This strategy is based on ensuring a cost effective solution
6. The central server infrastructure, located at Zero Control in Simmerpan will consist of a client server architecture, where end users may remotely access the Bernina Substation physical security information system based on a role-based access control method. This will allow remote operators to access functional capabilities of the solution upon demand and execute on a response strategy which may be automated or based on human intervention
7. The central infrastructure will be set-up for end users to access remote substations using advanced video wall technology similar to a national operations centre will full back-up storage capabilities in the form of a SANS storage network infrastructure
8. The centralized infrastructure will be located in the Simmerpan data centre, of which the design shall be defined in the details design stage of the POC project
9. The disaster recovery plan will consist of a procedure which outlines when and how the DR site will be activated in the form of a business continuity plan. For the purposes of the POC, the DR infrastructure and related equipment is not necessary. However, the supplier is required to prove and demonstrate that their solution can be set-up and configured for a fully redundant application and infrastructure

## 6. DATA & INFORMATION ARCHITECTURE

### 6.1. LOGICAL DATA & INFORMATION

The data and information architecture provides a description of the subject areas and information artefacts required by this architecture design.

#### 6.1.1. Target Data Catalog

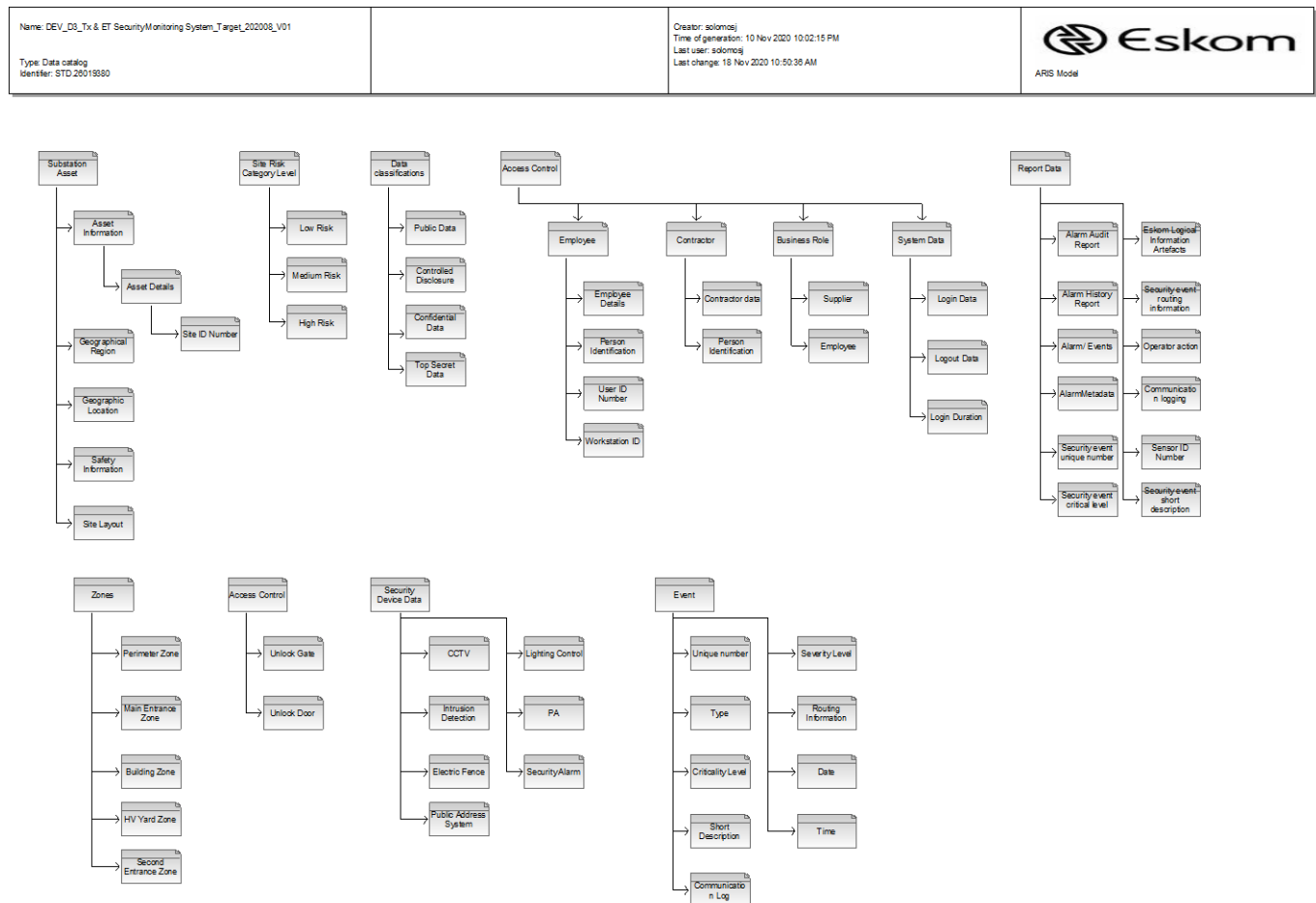


Figure 8: DEV\_D3\_Tx & ET Security Monitoring System\_Target\_202008\_V01 [Data Catalog]

Table 20: Logical Information Artefact Descriptions

Name	Description
Access Control	Capability to allow and restrict access to the PSIM
Alarm Audit Report	Log report detailing alarm information.
Alarm History Report	Comprehensive list of alarm reports set for a specific date and time.
Alarm/ Events	Meter Alarms or Events Received
AlarmMetadata	The Alarm Metadata table defines the alarm limits and associates the alarm with an area of the Power Station.
Asset Details	The details of the physical asset i.e. Bernina Substation
Asset Information	Set of attributes of an asset, representing typical data-sheet information of a physical device that can be instantiated and shared in different data exchange contexts: <ul style="list-style-type: none"> <li>- as attributes of an asset instance (installed or in stock)</li> <li>- as attributes of an asset model (product by a manufacturer)</li> <li>- as attributes of a type asset (generic type of an asset as used in designs/extension planning).</li> </ul>

