	<b>Group IT Business Requirement Specification (BRS)</b> DEM_2412993 & 2425114 Tx and ET Security Monitoring System	<b>Template Identifier</b>	240-83570075	Rev	6
		<b>Authorisation Date</b>	9 November 2018		
		<b>Review Date</b>	December 2021		


## SERVICE REQUEST DETAILS

<b>Business Division</b>	Transmission Central Grid Eskom Telecommunications
<b>Business Requestor(s)</b>	Gloria Mashego (Tx Representative) Nonhlanhla Nsibande (ET Representative)
<b>Business Senior Manager</b>	Harish Mohabir (Tx) Isabel Fick (ET)
<b>Demand Name</b>	2412993 Tx Central Grid Access Control System Project 2425114 ET Eskom Telecommunications Security Monitoring Pilot

### Controlled Disclosure

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

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/30.

	<b>Group IT Business Requirement Specification (BRS)</b> DEM_2412993 & 2425114 Tx and ET Security Monitoring System	Template Identifier	240-83570075	Rev	6
		Authorisation Date	9 November 2018		
		Review Date	December 2021		


## Contents

<b>1.</b>	<b>DOCUMENT TRACKER .....</b>	<b>3</b>
<b>2.</b>	<b>CUSTOMER AND STAKEHOLDER DETAILS.....</b>	<b>4</b>
2.1	Customer Information .....	4
2.2	Group IT Information.....	5
<b>3.</b>	<b>GLOSSARY OF TERMS / DEFINITIONS.....</b>	<b>6</b>
<b>4.</b>	<b>ABBREVIATIONS .....</b>	<b>8</b>
<b>5.</b>	<b>BUSINESS REQUIREMENTS SPECIFICATION FOCUS .....</b>	<b>10</b>
<b>6.</b>	<b>REASON FOR THE REQUIREMENT .....</b>	<b>10</b>
<b>6.1</b>	<b>Define the current business challenges / issues that need to be addressed .....</b>	<b>11</b>
<b>6.2</b>	<b>Define the high level gaps between the “As-Is” and “To-Be” state .....</b>	<b>12</b>
<b>7.</b>	<b>AS IS AND TO BE BUSINESS PROCESS ACTIVITY MAPPING .....</b>	<b>13</b>
7.1	As-is business process.....	13
7.2	To-Be business process .....	15
<b>8.</b>	<b>BUSINESS REQUIREMENTS .....</b>	<b>16</b>
8.1	High level Requirements.....	16
8.2	Detailed requirements and Business rules .....	16
8.3	Strategy and Methodology .....	23
8.4	Eskom Telecommunications.....	25
8.5	Data flow diagram OR Context diagram .....	26
8.6	Information/data requirements.....	31
8.7	Define the legal requirements.....	33
8.8	Intellectual Property.....	33
<b>9.</b>	<b>REPORTING REQUIREMENTS.....</b>	<b>33</b>
9.1	High level reporting requirements .....	33
9.2	Detailed reporting requirements.....	34
<b>10.</b>	<b>NON FUNCTIONAL REQUIREMENTS.....</b>	<b>37</b>
10.1	User interface requirements .....	37
10.2	Data Integrity, Confidentiality and Privacy .....	38
10.3	Device and Platform Integrity .....	38
10.4	Access Control Requirements.....	39
10.5	Threat Detection and Mitigation .....	39

### Controlled Disclosure

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

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/30.

	<b>Group IT Business Requirement Specification (BRS)</b> DEM_2412993 & 2425114 Tx and ET Security Monitoring System	Template Identifier	240-83570075	Rev	6
		Authorisation Date	9 November 2018		
		Review Date	December 2021		

10.6	Archiving requirements .....	40
10.7	Disaster recovery requirements .....	40
10.8	Business continuity requirements .....	40
10.9	Data Centers .....	40
11.	<b>TRAINING .....</b>	<b>40</b>
12.	<b>CORPORATE, DIVISIONAL AND DEPARTMENTAL PLAN ALIGNMENT .....</b>	<b>42</b>
12.1	System Integration requirements.....	42
12.2	Strategic alignment .....	42
13.	<b>REFERENCES .....</b>	<b>44</b>
14.	<b>DOCUMENT ACKNOWLEDGEMENT.....</b>	<b>46</b>
15.	<b>DOCUMENT APPROVAL .....</b>	<b>46</b>


## 1. DOCUMENT TRACKER

Date	Author Name	Changes (section changed, page number, from what to what)
20200512	Mulalo Ratsiku	Initial draft (with demand forms info)
20200513	Mulalo/Julie	Define stakeholder analysis & Reason for requirements with the customer (Julie Cheerkoot)
20200514	Mulalo Ratsiku	Document Update with functional requirements (from Standard doc)
20200515	Mulalo Ratsiku	Document Update functional requirements/ High level Requirements
20200516	Mulalo Ratsiku	Document Update (Additional requirements)
20200519	Mulalo Ratsiku	Updated the document with requested changes
20200520	Mulalo Ratsiku	High level process analysis
20200522	Mulalo Ratsiku	Document sent to stakeholders to address the comments
20200525	Mulalo Ratsiku	Consolidate feedback from stakeholders and update the document
20200526	Mulalo/Ezzard	Inclusion of Context Diagrams and Non-functional requirements
20200528	Mulalo/Julie	Document reviewed and additional Information (Confirmation of Scope, BCP and DR, and Reporting Requirements). Customer requested business requirements on section 8.2 to be changed and aligned with the standard for the physical security protection of Transmission installations
20200529	Mulalo Ratsiku	Document Update with information from Customer
20200601	Mulalo Ratsiku	Document Update
20200602	Mulalo/Ezzard	Document update with Data/Informational requirements with Ezzard de Lange and Confirmation/ alignment of scope on High level design
20200603	Mulalo Ratsiku	Updated the document with functional requirements
20200604	Mulalo Ratsiku	Finalise functional requirements, fixing alignment and Draft sent out

### Controlled Disclosure

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

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/30.

	<b>Group IT Business Requirement Specification (BRS)</b> DEM_2412993 & 2425114 Tx and ET Security Monitoring System	Template Identifier	240-83570075	Rev	6
		Authorisation Date	9 November 2018		
		Review Date	December 2021		

		to stakeholders for review
20200608	Mulalo/Julie	Addressing comments from Stakeholders
20200609	Mulalo/Julie	Addressing comments from Stakeholders / additional of Zero Control requirements from the updated Security Standard by Julie
20200610	Julie Cheerkoot	Input received from Julie (addressing Joe's comments), version updated
20200611	Mulalo Ratsiku	Document sent to Ezzard de Lange for Additional requirements and QA
20200615	Ezzard De Lange	Additional requirements and QA
20200617	Mulalo/Ezzard	Document updated with Stakeholder's input and addressing Comments (with Ezzard de Lange)
20200618	Mulalo Ratsiku	Document updated with Stakeholder's input and addressing comments
20200619	Mulalo Ratsiku	Document updated with Stakeholder's input and sent to SMEs for review
20200623	Mulalo/Julie	Document updated and sent to stakeholders
20200624	Mulalo Ratsiku	Document sent to Ezzard for Technical QA
20200629	Ezzard/Mulalo	Technical QA done by Ezzard and comments addressed by Mulalo. Document submitted to BPM for internal QA
20200702	Diane Small	BPM QA1 done by Diane
20200703	Mulalo Ratsiku	Comments addressed by Mulalo and sent to Ezzard for assistance
20200703	Mulalo/Ezzard	QA comments addressed and sent to BPM for final review
20200707	Diane Small	BRS received for BPM QA2.
20200707	Mulalo Ratsiku	QA passed and document is being sent out for acknowledgement by SMEs and approval by the Senior Managers/Sponsors

## 2. CUSTOMER AND STAKEHOLDER DETAILS


### 2.1 Customer Information

Name	Department & Division	Role / Expertise	Contact Info	Participation
Gloria Mashego	Central Grid & Transmission	Business Requestor	0152990427/ 0829532845	Demand form submission
Nonhlanhla Nsibande	Central Grid & Transmission	Business Requestor	0118713104	Demand form submission and provide technical input to business requirements
Julie Cheerkoot	Works Planning & Centralised Services: Transmission	Business Subject Matter Expert	0118004806/ 0825784672	Provide Physical Security input
Sibongile Chawe	Central Grid & Transmission	Project Manager	0118005243/ 072340 6162	Provide technical input to business

### Controlled Disclosure

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

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/30.