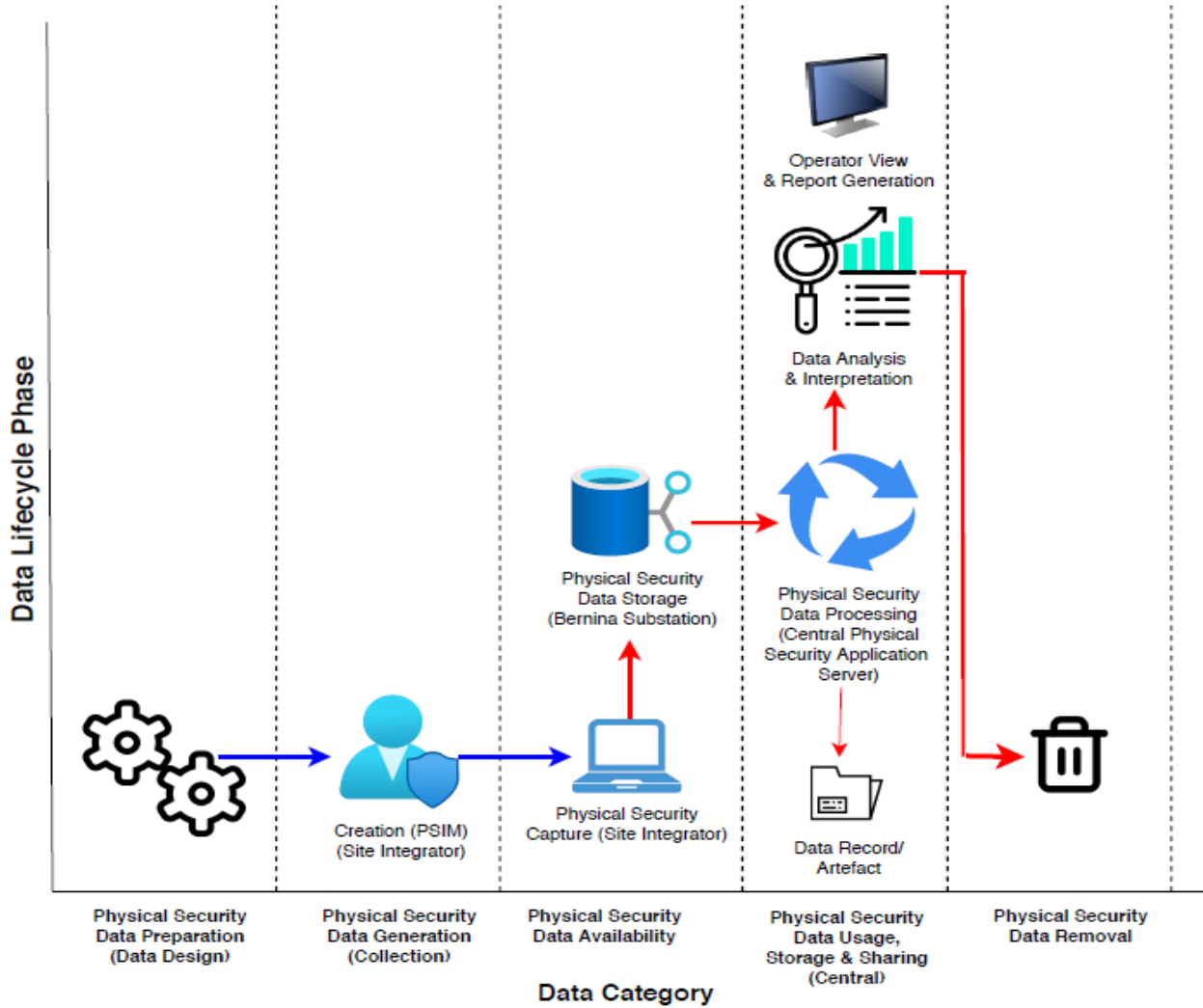
Name	Description
Business Role	A business role that this organisation plays. A single organisation typically performs many functions, each one described as a role.
CCTV	Closed circuit television for video surveillance
Communication Log	A log that records all communication between systems and sub-systems
Confidential Data	Data that is controlled through using security controls
Contractor	An outsourced partner that assists Eskom in delivering the system and ensuring it is implemented accordingly
Controlled Disclosure	Data and information that is secure based on pre-defined rules
Criticality Level	The levels defined by the business to determine the type of risks associated by the physical security system
Employee	An individual who works part-time or full-time under a contract of employment, whether oral or written, express or implied, and has recognized rights and duties. Also called worker.
Employee	An individual who works part-time or full-time under a contract of employment, whether oral or written, express or implied, and has recognized rights and duties. Also called worker.
Employee Details	The competency information of an employee to check whether she/he is allowed to perform work in a plant.
Event	A thing that happens or takes place, especially one of importance.
Geographic Location	Information that describes the physical location of the physical asset
Geographical Region	A geographical region of a power system network model.
High Risk	Category of risk
Intrusion Detection	System that is used to alert operators of an intrusion
Lighting Control	Control system that manages lighting
Login Data	Data that is used to describe when users login to the system
Login Duration	Data that is used to describe how long users accessed the system
Logout Data	Data that is used to describe when users logout to the system
Low Risk	Category of risk
Medium Risk	Category of risk
Operator action	Action of the operator in order to access information
Person Identification	Extension that caters for multiple identification methods for a person. For example, ID and passport.
Person Identification	Extension that caters for multiple identification methods for a person. For example, ID and passport.
Public Address System	A system used to communicate with on-site staff orally or verbally
Public Data	Information that is available to anyone

**Table 21: Data Security Classification**

<b>Name</b>	<b>Security Classification Level</b>
Access Control	Controlled Disclosure
Alarm Audit Report	Controlled Disclosure
Alarm History Report	Controlled Disclosure
Alarm/ Events	Controlled Disclosure
AlarmMetadata	Controlled Disclosure
Asset Details	Controlled Disclosure
Asset Information	Controlled Disclosure
Business Role	Controlled Disclosure
CCTV	Controlled Disclosure
Communication Log	Controlled Disclosure
Communication logging	Controlled Disclosure
Confidential Data	Controlled Disclosure
Contractor	Controlled Disclosure
Contractor data	Controlled Disclosure
Controlled Disclosure	Controlled Disclosure
Criticality Level	Controlled Disclosure
Data classifications	Controlled Disclosure
Date	Controlled Disclosure
Electric Fence	Controlled Disclosure
Employee	Controlled Disclosure
Employee	Controlled Disclosure
Employee Details	Controlled Disclosure
Eskom Logical Information Artefacts	Controlled Disclosure
Event	Controlled Disclosure
Geographic Location	Controlled Disclosure
Geographical Region	Controlled Disclosure
High Risk	Controlled Disclosure
Intrusion Detection	Controlled Disclosure
Lighting Control	Controlled Disclosure
Login Data	Controlled Disclosure
Login Duration	Controlled Disclosure
Logout Data	Controlled Disclosure
Low Risk	Controlled Disclosure
Medium Risk	Controlled Disclosure
Operator action	Controlled Disclosure
Person Identification	Controlled Disclosure

Name	Security Classification Level
Person Identification	Controlled Disclosure
Public Address System	Controlled Disclosure
Public Data	Controlled Disclosure
Report Data	Controlled Disclosure
Routing Information	Controlled Disclosure
Safety Information	Controlled Disclosure
Security event critical level	Controlled Disclosure
Security event routing information	Controlled Disclosure
Security event short description	Controlled Disclosure
Security event unique number	Controlled Disclosure
Sensor ID Number	Controlled Disclosure
Severity Level	Controlled Disclosure
Short Description	Controlled Disclosure
Site ID Number	Controlled Disclosure
Site Layout	Controlled Disclosure
Site Risk Category Level	Controlled Disclosure
Substation Asset	Controlled Disclosure
Supplier	Controlled Disclosure
System Data	Controlled Disclosure
Time	Controlled Disclosure
Top Secret Data	Controlled Disclosure
Type	Controlled Disclosure
Unique number	Controlled Disclosure
User ID Number	Controlled Disclosure

## Data Architecture for Physical Security Information System - Lifecycle Approach



The diagram above provides the lifecycle of data for the PSIM taking the proposed solution architecture into consideration.





**Figure 9: DEV\_D3\_Tx & ET Security Monitoring System\_Target\_202008\_V01 [Technology Portfolio Catalog]**

**Table 24: Technology Landscape Descriptions**

Name	Description
Client Hardware	<p>Generic term that is used to denote any device that is utilised by the end-user to access applications and services within Eskom.</p> <ol style="list-style-type: none"> <li>1. Server Hosted Client: Separation of the desktop hardware device from the Operating environment (Operating System and supported applications). This is achieved by hosting the client's operating system and applications on a server that is specifically used to host such operating environments. This technology enables centralised and efficient management of the operating environment.</li> <li>2. Desktops: A complete, autonomous computer with its own operating system and hard drive. The greatest strength and weakness of a desktop is its isolation; the computer continues to work even if a network infrastructure fails as opposed to a thin client that cannot operate without back-end infrastructure. It is called a client because in the corporate environment it is used as a client to a back-end system.</li> <li>3. Tablet PC: It is a slate-shaped mobile computer equipped with a touchscreen to operate the computer with a stylus or digital pen, or a fingertip and supports hand-written input.</li> <li>4. Personal Computing devices (PCD): A pocket size computer that performs the functions of the Personal Digital Assistant, mobile phone and has an ability and connectivity to act as a client to back-end systems.</li> </ol>
Client Operating System	An operating system (OS) is system software that manages computer hardware, software resources, and provides common services for computer programs.
Mobile Applications	Logical grouping for Mobile Applications
Server Hardware	These are hardware platforms that serve the needs of the enterprise and categorized as departmental, divisional as well as enterprise hardware platforms. They are primarily intended to provide a level of capacity, efficiency and security that is much higher than a typical personal computer such as a desktop. Web, Application, Database, Middleware, Business Intelligence and specialised servers are incorporated into this category.
Server Operating System	A server operating system, also called a server OS, is an operating system specifically designed to run on servers, which are specialized computers that operate within a client/server architecture to serve the requests of client computers on the network.
Storage Infrastructure	Hardware, including disk and tape, along with software for backup and recovery
Web Browser	A web browser (commonly referred to as a browser) is a software application for accessing information on the World Wide Web. Each individual web page, image, and video is identified by a distinct URL, enabling browsers to retrieve and display them on the user's device.