	<b>Group IT Business Requirement Specification (BRS)</b> DEM_2412993 & 2425114 Tx and ET Security Monitoring System	Template Identifier	240-83570075	Rev	6
		Authorisation Date	9 November 2018		
		Review Date	December 2021		

Name	Department & Division	Role / Expertise	Contact Info	Participation
				requirements
Tejin Gosai	Telecommunications: PTM (Protection Telecommunications Metering & Control) Engineering	Business Subject Matter Expert	0118712069/ 0832356494	Provide technical input to business requirements
<b>If BRS is being developed for an approved project the following additional information needs to be defined:</b>				
Harish Mohabir	Tx	Business Sponsor	0828063230/ 0118002795	Executive Support
Isabel Fick	ET	Business Sponsor	0828012843/ 0118712111	Executive Support


## 2.2 Group IT Information

Name	Department & Division	Role / Expertise	Contact Info	Participation
Mulalo Ratsiku	BPM & GIT	Group IT Business Analyst	0118002508/ 0821850585	Gather and document business requirements. Business process investigation
Themba Notununu	BRM & GIT	Group IT Business Relationship Manager	0118003963/ 0833089724	Demand registration and presentation to relevant GIT committee(s)
Carlos Betencourt	PD & GIT	Group IT Portfolio Manager	0116516721/ 0834445552	Present the BRS to relevant GIT committee(s)
Diane Small	BPM & GIT	Group IT Business Process Middle Manager	0118004049/ 0767313940	Assignment of the Business Analyst and Quality Assurance resource to a demand
Ezzard de Lange	SEA & GIT	Group IT Solution Architect	0116516879/ 0827819106	Solution design

### Controlled Disclosure

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

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/30.

	<b>Group IT Business Requirement Specification (BRS)</b> DEM_2412993 & 2425114 Tx and ET Security Monitoring System	<b>Template Identifier</b>	<b>240-83570075</b>	<b>Rev</b>	<b>6</b>
		<b>Authorisation Date</b>	<b>9 November 2018</b>		
		<b>Review Date</b>	<b>December 2021</b>		


### 3. GLOSSARY OF TERMS / DEFINITIONS

Term	Definition
Analytics	Refers to the business intelligence capability.
Business Continuity	Business continuity encompasses planning and preparation to ensure that an organisation can continue to operate in case of serious incidents or disasters and is able to recover to an operational state within a reasonably short period.
Business Intelligence	The term Business Intelligence (BI) refers to technologies, applications and practices for the collection, integration, analysis, and presentation of business information. The purpose of Business Intelligence is to support better business decision making. It can also be described as a broad set of data analysis applications, including ad hoc analysis and querying, enterprise reporting, online analytical processing (OLAP), mobile BI, real-time BI, operational BI, cloud and software as a service BI, open source BI, collaborative BI and location intelligence.
Business Requirements Specification	Business requirements specification is the eliciting, analysing and documenting of business requirements early in the development cycle to guide the design of the solution.
Business Rule	A business rule is a rule that defines or constrains some aspect of business and always resolves to either true or false. Business rules are intended to assert business structure or to control or influence the behaviour of the business. Business rules describe the operations, definitions and constraints that apply to an organization. Business rules can apply to people, processes, corporate behaviour and computing systems in an organization, and are put in place to help the organization achieve its goals.
Closed-circuit television (CCTV)	also known as video surveillance, is the use of video cameras to transmit a signal to a specific place, on a limited set of monitors
Change Request	A change request is when an enhancement is made to an existing system that meets specific criteria.
Control Site Access	The objective of Control Site Access is to ensure that only authorised individuals and carryon assets are allowed to enter and leave Eskom buildings and installations or specific designated areas (As per Manage Security Operations PCM)
External Agents	Sends information to and receive information from analysis area of study/focus area.
Heating, ventilation, and air conditioning (HVAC)	System is designed to achieve the environmental requirements of the comfort of occupants and a process. HVAC systems are more used in different types of buildings such as industrial, commercial, residential and institutional buildings
Innovation	Innovation generally refers to changing processes or creating more effective processes, products and ideas. For businesses, this could mean implementing new ideas, creating dynamic products or improving your existing services. Predominantly focuses on digitisation type projects.

#### Controlled Disclosure

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

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/30.

	<b>Group IT Business Requirement Specification (BRS)</b> DEM_2412993 & 2425114 Tx and ET Security Monitoring System	Template Identifier	240-83570075	Rev	6
		Authorisation Date	9 November 2018		
		Review Date	December 2021		


Term	Definition
Perimeter intrusion detection system	Is a device or sensor that detects the presence of an intruder attempting to breach the physical perimeter of a property, building, or other secured area.
Process	Set of activities that describe how an activity is executed.
Project	A project consists of a concrete and organized effort motivated by a perceived opportunity when facing a problem, a need, a desire or a source of. It seeks the realization of a unique and innovative deliverable, such as a product, a service, a process, or in some cases, a scientific research. Each project has a beginning and an end, and as such is considered a closed dynamic system. It is developed along the 4 Ps of project management: Plan, Processes, People, and Power. It is bound by the triple constraints that are calendar, costs and norms of quality, each of which can be determined and measured objectively along the project lifecycle. Each project produces some level of formal documentation, the deliverable(s), of course, and some impacts, which can be positive and/or negative.
Physical security	Is defined as all those measures that involve the use of physical and technological aids in the protection of assets. It is a set of tangible countermeasures designed to control the access and egress and to prevent the interruption of operations.
Pan-tilt-zoom (PTZ) camera	A pan-tilt-zoom (PTZ) camera works by moving the camera in different directions to get a whole picture of the surveillance area and zooming in for further detail of security events. The pan, tilt, and zoom capabilities make it possible to monitor large areas with a single camera while getting great detail at the same time.
Public Address System	Referred to as PA system - is an electronic system comprising microphones, amplifiers, loudspeakers, and related equipment. It increases the apparent volume (loudness) of a human voice, musical instrument, or other acoustic sound source or recorded sound or music.
Simple Network Management Protocol	Is a way for different devices on a network to share information with one another. It allows devices to communicate even if the devices are different hardware and run different software.
Software License Purchase	A software license is a legal instrument (usually by way of contract law, with or without printed material) governing the use or redistribution of software. All software is copyright protected, in source code as also object code form. The only exception is software in the public domain. A typical software license grants the licensee, typically an end-user, permission to use one or more copies of software in ways where such a use would otherwise potentially constitute copyright infringement of the software owner's exclusive rights under copyright law.
System	An organized, purposeful structure that consists of interrelated and interdependent elements (components, entities, factors, members, parts etc.). These elements continually influence one another (directly or indirectly) to maintain their activity and the existence of the system, in order to achieve the goal of the system
TCP/IP	Transmission Control Protocol/Internet Protocol is a suite of communication protocols used to interconnect network devices on the internet.

### Controlled Disclosure

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

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/30.



	<b>Group IT Business Requirement Specification (BRS)</b> DEM_2412993 & 2425114 Tx and ET Security Monitoring System	Template Identifier	240-83570075	Rev	6
		Authorisation Date	9 November 2018		
		Review Date	December 2021		

Term	Definition
Wheeling	Wheeling entails transmitting a contractual amount of power for specified time periods through the system of an operating member who is neither the seller nor the buyer of this power.

#### 4. ABBREVIATIONS


Abbreviation	Description
AAA	Authentication, Authorisation and Accounting
ACE	Analytics Centre of Excellence Department
AES	Advanced Encryption Standard
ARIS	Architecture of Integrated Information Systems
ANSI	American National Standard for Protocol Specification for Interfacing to Data Communication Networks
BCP	Business Continuity Plan
BI	Business Intelligence
BPM	Business Process Manager
BRM	Business Relationship Manager
BRS	Business Requirements Specification
CCTV	Closed-Circuit Television (also known as video surveillance)
COSEM	Companion Specification for Energy Metering
CR	Change Request
DLMS	Device Language Message Specification
DR	Disaster Recovery
DFD	Data Flow Diagram
DTLS	Datagramme Transport Layer Settings
EAP	Extensible Authentication Protocol
EIL	Electronic Incident Logbook
ET	Eskom Telecommunications
FAN	Field Area Network
FAR	False Acceptance Rate
GRE	Generic Routing Encapsulation
GIT	Group Information Technology Division, also referred to as Group IT
HVAC	Heating, ventilation, and air conditioning system
IDM	Integrated Demand Management
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IEEE Standards	Institute of Electrical and Electronics Engineers

#### Controlled Disclosure

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

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/30.




	<b>Group IT Business Requirement Specification (BRS)</b> DEM_2412993 & 2425114 Tx and ET Security Monitoring System	Template Identifier	240-83570075	Rev	6
		Authorisation Date	9 November 2018		
		Review Date	December 2021		

IPSec	IP Security
ITSO	Information Technology Service Operations
IT	Information Technology
JPC	Joint planning committee
QoS	Quality of Service
KPA	Key Performance Area
KPI	Key Performance Indicator
NCC	National Control Centre
NERSA	National Energy Regulation of South Africa
NKP	National Key Point
NLEPDS	Standard for Non-Lethal Energized Perimeter Detection System Electrical Components
NMC	Network Management Centre
OHS	Occupational Health and Safety
OT	Operations Technology
PA	Public Address System
PCM	Process Control Manual
PD	Project Delivery
PIDS	Perimeter Intrusion detection system
PSIM	Physical Security Infrastructure Management
PTZ	Pan, Tilt and Zoom camera
RSCCs	Regional Security Control Centres
SCC's	Security Control Centres
SANS standard	South African National Standard
SADC	Southern African Developing Community
SAE	Southern African Energy
SEA	Strategy Execution and Architecture
SIEM	Security Incident and Event Manager
SLA	Service Level Agreement
SIS	Strategic Intent Statement
SNMP	Simple Network Management Protocol
SOP	Standard Operating Procedure
TCP/IP	Transmission Control Protocol/Internet Protocol
Tx	Transmission Division
UI	User Interface
VLAN	Virtual Local Area Network
VMS	Video Management System
VPN	Virtual Private Network

### Controlled Disclosure

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

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/30.