**Table 25: Technology Service Descriptions**

Name	Description
Anti-Malware & Anti-Spyware	Provides Anti-Malware and anti-spy ware services other than end user security
Application Security	Application security encompasses measures taken throughout the code's life-cycle to prevent gaps in the security policy of an application or the underlying system (vulnerabilities) through flaws in the design, development, deployment, upgrade, or maintenance of the application.
Availability & Fault Management	Availability and Fault Management services allow a system to react to the loss or incorrect operation of system components including hardware, platform software, and application software.
Capacity Management Service	Capacity Management services address three basic functions: <ul style="list-style-type: none"> <li>* Capacity management analyzing current and historic performance and capacity;</li> <li>* Workload management to identify and understand applications that use the system;</li> <li>* Capacity planning to plan required hardware resources for the future.</li> </ul>
Change Management	Change Management services provide for version identification and configuration management of object interfaces, implementations, and instances.
Communication Infrastructure	Network services are provided to support distributed applications requiring data access and applications interoperability in heterogeneous or homogeneous Networked environments. A Network service consists of both an interface and an underlying protocol.
Communication Infrastructure	Network services are provided to support distributed applications requiring data access and applications interoperability in heterogeneous or homogeneous Networked environments. A Network service consists of both an interface and an underlying protocol.
Configuration Management	Configuration Management services address four basic functions: <ul style="list-style-type: none"> <li>* Identification and specification of all component resources;</li> <li>* Control, or the ability to freeze configuration items, changing them only through agreed processes;</li> <li>* Status accounting of each configuration item;</li> <li>* Verification through a series of reviews to ensure conformity between the actual configuration item and the information recorded about it</li> </ul> These services include: 1. Processor CM - takes a platform-centric approach; 2. Network CM & Distributed System CM - services allow remote systems to be managed and monitored including the interchange of Network status, 3. Topology CM - is used to control the topology of physical or logical entities that are distributed, and 4. Application CM - focuses on applications.
Content Management	Will enforce controls in order to ensure that information being accessed is legitimate, malware free and appropriate for business use. (Email and Internet)
Cross Functional Security	Is an approach where all the services within this category are consumed by the entire Eskom and will be difficult to compartmentalise as this includes Cloud Security, Cyber Threat Intelligence, SIEM, Public Key Infrastructure, Enterprise Mobile Security
Cross Functional Services (CMP)	Security Guidance for Critical Areas of Focus in Cloud Computing
Cyber Threat Intelligence	Evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging

Name	Description
	menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard.
DC Switching and Routing	
Data & Information Security	Data & Information security ensures the protection of data, within a database, files server, hosting site, from destructive forces and from the unwanted actions of unauthorized users.
Data Centre Security	Data center security is the pursuit of practices that make a data center more secure from a range of different kinds of threats and attacks. The data center, as a major primary resource for Eskom.
Data Classification	Capability to Classify the data within Eskom as guided by the Data Owner and Steward
Data Dictionary / Repository	Data Dictionary/Repository services allow data administrators and information engineers to access and modify data about data (i.e., metadata). Such data may include internal and external formats, integrity and security rules, and location within a distributed system. Data dictionary and repository services also allow end users and applications to define and obtain data that is available in the database. Data administration defines the standardization and registration of individual data element types to meet the requirements for data sharing and interoperability among information systems throughout the enterprise. Data administration functions include procedures, guidelines, and methods for effective data planning, analysis, standards, modelling, configuration management, storage, retrieval, protection, validation, and documentation. Data dictionaries are sometimes tied to a single Database Management System (DBMS), but heterogeneous data dictionaries will support access to different DBMSs. Repositories can contain a wide variety of information including Management information Bases (MIB) or CASE-related information.
Data Hosting	A ICT data hosting service.
Data Hosting Infrastructure	Database Management System (DBMS) services provide controlled access to structured data. To manage the data, the DBMS provides concurrency control and facilities to combine data from different schemas. Different types of DBMS support different data models, including relational, hierarchical, network, object-oriented, and flat-file models. Some DBMSs are designed for special functions such as the storage of large objects or multimedia data. DBMS services are accessible through a programming language interface, an interactive data manipulation language interface (such as SQL), or an interactive/fourth-generation language interface. For efficiency, DBMSs often provide specific services to create, populate, move, backup, restore, recover, and archive databases, although some of these services could be provided by the general file management capabilities or a specific backup service. Some DBMSs support distribution of the database, including facilities for remotely updating records, data replication, locating and caching data, and remote management.
Data Hosting Infrastructure	Database Management System (DBMS) services provide controlled access to structured data. To manage the data, the DBMS provides concurrency control and facilities to combine data from different schemas. Different types of DBMS support different data models, including relational, hierarchical, network, object-oriented, and flat-file models. Some DBMSs are designed for special functions such as the storage of large objects or multimedia data. DBMS services are accessible through a programming language interface, an interactive data manipulation language interface (such as SQL), or an interactive/fourth-generation language interface. For efficiency, DBMSs often provide specific services to create, populate, move, backup, restore, recover, and archive databases, although some of these services could be provided by the general file management capabilities

Name	Description
	or a specific backup service. Some DBMSs support distribution of the database, including facilities for remotely updating records, data replication, locating and caching data, and remote management.
Data Integration	
Data Loss Prevention	To guide and mitigate that end users do not send sensitive or critical information outside the corporate network.
Data Rights Management	Rights management (RM) is a subset of digital rights management (DRM), technologies that protect sensitive information from unauthorized access.
Data Warehousing	Warehousing functions that provide the capability to store very large amounts of data — usually captured from other database systems — and to perform online analytical processing on it in support of ad hoc queries.
Database Activity Monitoring	<p>Database activity monitoring (DAM) is a database security technology for monitoring and analyzing database activity that operates independently of the database management system (DBMS) and does not rely on any form of native (DBMS-resident) auditing or native logs such as trace or transaction logs. DAM is typically performed continuously and in real-time.</p> <p>Database activity monitoring and prevention (DAMP) is an extension to DAM that goes beyond monitoring and alerting to also block unauthorized activities.</p>
Database Management Service	Database Management System (DBMS) services provide controlled access to structured data. To manage the data, the DBMS provides concurrency control and facilities to combine data from different schemas. Different types of DBMS support different data models, including relational, hierarchical, network, object-oriented, and flat-file models. Some DBMSs are designed for special functions such as the storage of large objects or multimedia data. DBMS services are accessible through a programming language interface, an interactive data manipulation language interface (such as SQL), or an interactive/fourth-generation language interface. For efficiency, DBMSs often provide specific services to create, populate, move, backup, restore, recover, and archive databases, although some of these services could be provided by the general file management capabilities or a specific backup service. Some DBMSs support distribution of the database, including facilities for remotely updating records, data replication, locating and caching data, and remote management.
Database Vulnerability Management	Vulnerability management (databases) is the cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities
Encryption	Encryption services provide ways of encoding data such that it can only be read by someone who possesses an appropriate key, or some other piece of secret information. As well as providing data confidentiality for trusted communication, encryption services are used to underpin many other services including identification and authentication, system entry control, and access control services.
End user Endpoint Encryption	Endpoint Encryption, provides Eskom with strong full-disk and removable media encryption
Endpoint Security	Endpoint security refers to a methodology of protecting the corporate network when accessed via remote devices such as laptops or other wireless and mobile devices. Each device with a remote connecting to the network creates a potential entry point for security threats.
Enterprise Mobile Security	An all-encompassing approach to securing and enabling employee use of mobile devices
Enterprise Mobility	

Name	Description
Event (Incident and Problem) Management	Event Management services provide basic capabilities for the management of events, including asynchronous events, event “fan-in”, notification “fan-out”, and reliable event delivery.
File	
File Management	File Management services provide data management through file access methods including indexed sequential (ISAM) and hashed random access.
Firewall	A network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules
Geospatial	Geospatial data storage refers to both a geospatial database or flat file type of structures, optimised for and having geospatial capabilities to store, manage, edit and query geographic or geospatial data. It usually supports both vector geometry (point, line and polygons or areas) and raster or gridded data models. Some geospatial databases can handle complex structures such as topological models, networks and 3D objects.
Graphic User Interface	
Graphics & Imaging	<p>Graphics services provide functions required for creating, storing, retrieving, and manipulating images. These services include:</p> <ul style="list-style-type: none"> <li>* Graphical Object Management services, including defining multi-dimensional graphic objects in a form that is independent of output devices, and managing hierarchical structures containing graphics data. Graphical data formats include two- and three- dimensional geometric drawings as well as images.</li> <li>* Drawing services support the creation and manipulation of images with software such as GKS, PEX, PHIGS, or OpenGL.</li> </ul>
Hosting Platform	The basic hardware (computer) and software (operating system) on which software applications can be run or a base upon which other applications, processes or technologies are developed.
Hosting Platform	The basic hardware (computer) and software (operating system) on which software applications can be run or a base upon which other applications, processes or technologies are developed.
IT Asset Management Service	
Identification & Authentication	<p>Identification and Authentication services provide:-</p> <ul style="list-style-type: none"> <li>* Identification, accountability, and audit of users and their actions;</li> <li>* Authentication and account data;</li> <li>* Protection of authentication data;</li> <li>* Active user status information;</li> <li>* Password authentication mechanisms.</li> </ul>
Information Security Asset Management	Asset Manager can detect a new device as it is being attached to the network, or match a user ID to the asset it is using as soon as the user authenticates to the network.
Infrastructure Security	Is the security services provided to protect the technology infrastructure (Excludes Physical Security) especially critical infrastructure that supports the overall Eskom technology components that reside within the Data Centers inclusive of the data center's.
Inventory Management	
License Management	License Management services support the effective enforcement of software license agreements.
Local Area Network (LAN)	A local area network (LAN) is a computer network that interconnects computers within a limited area such as a residence, school, laboratory, university campus or office building.

Name	Description
Location and Directory	Location and directory services provide specialized support for locating required resources and for mediation between service consumers and service providers.
Mobile Security	Mobile Security is the Anti-Malware Services for mobile devices accessing the Eskom Network
Mobile Solutions Provisioning	
Monitoring & Management	Information systems are composed of a wide variety of diverse resources that must be managed effectively to achieve the goals of an open system environment. While the individual resources (such as printers, software, users, processors) may differ widely, the abstraction of these resources as managed objects allows for treatment in a uniform manner. The basic concepts of management — including operation, administration, and maintenance — may then be applied to the full suite of information system components along with their attendant services. System and Network management functionality may be divided in several different ways; one way is to make a division according to the management elements that generically apply to all functional resources.
Network Access Management	Network Access Management is an approach that attempts to unify endpoint security technology (such as antivirus, host intrusion prevention, and vulnerability assessment), user or system authentication and network security enforcement.
Network Infrastructure Security	Network infrastructure Security refers to the hardware and software security resources of Eskom's network that enable network connectivity, communication, operations and management.an enterprise network.
Network Security	
Network Security Platform	Network Security appliances that monitor network and/or system activities for malicious activity (NIPS)
Network Threat Behaviour Analysis	Network behavior analysis (NBA) is a way to enhance the security of a proprietary network by monitoring traffic and noting unusual actions or departures from normal operation. NBA solutions watch what's happening inside the network, aggregating data from many points to support offline analysis.
Networks Operations	Network Management services comprise elements of all the services described above, but are often treated as a separate service.
Non-Repudiation	Non-Repudiation services provide proof that a user carried out an action, or sent or received some information, at a particular time.
Object-Oriented Database Management System	Object-Oriented Database Management System (OODBMS) services provide storage for objects and interfaces to those objects. These services may support the Implementation Repository, Interface Repository, and Persistent Object services.
Object-Oriented Database Management System	Object-Oriented Database Management System (OODBMS) services provide storage for objects and interfaces to those objects. These services may support the Implementation Repository, Interface Repository, and Persistent Object services.
Office Productivity	
Office Services	
Operating System Security	Operating system security (OS security) is the process of ensuring OS integrity, confidentiality and availability in the Server Estate of Eskom.
Operating System Vulnerability Management	Vulnerability management (operating systems) is the cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities. Vulnerability management (operating systems) is the cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities

Name	Description
Performance Management	Performance Management services monitor performance aspects of hardware, platform and application software, and Network components and provide ways to tune the system to meet performance targets.
Peripheral Devices	
Printing	Printing services support output of text and/or graphical data, including any filtering or format conversion necessary. Printing services may include the ability to print all or part of a document, to print and collate more than one copy, to select the size and orientation of output, to choose print resolution, colors, and graphical behavior, and to specify fonts and other characteristics.
Privilege Access Management	
Public Key Infrastructure	A public key infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.
Query Processing functions	Query Processing functions that provide for interactive selection, extraction, and formatting of stored information from files and databases. Query processing functions are invoked via user-oriented languages and tools (often referred to as fourth generation languages), which simplify the definition of searching criteria and aid in creating effective presentation of the retrieved information (including use of graphics).
Relational Database (RDBMS)	
Report Generation functions	Report Generation functions that provide the capability to define and generate hardcopy reports composed of data extracted from a database.
Role Based Access Control	Access Control services provide:- <ul style="list-style-type: none"> <li>* Access control attributes for subjects (such as processes) and objects (such as files);</li> <li>* Enforcement of rules for assignment and modification of access control attributes;</li> <li>* Enforcement of access controls;</li> <li>* Control of object creation and deletion, including ensuring that re-use of objects does not allow subjects to accidentally gain access to information previously held in the object.</li> </ul>
Routing	
SOA Security	A service-oriented architecture (SOA) is an architectural pattern in computer software design in which application components provide services to other components via a communications protocol, typically over a network. The principles of service-orientation are independent of any vendor, product or technology.
Screen Generation functions	Screen Generation functions that provide the capability to define and generate screens that support the retrieval, presentation, and update of data.
Security	Security services are necessary to protect sensitive information in the information system. The appropriate level of protection is determined based upon the value of the information to the business area end users and the perception of threats to it. To be effective, security needs to be made strong, must never be taken for granted, and must be designed into an architecture and not bolted on afterwards. Whether a system is stand-alone or distributed, security must be applied to the whole system. It must not be forgotten that the requirement for security extends not only across the range of entities in a system but also through time. In establishing a security architecture, the best approach is to consider

Name	Description
	what is being defended, what value it has, and what the threats to it are. The principal threats to be countered are: Loss of confidentiality of data, Unavailability of data or services, Loss of integrity of data, Unauthorized use of resources.
Security Compliance Management	Compliance is either a state of being in accordance with established guidelines or specifications, or the process of becoming so – which will be applied within the Eskom environment
Security Information & Event Management (SIEM)	Security information and event management (SIEM) is an approach to security management that seeks to provide a holistic view of an organization's information technology (IT) security
Security Risk & Security Compliance	Define and assign roles critical for managing Security Risks, including the specific responsibility for information security, physical security and compliance. Establish risk and security management responsibility at the enterprise level to deal with organisation wide issues. Additional security management responsibilities may need to be assigned at a system-specific level to deal with related security issues. Obtain direction from senior management on the appetite for IT risk and approval of any residual Security Risks.
Security Risk Management	Security Risk management is the identification, assessment, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events[or to maximize the realization of opportunities. Security Risk management's objective is to assure uncertainty does not deflect the endeavor from the business goals.
Server Hardware	
Server Operating System	
Shared - On Premise	
Storage Infrastructure	
Storage Security	Storage security is a specialty area of security that is concerned with securing data storage systems and ecosystems and the data that resides on these systems.
Switching	
Threat & Vulnerability Management	
Transactional DBMS	Database Management System (DBMS) services provide controlled access to structured data. To manage the data, the DBMS provides concurrency control and facilities to combine data from different schemas. Different types of DBMS support different data models, including relational, hierarchical, network, object-oriented, and flat-file models. Some DBMSs are designed for special functions such as the storage of large objects or multimedia data. DBMS services are accessible through a programming language interface, an interactive data manipulation language interface (such as SQL), or an interactive/fourth-generation language interface. For efficiency, DBMSs often provide specific services to create, populate, move, backup, restore, recover, and archive databases, although some of these services could be provided by the general file management capabilities or a specific backup service. Some DBMSs support distribution of the database, including facilities for remotely updating records, data replication, locating and caching data, and remote management.
User Interface	User interface services define how users may interact with an application.
User Management	User Management services provide the ability to maintain a user's preferences and privileges.