	<b>Group IT Business Requirement Specification (BRS)</b> DEM_2412993 & 2425114 Tx and ET Security Monitoring System	Template Identifier	240-83570075	Rev	6
		Authorisation Date	9 November 2018		
		Review Date	December 2021		

VRF's	Virtual Routing and Forwarding
WAN	Wide Area Network

## 5. BUSINESS REQUIREMENTS SPECIFICATION FOCUS

The purpose of this document is thus to record and confirm the business requirements for:

- This is a business project and the business requirements documented in this BRS covers the full scope of the project which includes Information Technology (IT), Operational Technology (OT) as well as the Physical Security Requirements. Group IT is not held responsible for the execution of the entire project as this is a Security Project. There are some actual components that will be executed by solely IT, some jointly by IT plus business, and some strictly by business. Refer to Section 8.2 for details.
- The replacement as well as upgrade of the physical security infrastructure and physical security solutions of the Transmission Division Substations and Eskom Telecommunications High Sites, respectively.
- The scope of this initiative is therefore limited to the Transmission Division Substations and the Eskom Telecommunications High Sites.
- The proposed system must integrate with and be compatible to the following engineering standards:
  - a) 240-78980848 Standard for Non-Lethal Energized Perimeter Detection System Electrical Components (NLEPDS) and electric fencing.
  - b) 240-86738968 integrated security alarm system for protection of Eskom installations and its subsidiaries.
  - c) 240-91190304 Specification for CCTV (Closed Circuit Television Circuit) surveillance with intruder detection.
  - d) 240-102220945 Specification for IACS (Integrated Access Control System).
  - e) 240-170000098 Security PA (Public Address) systems for substations and telecommunications high sites.
  - f) 240-170000096 Physical security integration standard (site level integration), Bernina site scope of work.
  - g) 240-146054527 Information and Communications Technology Network Security Framework.
  - h) 240-140068033 Standard for IPSeC (Internet Protocol Security) in Operational Networks.


## 6. REASON FOR THE REQUIREMENT

- The aim of the required security monitoring solution is to assess the security vulnerabilities of Eskom assets to physical security risks and to reduce these vulnerabilities to acceptable levels
- The required solution will empower the business to proactively predict and respond to physical security incidents.
- The proposed solution will address the existing inadequate physical access control and CCTV systems, respectively through the availability of security incident logs and CCTV footages.

### Controlled Disclosure

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

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/30.

	<b>Group IT Business Requirement Specification (BRS)</b> DEM_2412993 & 2425114 Tx and ET Security Monitoring System	Template Identifier	240-83570075	Rev	6
		Authorisation Date	9 November 2018		
		Review Date	December 2021		

- This will assist the business to conduct comprehensive security incident investigations related to logged security breach occurrences.
- This solution will 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.


## 6.1 Define the current business challenges / issues that need to be addressed

- Recently, concerns regarding Eskom's resilience to physical security threats became apparent.
- Annual audits and assessments on physical security infrastructure, shows a clear deterioration.
- The increasing high demand for non-ferrous metals has highlighted the vulnerability of Eskom infrastructure and facilities to vandalism and theft.
- Increases in barrier intrusions have proven that current barriers are inadequate.
- The existing barriers and perimeter lighting have mostly reached the end of their life span.
- 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 Pieterboth 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.
- The physical location of substations makes substations vulnerable to criminal activities.
- 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.
- Minimal refurbishment and replacement of physical security infrastructure over the past 25 years resulted in significant occurrences of physical security incidents.
- 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.
- Significant retrofitting of security capabilities, which results in excessive costs.
- Lack of physical security standardisation across the organisation, which results in misaligned physical security designs that potentially contradict the approved physical security standards.
- Ineffective physical security monitoring and response capabilities across the organisation.
- Lack of maintenance and support for physical security systems.
- 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.
- 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.

### Controlled Disclosure

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

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/30.

	<b>Group IT Business Requirement Specification (BRS)</b> DEM_2412993 & 2425114 Tx and ET Security Monitoring System	Template Identifier	240-83570075	Rev	6
		Authorisation Date	9 November 2018		
		Review Date	December 2021		

- 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.
- A physical security infrastructure upgrade or replacement will positively contribute to both operational efficiency and realise financial savings for the organisation.
- 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.


## 6.2 Define the high level gaps between the “As-Is” and “To-Be” state

As Is Statement	To Be Statement	Therefore the high level gap is:
Business: The current physical security systems neither mitigates against the on-going prevailing physical security threats and neither does it meet Eskom’s statutory obligations as determined by the security threat and risk assessments.	The primary fence, wall and other physical barriers are required to provide the first line of defence to the premises.	There is no primary fence (demarcate and deter) that serve as a boundary to demarcate the facility to prevent people and large animals from approaching the detection system by generating nuisance alarms.
Business: There is a lack of adequate perimeter intrusion detection system at the various Eskom Telecommunications High Sites and Eskom Transmission Substations respectively.	There is a business need to implement electronic perimeter intrusion detection (i.e. sensors) to detect and deter the presence of intruders attempting to breach the physical perimeter of an Eskom property, building or other secured area.	Unavailability of electronic perimeter intrusion detection and prevention systems.
Business and IT: Inadequate CCTV systems resulted in logs and CCTV footage evidence not being available to conduct incident investigations after the occurrence of an incident.	A suitable replacement for the current CCTV systems to support proper incident investigations.	Unavailability of incident logs and CCTV footage.
Business: The current physical security measures pose a risk to the security guards and Eskom employees, as they do not provide an adequate first line of defense.	Bullet resistant guard facilities is required.	No bullet resistant guard facilities on site.

### Controlled Disclosure

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

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/30.

	<b>Group IT Business Requirement Specification (BRS)</b> DEM_2412993 & 2425114 Tx and ET Security Monitoring System	Template Identifier	240-83570075	Rev	6
		Authorisation Date	9 November 2018		
		Review Date	December 2021		

As Is Statement	To Be Statement	Therefore the high level gap is:
Business and IT: Inadequate Alarm Systems.	An integrated site alarm system, monitored from Eskom Zero Control site.	Integrate all alarms to the main physical security control room (Eskom Zero Control) through site integration.
Business: Eskom Telecommunications has approximately 471 telecommunications sites.	Upgrade the 2 Eskom Telecommunications Sites (Driehoek Radio Site and Roodepan High-Site) as part of the initial pilot physical security upgrade. In future, all Eskom Telecommunications sites will be upgraded.	
Business: Eskom Transmission has approximately 168 substation sites.	Upgrade all of the 13 Eskom Transmission NKP (National Key Point) sites as well as the critical substations.	

## 7. AS IS AND TO BE BUSINESS PROCESS ACTIVITY MAPPING

### 7.1 As-is business process

The alignment to the HPUM framework is as follows:

- ❖ Eskom High Performance Utility Model (EHPUM)
  - Level 1 Develop the Enterprise
    - Level 2 Sustainability Management
      - ◆ Level 3 Security Management
        - Level 4 Manage Security Operations
          - ✓ Level 5 Control Site Access


Manage Security Operations process PCM:

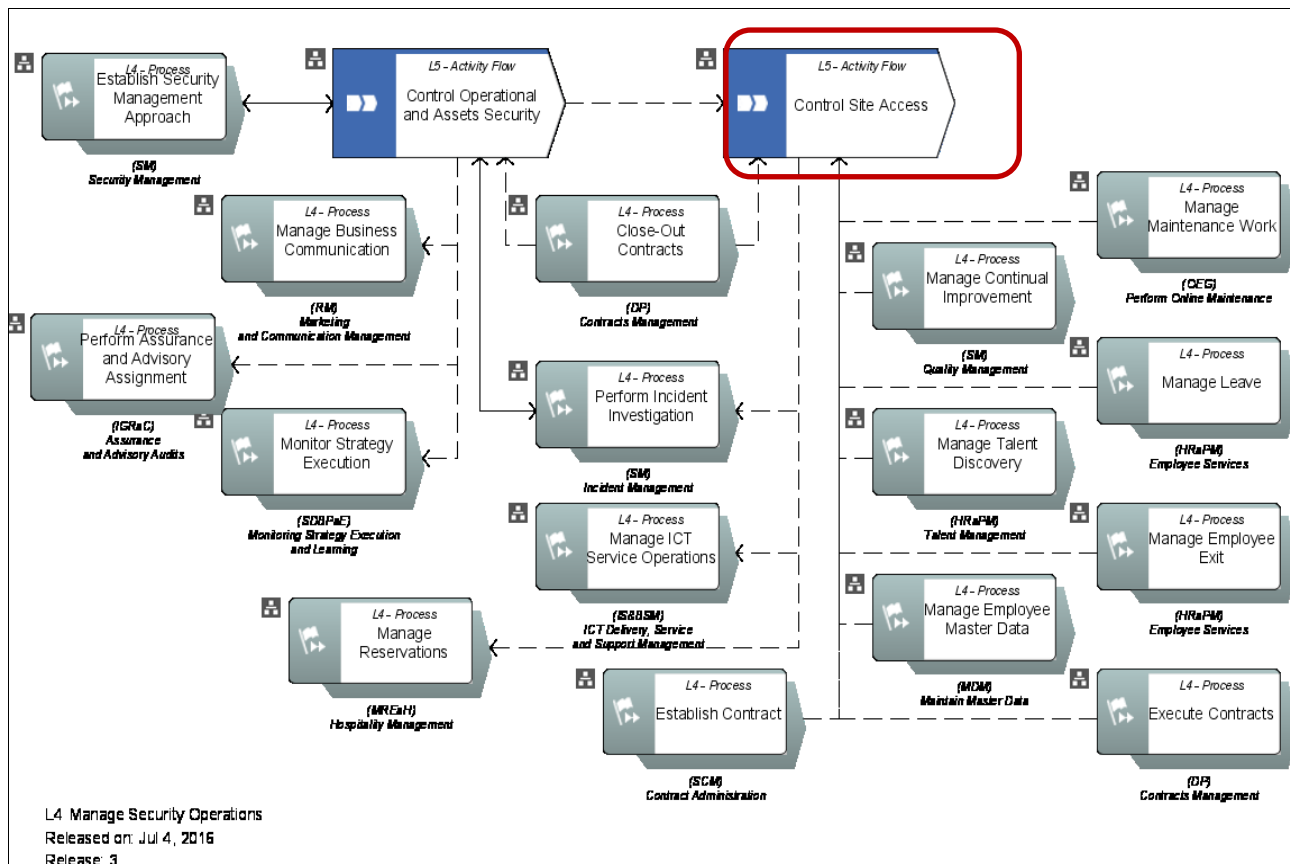
- The impacted Activity is the Control Site Access outlined in red.
- The Control Site Access process is detailed in level5 of Manage Security Operations (See Figure 2).

### Controlled Disclosure

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

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/30.

	<b>Group IT Business Requirement Specification (BRS)</b> DEM_2412993 & 2425114 Tx and ET Security Monitoring System	Template Identifier	240-83570075	Rev	6
		Authorisation Date	9 November 2018		
		Review Date	December 2021		




**Figure 1: Level 4 Manage Security Operations**

### Controlled Disclosure

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

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/30.

	<b>Group IT Business Requirement Specification (BRS)</b> DEM_2412993 & 2425114 Tx and ET Security Monitoring System	Template Identifier	240-83570075	Rev	6
		Authorisation Date	9 November 2018		
		Review Date	December 2021		

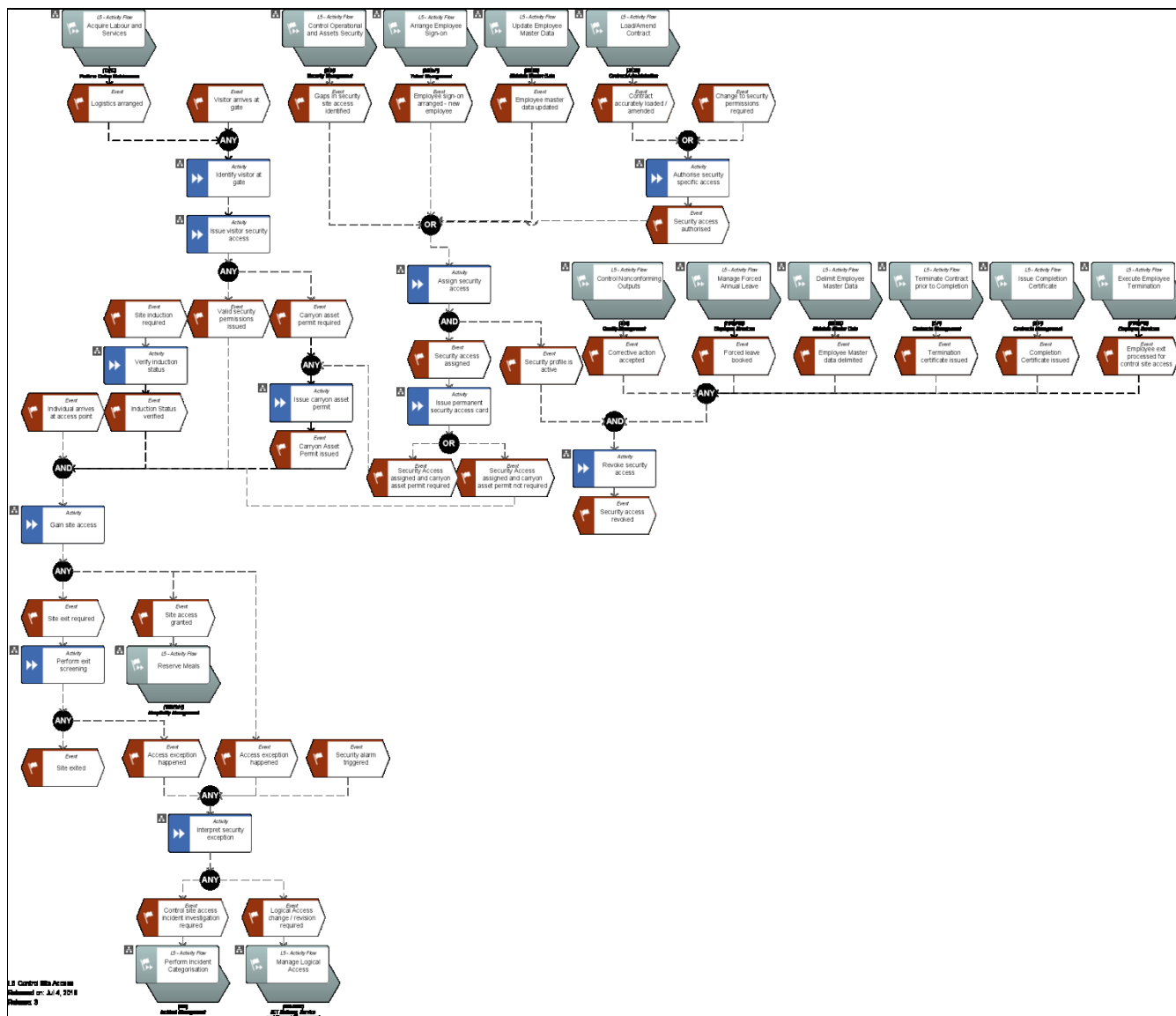


Figure 2: Level 5 Control Site Access

## 7.2 To-Be business process


The current process (Manage Security Operations PCM) is due for review, if there are changes required due to this demand, the business must log a change request to address the new changes. The changes will be resolved during review of the whole PCM.

### Controlled Disclosure

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

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/30.



	<b>Group IT Business Requirement Specification (BRS)</b> DEM_2412993 & 2425114 Tx and ET Security Monitoring System	Template Identifier	240-83570075	Rev	6
		Authorisation Date	9 November 2018		
		Review Date	December 2021		

## 8. BUSINESS REQUIREMENTS

### 8.1 High level Requirements

- The business needs an electronic intrusion detection system to detect the presence of an intruder attempting to breach the physical perimeter of an Eskom property, building or any secured area.
- An integrated physical security system is required that comprises of a combination of human resources, procedures and technologies that are successfully integrated into a single framework, which are capable of providing the required level of protection against physical security incidents that would otherwise cause damage to the facility and the associated assets.

### 8.2 Detailed requirements and Business rules

The table below illustrates the functional requirements of the security project. The functionality grouping column indicates the actual components which IT and the business will be responsible for execution thereof.

**The actual requirement components and area of responsibility for the execution are as follows:**


- Barriers – Business
- Non-lethal fence and gates – Business
- Perimeter security lighting - Business
- PISM Requirements – IT
- Bullet resistant guard facilities – Business
- Access control system – Business
- Patrol roads – Business
- Walkways – Business
- Public address system and panic buttons - Business
- Telecommunications - Business
- Control Centre functional requirements - IT plus Business
- The Security control centre - IT plus Business
- Event Management - IT plus Business
- The Video Management System (VMS) Requirements - IT plus Business
- Cybersecurity - IT plus Business
- Site power supply - IT plus Business

Functionality grouping	BRS Number	Functionality	Priority / phasing
<b>Barriers:</b> (Business)	<b>BRS 1.0</b>	The <b>outer barrier</b> security measures shall comprise of:	High
	<b>BRS 1.1</b>	A concrete wall with an intrusion detection system; or	

### Controlled Disclosure

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

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/30.