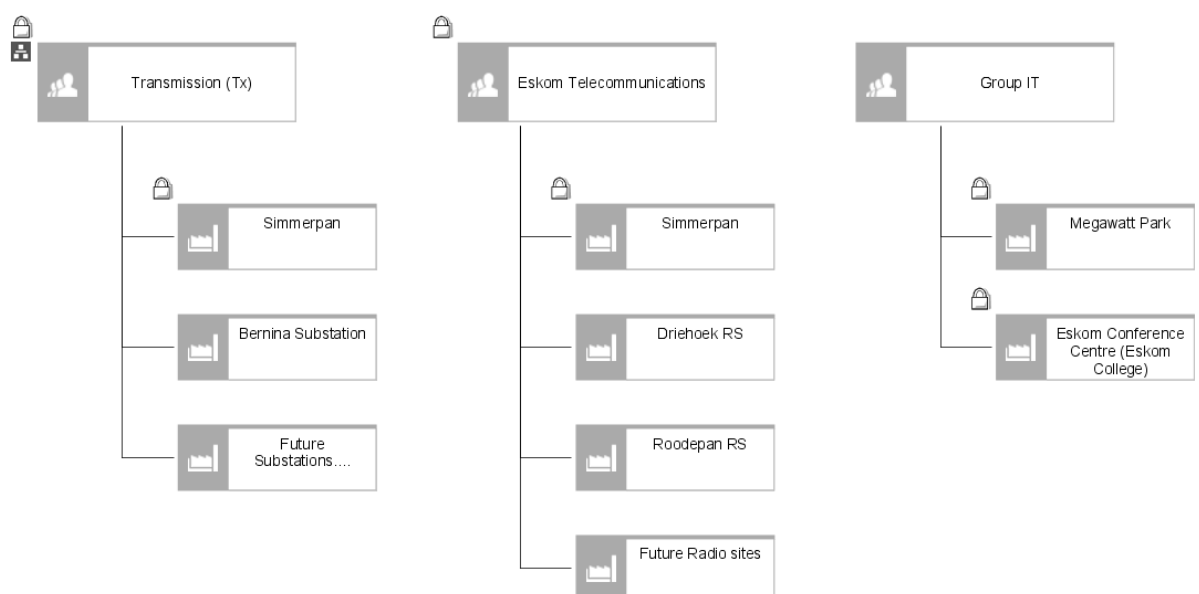
Name	Description
Virtualisation Security	Virtualization security is the collective measures, procedures and processes that ensure the protection of a virtualization infrastructure / environment.  It addresses the security issues faced by the components of a virtualization environment and methods through which it can be mitigated or prevented.
Web Services Security	Web Services security encompasses measures taken throughout the code's life-cycle to prevent gaps in the security policy of an application or the underlying system (vulnerabilities) through flaws in the design, development, deployment, upgrade, or maintenance of the application.
Wide Area Network (WAN) Operations	A wide area network (WAN) is a telecommunications network or computer network that extends over a large geographical distance.
Wireless	

## 7.2. USER LOCATIONS

The user location view describes where the users of the application are located.

### 7.2.1. Target Application User Location Diagram

Name: DEV_D3_Tx & ET Security Monitoring System_Target_202008_V01  Type: Application user location diagram Identifier: STD.26019180	Creator: solomosj Time of generation: 10 Nov 2020 8:36:46 PM Last user: solomosj Last change: 12 Nov 2020 11:59:40 AM	
--	--	---



**Figure 10: DEV\_D3\_Tx & ET Security Monitoring System\_Target\_202008\_V01 [Application User Location Diagram]**

**Table 27: Location Descriptions**

**Table 28: Organizational Unit Descriptions**

Name	Description
Eskom Telecommunications	A department in Eskom which plans and manages all telecommunication infrastructure for Eskom Holdings

Name	Description
Group IT	A department in Eskom which manages information and information technology for Eskom Holdings
Transmission (Tx)	<ul style="list-style-type: none"> <li>* Plans the development of the Transmission system</li> <li>* Manages Transmission operations, maintenance and restoration</li> <li>* Ensures optimal management of Transmission assets</li> <li>* Manages the interconnected power system</li> <li>* Plans for adequate electricity resources, buys power from Independent Power Producers (IPPs)</li> <li>* Ensures the development and execution of business opportunities in Africa</li> </ul>

## 8. DELIVERABLE ACCEPTANCE

### 8.1. DOCUMENT GENERATED

Date	Compiler	Remarks
14-11-2020	Shaun SOLOMON (solomosj)	

### 8.2. SUPPORTING MODELS

The architecture repository acts as the holding area for all architecture-related work products within the enterprise. The repository allows stakeholders to manage their deliverables, locate re-usable assets, and publish outputs to interested parties. The supporting ARIS models that relates to this architecture definition can be found at the following location(s):

Groups:

Group Path
MnGrp\Enterprise Architecture Continuum\30 Architecture Design (Development)\10 Business Projects\Tx & ET Security Monitoring System

Models:

Model Name	Model Type	ARIS QA Status	QA Run Date
DEV_D3_Tx & ET Security Monitoring System_Target_202008_V01	Application function decomposition	Passed	
DEV_D1_Tx & ET Security Monitoring System_Target_202008_V01	Risk catalog	Passed	
DEV_D3_Tx & ET Security Monitoring System_Target_202008_V01	Application user location diagram	Passed	
DEV_D1_Tx & ET Security Monitoring System_Target_202008_V01	Work package catalog	Passed	Sep 10, 2014 2:19:01 PM
DEV_D3_Tx & ET Security Monitoring System_Target_202008_V01	Stakeholder analysis diagram	Passed	Jun 27, 2014 3:21:53 PM
DEV_D1_Tx & ET Security Monitoring System_Target_202008_V01	Requirement catalog	Passed	Jul 10, 2014 1:02:21 PM
DEV_D3_Tx & ET Security Monitoring System_Target_202008_V01	Data catalog	Passed	
DEV_D3_Tx & ET Security Monitoring System_Target_202008_V01	Technology portfolio catalog	Passed	
DEV_D3_Tx & ET Security Monitoring System_Target_202008_V01	Application communication diagram	Passed	
DEV_D3_Tx & ET Security Monitoring System_Target_202008_V01	Application portfolio catalog	Passed	

### 8.3. ACCEPTANCE

This document has been reviewed and accepted by:

Name	Designation	Signature

## 9. APPENDIX

### 9.1. DEFINITIONS

Term	Definition
Architecture	A formal description of a system, or a detailed plan of the system at component level, to guide its implementation. The structure of components, their inter-relationships, and the principles and guidelines governing their design and evolution over time (TOGAF).
Architecture Development Method (ADM)	A step-by-step approach to develop and use the enterprise architecture (TOGAF).
Architecture Vision	A succinct description of the Target Architecture that describes its business value and the changes to the enterprise that will result from its successful deployment. It serves as an aspirational vision and a boundary for detailed architecture development (TOGAF).
Baseline Architecture	A specification that has been formally reviewed and agreed upon, that thereafter serves as the basis for further development or change and that can be changed only through formal change control procedures or a type of procedure such as configuration management (TOGAF).
Integration	This is the linking of multiple application systems and their subsystems to communicate together seamlessly.
Target Architecture	The description of a future state of the architecture being developed for an organization. There may be several future states developed as a roadmap to show the evolution of the architecture to a target state (TOGAF).
Work Package	A logical group of architecture development work identified to achieve one or more objectives for the business. A work package can be created as result of a business request for IT work, an approved change request, terms of reference for architecture work or from migration planning (TOGAF).

### 9.2. ABBREVIATIONS

Abbreviation	Description
ACF	Architecture Content Framework
ADM	Architecture Development Method
API	Application Programming Interface
BAM	Business Activity Monitoring
BPEL	Business Process Execution Language
BPM	Business Process Management
CAD	Conceptual Architecture Definition
CIM	Common Information Model
CRA	Concept Release Approval
DMZ	Demilitarized Zone
DRA	Design Release Approval
EAI	Enterprise Application Integration
EHPUM	Eskom High Performance Utility Model
ESB	Enterprise Service Bus
ERA	Execution Release Approval
FIFO	First In, First Out

Abbreviation	Description
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
ICoE	Integration Centre of Excellence
IDE	Integrated Development Environment
IEP	Intelligent Event Processing
IRA	Implementation Release Approval
IS	Information System
IT	Information Technology
JB1	Java Business Integration
JMS	Java Message Service
LAD	Logical Architecture Definition
LDAP	Lightweight Directory Access Protocol
PAD	Physical Architecture Definition
POJO	Plain Old Java Object
SOA	Service-Oriented Architecture
SoAW	Statement of Architecture Work
SOP	Standard Operating Procedure
SMS	Short Message Service
SQL	Structured Query Language
TBC	To Be Confirmed
TCoE	Testing Centre of Excellence
TOGAF	The Open Group Architecture Framework
UML	Unified Modelling Language
UNIX	Uniplexed Information Computing System
WP	Work Package
WSDL	Web Services Description Language
XML	Extensible Markup Language
XSD	XML Schema Definition
XSLT	Extensible Stylesheet Language Transformations

### 9.3. SYMBOL REFERENCE SHEET

Symbol Name	Symbol
Application Function*	
Application Service	
Assumption*	
Benefit	
Business Role	
Constraint*	
D Attribute (ERM)*	
Data Entity	
Data Subject Area	
Driver	
Eskom Managed Documents	
FK Attribute (ERM)*	
Function	
Generalization	

Symbol Name	Symbol
Governance Category	
Governance*	
Information System	
Interface	
K Attribute (ERM)*	
Key Performance Indicator Instance	
Location	
Logical Information Artefact	
Logical Technology Component	
Objective	
Organizational Unit	
Person	
Physical Application Component	
Physical Data Component	

Symbol Name	Symbol
Physical Hardware Technology Component	
Physical Information Artefact	
Physical Software Technology Component	
Position	
Principle	
Requirement	
Risk	
Risk Category	
Stakeholder Group	
Stakeholder Role Description	
Technology Service	
VACD Process Interface*	
Value Added Chain (EA)	
Work Package	

## **10. INDEX**

### **10.1. LIST OF FIGURES**

Figure 1: DEV\_D1\_Tx & ET Security Monitoring System\_Target\_202008\_V01 [Work Package Catalog]  
Figure 2: DEV\_D1\_Tx & ET Security Monitoring System\_Target\_202008\_V01 [Requirement Catalog]  
Figure 3: DEV\_D1\_Tx & ET Security Monitoring System\_Target\_202008\_V01 [Risk Catalog]  
Figure 4: DEV\_D3\_Tx & ET Security Monitoring System\_Target\_202008\_V01 [Application Portfolio Catalog]  
Figure 5: DEV\_D3\_Tx & ET Security Monitoring System\_Target\_202008\_V01 [Application Communication Diagram]  
Figure 6: DEV\_D3\_Tx & ET Security Monitoring System\_Target\_202008\_V01 [Stakeholder Analysis Diagram]  
Figure 7: DEV\_D3\_Tx & ET Security Monitoring System\_Target\_202008\_V01 [Application Function Decomposition]  
Figure 8: DEV\_D3\_Tx & ET Security Monitoring System\_Target\_202008\_V01 [Data Catalog]  
Figure 9: DEV\_D3\_Tx & ET Security Monitoring System\_Target\_202008\_V01 [Technology Portfolio Catalog]  
Figure 10: DEV\_D3\_Tx & ET Security Monitoring System\_Target\_202008\_V01 [Application User Location Diagram]

### **10.2. LIST OF TABLES**

Table 1: Work Package Descriptions  
Table 2: Gap Analysis  
Table 3: Requirement Descriptions  
Table 4: Gap Analysis  
Table 5: Risk Descriptions  
Table 6: Gap Analysis  
Table 7: Physical Application Component Attributes  
Table 8: Information System Descriptions  
Table 9: Physical Application Component Descriptions  
Table 10: Gap Analysis  
Table 11: Interface Descriptions  
Table 12: Physical Application Component Descriptions  
Table 13: Physical Software Technology Component Descriptions  
Table 14: Gap Analysis  
Table 15: Gap Analysis  
Table 16: Application Function\* Descriptions  
Table 17: Physical Application Component Descriptions  
Table 18: Gap Analysis  
Table 19: Reference Architectures  
Table 20: Logical Information Artefact Descriptions  
Table 21: Data Security Classification  
Table 22: Gap Analysis  
Table 23: Reference Architectures  
Table 24: Technology Landscape Descriptions  
Table 25: Technology Service Descriptions  
Table 26: Gap Analysis  
Table 27: Location Descriptions  
Table 28: Organizational Unit Descriptions  
Table 29: Gap Analysis