	<b>Group IT Business Requirement Specification (BRS)</b> DEM_2412993 & 2425114 Tx and ET Security Monitoring System	<b>Template Identifier</b>	<b>240-83570075</b>	<b>Rev</b>	<b>6</b>
		<b>Authorisation Date</b>	<b>9 November 2018</b>		
		<b>Review Date</b>	<b>December 2021</b>		

Functionality grouping	BRS Number	Functionality	Priority / phasing
	<b>BRS 1.2</b>	A high tensile steel fence with an intrusion detection system.	
	<b>BRS 1.3</b>	Outer barriers to consist of a concrete anti-tunnelling feature.	
	<b>BRS 1.4</b>	Double v overhang with razor coils.	
	<b>BRS 2.0</b>	The <b>inner barrier</b> security measures shall comprise of:	
	<b>BRS 2.1</b>	An inner fence consisting of welded mesh.	
	<b>BRS 2.2</b>	Single overhang.	
<b>Non-lethal fence and gates:</b> (Business)	<b>BRS 3.0</b>	Must comprise of a minimum of 5 joules throughout. Refer to section 13 for Non-Lethal Fence Specification.	High
	<b>BRS 3.1</b>	Access gates control consisting of 3 automated sliding gates; and	
	<b>BRS 3.2</b>	Emergency exits need to have the same characteristic continuous flow throughout the security measures to ensure that the integrity of the perimeter is maintained.	
	<b>BRS 3.3</b>	There will be sufficient distance between the internal and external security perimeter fence to effect maintenance.	
	<b>BRS 3.4</b>	The construction of a concrete plinth will prevent vegetation encroaching onto the electric fence.	
<b>Perimeter security lighting</b> (Business)	<b>BRS 4.0</b>	Provision of lighting to provide visibility for observation and optimum CCTV functionality. Refer to section 13 for CCTV specification.	High
	<b>BRS 4.1</b>	The perimeter security lighting will zoned. Refer to section 13 for the Security Lighting Specification.	
	<b>BRS 4.2</b>	Activation of the perimeter security lighting zones by means of a signal. Refer to section 13 for the Security Lighting Specification.	
	<b>BRS 4.3</b>	Manual activation of individual zones for testing and security purposes from the main gate security control room.	
<b>Bullet resistant guard facilities</b> (Business)	<b>BRS 5.0</b>	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 <b>guardhouse / security control room</b> will be equipped with the following:	High
	<b>BRS 5.1</b>	Kitchen.	

### Controlled Disclosure

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

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/30.


	<b>Group IT Business Requirement Specification (BRS)</b> DEM_2412993 & 2425114 Tx and ET Security Monitoring System	<b>Template Identifier</b>	<b>240-83570075</b>	<b>Rev</b>	<b>6</b>
		<b>Authorisation Date</b>	<b>9 November 2018</b>		
		<b>Review Date</b>	<b>December 2021</b>		

Functionality grouping	BRS Number	Functionality	Priority / phasing
	<b>BRS 5.2</b>	Ablution facilities.	
	<b>BRS 5.3</b>	Equipment room.	
	<b>BRS 5.4</b>	Mimic panels.	
	<b>BRS 5.5</b>	Bulletproof windows.	
	<b>BRS 5.6</b>	Hardened doors.	
	<b>BRS 5.7</b>	Air conditioning for the equipment.	
	<b>BRS 5.8</b>	Panic buttons.	
	<b>BRS 5.9</b>	Firearm safe. The Firearm safe shall integrate to the Eskom Arsenal Register.	
	<b>BRS 5.10</b>	Firearm safe making area (bullet catch).	
<b>Access control system:</b> (Business)	<b>BRS 6.0</b>	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.	High
	<b>BRS 6.1</b>	Obtain approval from the Grid in line with HV (High Voltage) Regulations for access to any Eskom Transmission or Eskom Telecommunications sites.	
<b>Surveillance and detection systems:</b> (Business)	<b>BRS 7.0</b>	The surveillance systems shall comprise of the following (Refer to section 13 for the Security Lighting Specification):	High
	<b>BRS 7.1</b>	A CCTV system with static cameras on the perimeter of the substation, with PTZ (Pan, Tilts and Zoom) capability at strategic points.	
	<b>BRS 7.2</b>	Cameras installed at key points (i.e. substation buildings and entrances) to identify both vehicles and persons.	
	<b>BRS 7.3</b>	This system should support video analytics to detect unauthorised activities.	
	<b>BRS 7.4</b>	Stream real-time video footage to Eskom Zero Control for remote monitoring.	
	<b>BRS 7.5</b>	Passive infrared beams to assist with detection of security threats to critical assets.	
	<b>BRS 7.6</b>	Capable of operating in adverse weather conditions and function effectively at day and night.	
	<b>BRS 7.7</b>	An audible siren activated during any security event triggered by any deployed physical security sensor.	
	<b>BRS 7.8</b>	Security managers/ management to view CCTV	

### Controlled Disclosure

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

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/30.


	<b>Group IT Business Requirement Specification (BRS)</b> DEM_2412993 & 2425114 Tx and ET Security Monitoring System	<b>Template Identifier</b>	<b>240-83570075</b>	<b>Rev</b>	<b>6</b>
		<b>Authorisation Date</b>	<b>9 November 2018</b>		
		<b>Review Date</b>	<b>December 2021</b>		

Functionality grouping	BRS Number	Functionality	Priority / phasing
		visuals via a remote location.	
	<b>BRS 7.9</b>	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.	
<b>Intruder Alarm systems:</b> (Business)	<b>BRS 8.0</b>	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.	High
	<b>BRS 8.1</b>	Internal alarm systems to monitor entry into the control rooms or other critical building or identified area.	
	<b>BRS 8.2</b>	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.	
<b>Patrol roads:</b> (Business)	<b>BRS 9.0</b>	Patrol roads shall consist of 3-meter gravel roads on the inside and outside of the outer perimeter barrier.	High
<b>Walkways:</b> (Business)	<b>BRS 10</b>	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
<b>Public address system and panic buttons:</b> (Business)	<b>BRS 11.0</b>	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.	High
	<b>BRS 11.1</b>	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.	
<b>Telecommunications:</b>	<b>BRS 12.0</b>	Telecommunication infrastructure shall be in place to transfer all security information from the	High

### Controlled Disclosure

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

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/30.


	<b>Group IT Business Requirement Specification (BRS)</b> DEM_2412993 & 2425114 Tx and ET Security Monitoring System	<b>Template Identifier</b>	<b>240-83570075</b>	<b>Rev</b>	<b>6</b>
		<b>Authorisation Date</b>	<b>9 November 2018</b>		
		<b>Review Date</b>	<b>December 2021</b>		

Functionality grouping	BRS Number	Functionality	Priority / phasing
(Business)		physical security systems to the remote control centre.	
<b>Alarm monitoring and response</b> (Business)	<b>BRS 13.0</b>	Detected alarms at the Control Centres are necessary to support the response plan and action by the security operators.	High
	<b>BRS 13.1</b>	Mimic panels with demarcated zones need to be available in guardhouses for guards to respond to the exact location of the alarms.	
	<b>BRS 13.2</b>	Send Eskom Telecommunication site alarms to Zero Control and NMC (Network Management Center) to alert them of events and incidents.	
	<b>BRS 13.3</b>	Send alert SMS's to the relevant security response teams when security incidents occur.	
	<b>BRS 13.4</b>	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.	
	<b>BRS 13.5</b>	Provide feedback to the security control centre to inform them of workflow progress.	
	<b>BRS 13.6</b>	Armed response contracts to be established.	
<b>PISM Requirements:</b> (IT and Business)	<b>BRS 14.0</b>	Ensure enterprise-wide integration of physical security systems.	High
	<b>BRS 14.1</b>	Collect and correlate data from multiple unconnected or diverse security subsystems and components.	
	<b>BRS 14.2</b>	Manage incidents in real time.	
	<b>BRS 14.3</b>	Proactively resolve situations by empowering the security personnel.	
	<b>BRS 14.4</b>	Creates real-time dashboards and reports.	
<b>Control Centre functional requirements:</b> (IT and Business)	<b>BRS 15.1</b>	To function as a nerve centre with monitoring, analysis and control functions.	High
	<b>BRS 15.2</b>	To maintain, sustain and improve reliable security operations effectively.	
	<b>BRS 15.3</b>	Serve Eskom Transmission and Eskom Telecommunication's sites.	
	<b>BRS 15.4</b>	Shall be self-sufficient regarding services (i.e. backup power and HVAC).	
	<b>BRS 15.5</b>	Shall present site-relevant information in a GIS (Geographical Information System) format to enhance situational awareness.	

### Controlled Disclosure

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

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/30.

	<b>Group IT Business Requirement Specification (BRS)</b> DEM_2412993 & 2425114 Tx and ET Security Monitoring System	<b>Template Identifier</b>	<b>240-83570075</b>	<b>Rev</b>	<b>6</b>
		<b>Authorisation Date</b>	<b>9 November 2018</b>		
		<b>Review Date</b>	<b>December 2021</b>		


Functionality grouping	BRS Number	Functionality	Priority / phasing
	<b>BRS 15.6</b>	The PSIM shall manage the information flow between the security control centre and its associated physical security systems.	
	<b>BRS 15.7</b>	Different SCC's (Security Control Centres) will exist, i.e. RSCCs (Regional Security Control Centres) and NSCCs (National Security Control Centres).	
	<b>BRS 15.8</b>	These Control Centres will make use of Eskom-owned Data Centre Facilities and connect via Eskom-owned Telecommunications infrastructure.	
	<b>BRS 15.9</b>	The SCCs will be responsible for monitoring and responding to its own site occurrences and incidents as well as generate notifications and alarms.	
	<b>The Security control centre shall have the following general functional requirements: (IT and Business)</b>		High
	<b>BRS 15.10</b>	Responsible for monitoring access control to the sites.	
	<b>BRS 15.11</b>	Classify incidents, apply the appropriate response and create alarms and notifications.	
	<b>BRS 15.12</b>	Manage incident response and escalate to the level of response needed.	
	<b>BRS 15.13</b>	Continuous monitoring of site perimeters.	
	<b>BRS 15.14</b>	Monitor general surveillance and anti-tampering/ sabotage observations.	
	<b>BRS 15.15</b>	Control of PTZ cameras to verify an incident as being a nuisance alarm or a real threat.	
	<b>BRS 15.16</b>	Monitor of all detection incidents.	
	<b>BRS 15.17</b>	Use the PA system to deter any threat.	
	<b>BRS 15.18</b>	Investigate user security profiles and behaviours.	
	<b>BRS 15.19</b>	Respond to emergency/ evacuation notifications.	
	<b>BRS 15.20</b>	Maintain the ELB (Electronic Incident Logbook) continuously during a shift handover and generate daily/ weekly reports.	
	<b>BRS 15.21</b>	Support regulatory compliance in all spheres of the Eskom business.	

### Controlled Disclosure

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

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/30.



	<b>Group IT Business Requirement Specification (BRS)</b> DEM_2412993 & 2425114 Tx and ET Security Monitoring System	<b>Template Identifier</b>	<b>240-83570075</b>	<b>Rev</b>	<b>6</b>
		<b>Authorisation Date</b>	<b>9 November 2018</b>		
		<b>Review Date</b>	<b>December 2021</b>		


Functionality grouping	BRS Number	Functionality	Priority / phasing
<b>Event Management</b> (IT and Business)	<b>BRS 16.</b>	Ability to replay any event or incident from the stored database for further investigation.	
<b>The VMS (Video Management System) Requirements:</b> (IT and Business)	<b>BRS 16.1</b>	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 stream the video from the site.	High
	<b>BRS 16.2</b>	Support an event queue to allow the management and acknowledgment of multiple alarm events.	
	<b>BRS 16.3</b>	It shall be possible to look at a new event without having acknowledged a previous event.	
	<b>BRS 16.4</b>	Support PTZ control including PTZ pre-set positions.	
	<b>BRS 16.5</b>	Allow the transmission of voice from the controller to the PA system on site.	
	<b>BRS 16.6</b>	Allow for the controller to control lights at the site.	
	<b>BRS 16.7</b>	Allow controller to view the location of alarms and cameras on a site layout	
	<b>BRS 16.8</b>	Allow controller to view the location and status of all sites on a map	
	<b>BRS 16.9</b>	Link comments from the controller to an event.	
	<b>BRS 16.10</b>	Enable the escalation of incidents to another workstation running the client software (e.g. another controller).	
	<b>BRS 16.11</b>	Log events and actions for auditing purposes.	
	<b>BRS 16.12</b>	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).	
<b>Cybersecurity</b> (IT plus Business)	<b>BRS 17.0</b>	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.	High
	<b>BRS 17.1</b>	Certificate-based authentication supported by an Eskom HSM (Hardware Security Module).	
	<b>BRS 17.2</b>	Eskom-owned Data Centre facilities to house the physical security management platforms.	
<b>Site power</b>	<b>BRS 18.0</b>	Supply power from a central point to all physical	High

### Controlled Disclosure

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

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/30.



	<b>Group IT Business Requirement Specification (BRS)</b> DEM_2412993 & 2425114 Tx and ET Security Monitoring System	Template Identifier	240-83570075	Rev	6
		Authorisation Date	9 November 2018		
		Review Date	December 2021		

Functionality grouping	BRS Number	Functionality	Priority / phasing
supply: (IT plus Business)		security elements.	
	BRS 18.1	Backup power is required to power the physical security equipment in the event of an unplanned power failure.	

### 8.3 Strategy and Methodology

The installations will comply with a defined SL (Security Level). The **security matrix** (see Figure 3) defines a **security level** for a substation, which in turn informs the design.

See next page


SECURITY LEVEL MATRIX							
			Threat Assessment				
			Exposure Index (EI)				
			Low	Medium	High	Critical	
Importance Assessment	Criticality Index (CI)	Critical	III	II	II	I	Critical to supply infrastructure - failure could significantly impact national supply in the short/medium term
		High	III	III	II	II	Disruption could impact local supply / achievement of business objectives in the short/medium term
		medium	IV	III	III	II	Disruption could impact local supply / effectiveness in the short term
		Low	IV	IV	III	III	Disruption could have limited short term impact on the locality / business area
			No specific vulnerability	Known vulnerability requiring limited response	Known or increasing vulnerability requiring focussed response	Specific substantial vulnerability requiring ongoing assessment and response	

Figure 3: Security Level Matrix

### Controlled Disclosure

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

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/30.

	<b>Group IT Business Requirement Specification (BRS)</b> DEM_2412993 & 2425114 Tx and ET Security Monitoring System	<b>Template Identifier</b>	<b>240-83570075</b>	<b>Rev</b>	<b>6</b>
		<b>Authorisation Date</b>	<b>9 November 2018</b>		
		<b>Review Date</b>	<b>December 2021</b>		

### Stage 1:

The matrix will assist to categorise the criticality and exposure of an asset or site:

- This matrix should be applied across the network of any particular facility to achieve service delivery and business objectives (potential consequences of losing the service). The criticality of substations are determined by means of the official ranking criteria as published by the System Operator and Planning (Unique Identifier 240-47975392) taking into consideration energy capacity, sensitivity, interdependence, cost, highest transformer rating and special equipment and should form the basis of such assessments.
- The exposure of the facility including factors such as value, sensitivity, historical threats, proximity to known threats and other significant factors (likelihood of an incident). This information is provided by Grid Security.

### Stage 2:


- Based upon the four categories (I to IV) indicated in the matrix (see Figure 3), the baseline level of security measures and response capabilities are indicated in Table 1:
- Those indicated with no differentiation utilise the same option for all the levels and NA indicates that the component will not be applied for the particular security level.

Physical Security Components	Component Options per Security Level (SL)			
	SL1 - critical	SL2 - high	SL3 - medium	SL4 - low
<b>Perimeter Barrier Components:</b>				
a) Outer perimeter barrier 2,400mm	Concrete or Double welded mesh	Double welded mesh	Double welded mesh	Razor welded mesh
b) Overhang over outer barrier	Double overhang and razor coil	Double overhang and razor coil	Double overhang and razor coil	Double overhang and razor coil
c) Inner barrier	Welded diamond mesh	Welded diamond mesh	Welded diamond mesh	Welded diamond mesh
d) Overhang on inner barrier	Single overhang	Single overhang	N/A	N/A
e) Perimeter intrusion detection system	On outer barrier	On outer barrier	On outer barrier	On outer barrier
f) Perimeter patrol roads	Gravel road	Gravel road	Foot path	Foot path
<b>Perimeter Detection and Surveillance Components:</b>				

### Controlled Disclosure

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

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/30.

	<b>Group IT Business Requirement Specification (BRS)</b> DEM_2412993 & 2425114 Tx and ET Security Monitoring System	Template Identifier	240-83570075	Rev	6
		Authorisation Date	9 November 2018		
		Review Date	December 2021		

Perimeter Lighting	No differentiation			
Detection elements	Yes	Yes	Yes	No
Energized fence (non-lethal)	No differentiation			
CCTV Cameras inclusive of PTZ	Activation with on and off site monitoring.	Activation with on and off site monitoring.	Activation with off-site monitoring.	Activation with off-site monitoring.
Access gates to suit barrier and energised fence as applicable	No differentiation			
Guard house and/or access control building	No differentiation		NA	
Access control system	No differentiation			
Alarm system	No differentiation	No differentiation	N/A	N/A
PA system and panic buttons	No differentiation			
Off-site response	Armed response	Armed response	Armed response	Armed response
On site response	Security Guards	Security Guards	N/A	N/A

**Table 1: Physical Security Components and Security Level Options**

#### 8.4 Eskom Telecommunications


The Eskom Telecommunications high sites are equally vulnerable to criminals and classified as High/ Medium or Low risk. Table 2 outlines the security measures as per the classification of the Eskom Telecommunications high site.

Physical Security Measure	ET– High Risk Site	ET– Medium Risk Site	ET– Low Risk Site
a) Double barrier fence with anti-tunneling	Yes	Yes	Yes
b) Non-lethal electrical fence	Yes	Yes	N/A
c) Audible alarm when triggered	Yes	Yes	Yes

#### Controlled Disclosure

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

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/30.

	<b>Group IT Business Requirement Specification (BRS)</b> DEM_2412993 & 2425114 Tx and ET Security Monitoring System	Template Identifier	240-83570075	Rev	6
		Authorisation Date	9 November 2018		
		Review Date	December 2021		

d) Electrified gates with special locks	Yes	Yes	N/A
e) Perimeter lighting	Yes	Yes	Yes
f) CCTV cameras inclusive of PTZ cameras	Yes, dependant on bandwidth available	Yes, dependant on bandwidth available	N/A
g) Remote alarm going through to Zero control. NMC must be alerted on events and relevant persons must be alerted via SMS on events.	Yes, through to NMC	Yes, through to NMC	Access procedure through to NMC
h) PA systems	No	No	No
i) The outer barrier to be fitted with a perimeter intrusion detection system	Yes	Yes	Yes
j) On site recording and of storage of video and local viewing and recording	Yes	Yes	No
k) Biometric access control system to replace card readers, and install CCTV at entrance of substation for positive identification	Access control through NMC	Access control through NMC	Access control through NMC
l) Panic buttons at strategic places in the control room	Yes, battery room and comms room	Yes, battery room and coms room	Yes, battery room and comms room
m) Security alarm system in control room.	Yes, comms room	Yes, comms room	No

**Table 2: ET Physical Security Components and Security Level Options**


## 8.5 Data flow diagram OR Context diagram

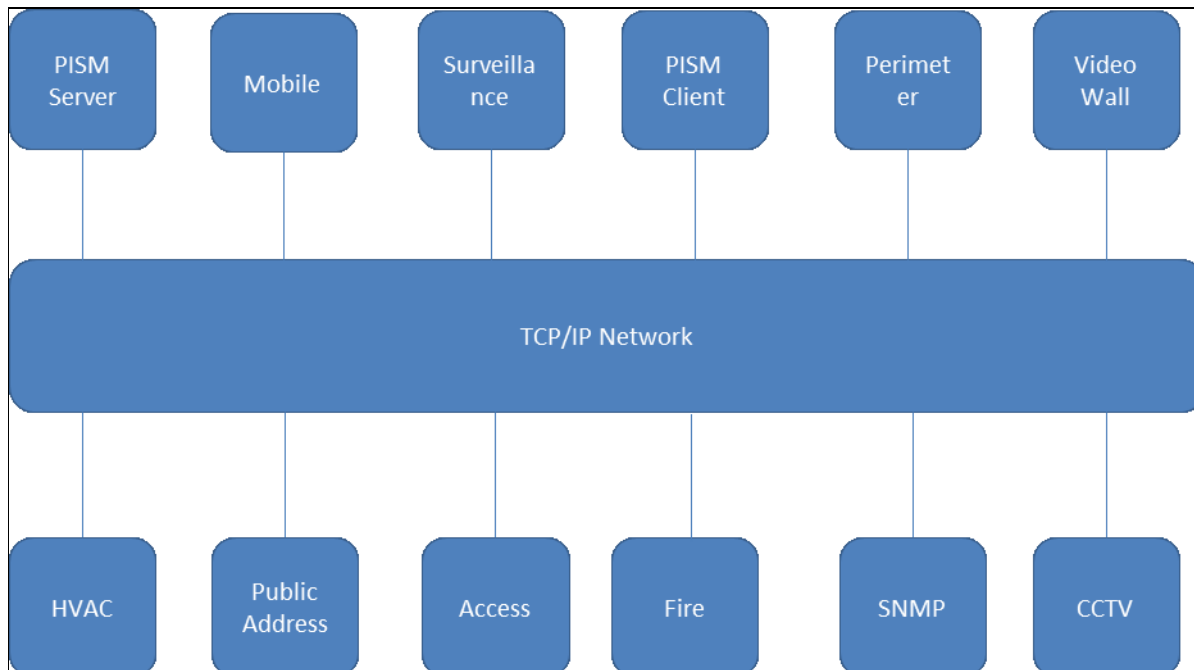
Context diagram for the proposed PSIM (Physical Security Infrastructure Management) system (The “To-Be” view), see Figure 4.

### Controlled Disclosure

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

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/30.

	<b>Group IT Business Requirement Specification (BRS)</b> DEM_2412993 & 2425114 Tx and ET Security Monitoring System	Template Identifier	240-83570075	Rev	6
		Authorisation Date	9 November 2018		
		Review Date	December 2021		



**Figure 4: PSIM (Physical Security Information Management) System**

The PSIM will be housed in an Eskom-owned Data Centre, which will form part of the Core Data Network.


Figure 5, depicts the context diagram of how the interaction between the physical security systems will happen on site.

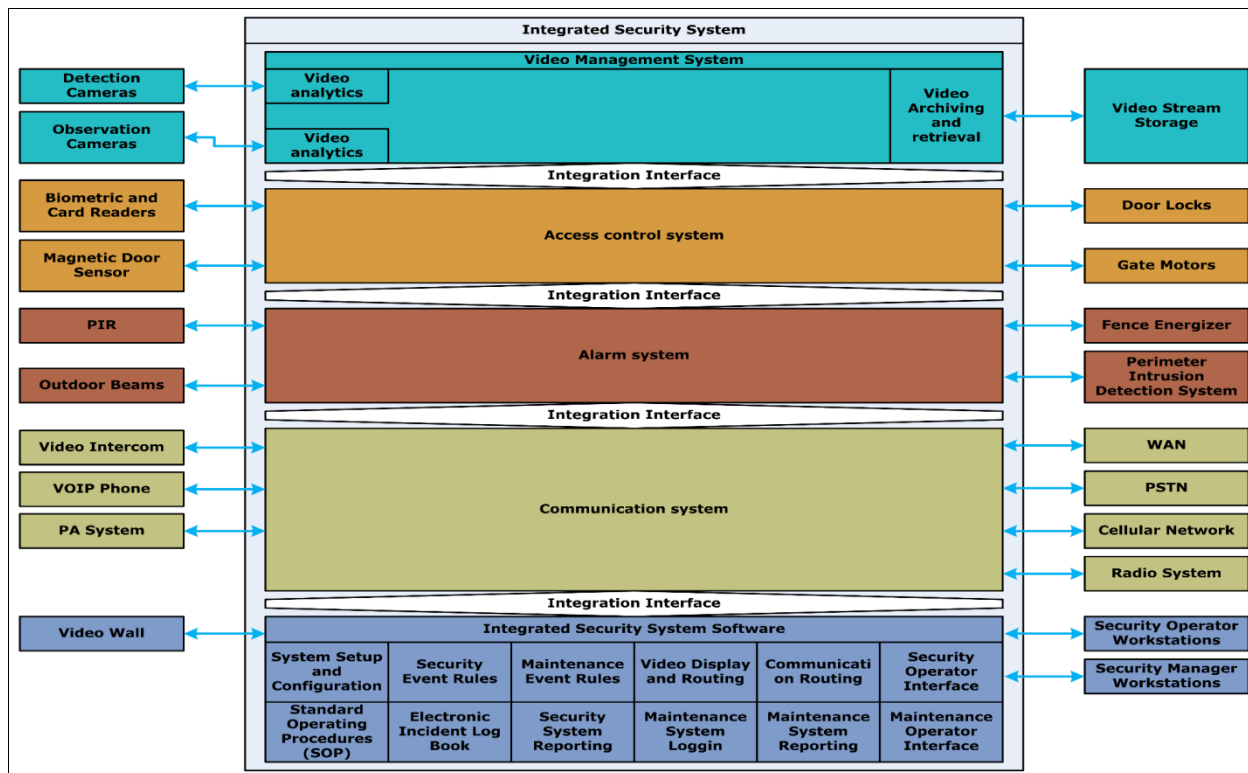
[See next page](#)

### **Controlled Disclosure**

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

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/30.

	<b>Group IT Business Requirement Specification (BRS)</b> DEM_2412993 & 2425114 Tx and ET Security Monitoring System	Template Identifier	240-83570075	Rev	6
		Authorisation Date	9 November 2018		
		Review Date	December 2021		



**Figure 5: Interaction between Physical Security Systems**


The PSIM Functional Data Flow topology is depicted in Figure 6.

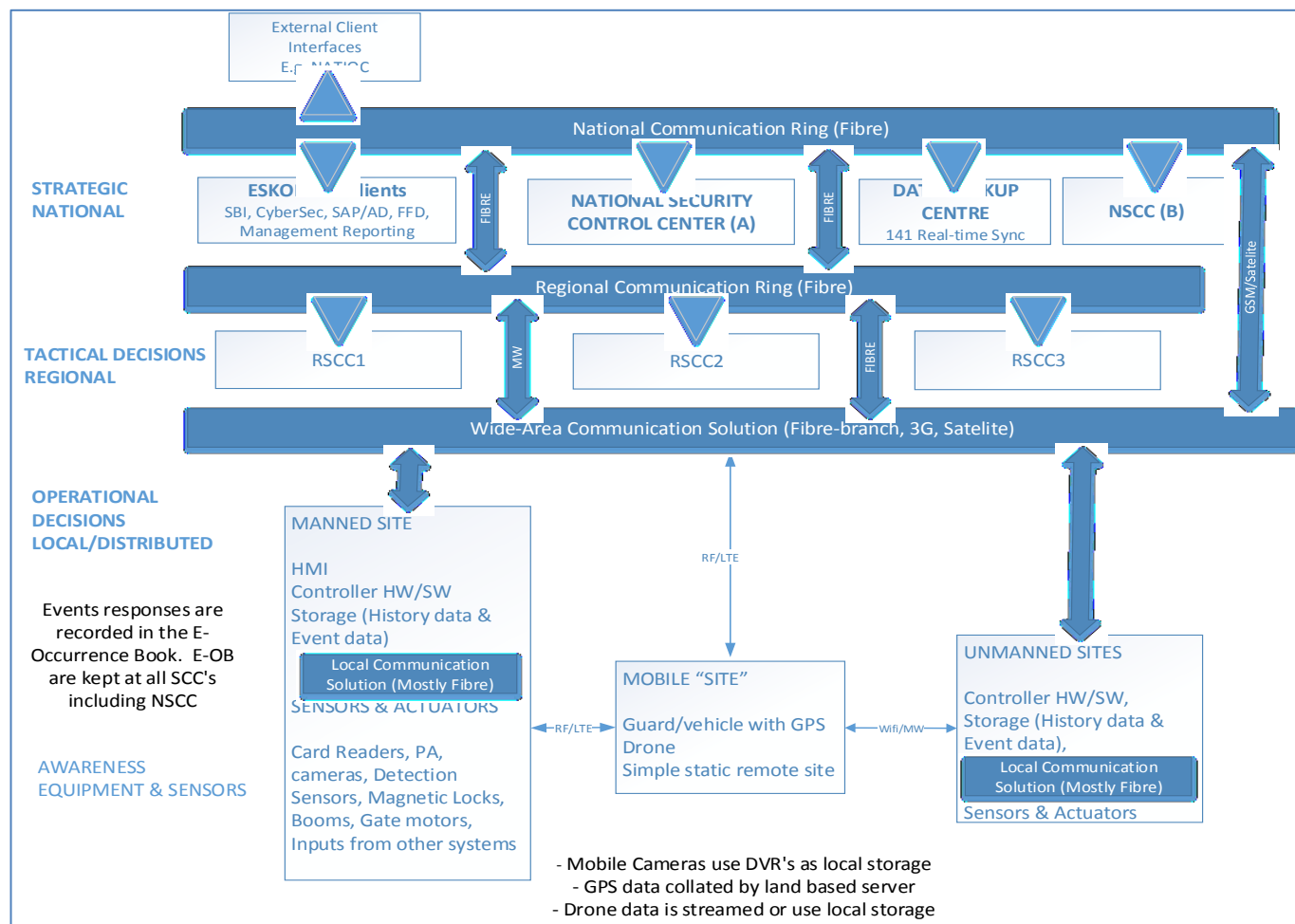
See next page

### Controlled Disclosure

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

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/30.

	<b>Group IT Business Requirement Specification (BRS)</b> DEM_2412993 & 2425114 Tx and ET Security Monitoring System	Template Identifier	240-83570075	Rev	6
		Authorisation Date	9 November 2018		
		Review Date	December 2021		



**Figure 6: PSIM Functional Data Flow Topology**

The proposed Tiered communications networks as well as the minimum security managers are depicted in Figure 7.

Figure 8 depicts the separate security zones for the IT, OT and Physical Security Systems to ensure that all traffic are managed as per their unique data and technology classification requirements.


See next page

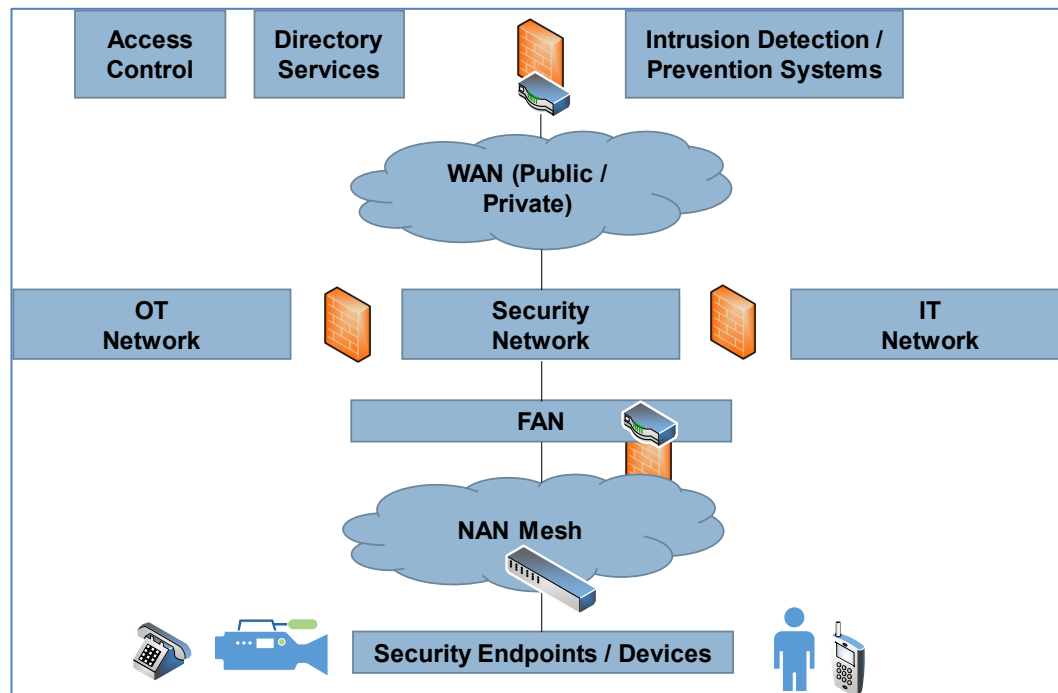
### Controlled Disclosure

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

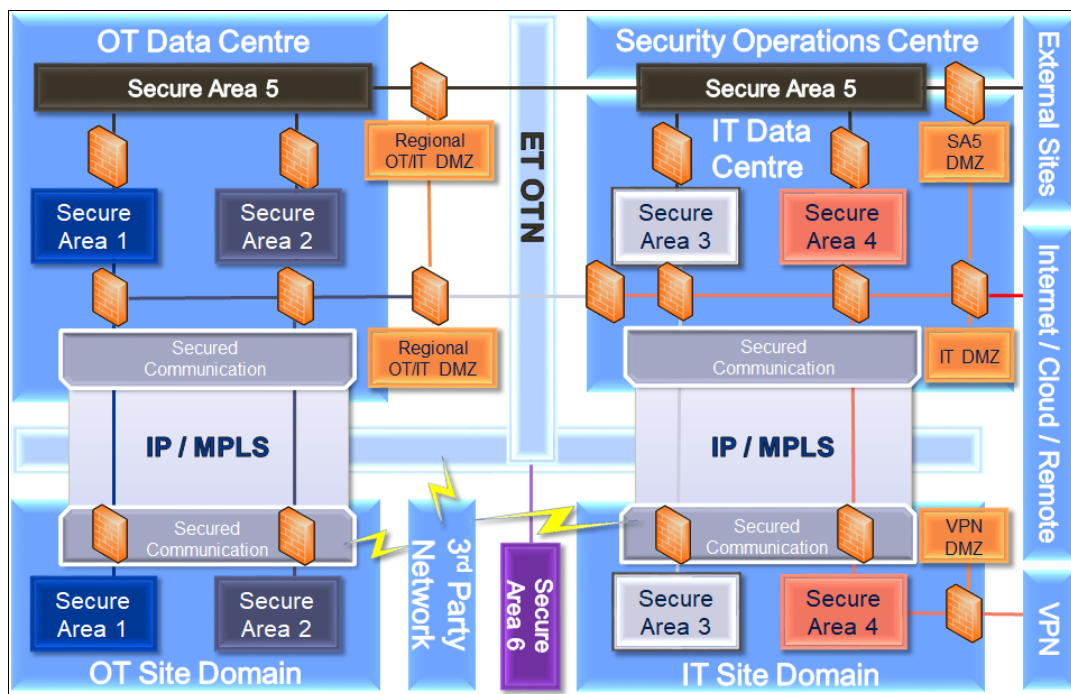
No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/30.



	<b>Group IT Business Requirement Specification (BRS)</b> DEM_2412993 & 2425114 Tx and ET Security Monitoring System	Template Identifier	240-83570075	Rev	6
		Authorisation Date	9 November 2018		
		Review Date	December 2021		



**Figure 7: Tiered Communications Network and Minimum Security Managers**




**Figure 8: Proposed Security Zones for the OT, IT and Physical Security Systems**

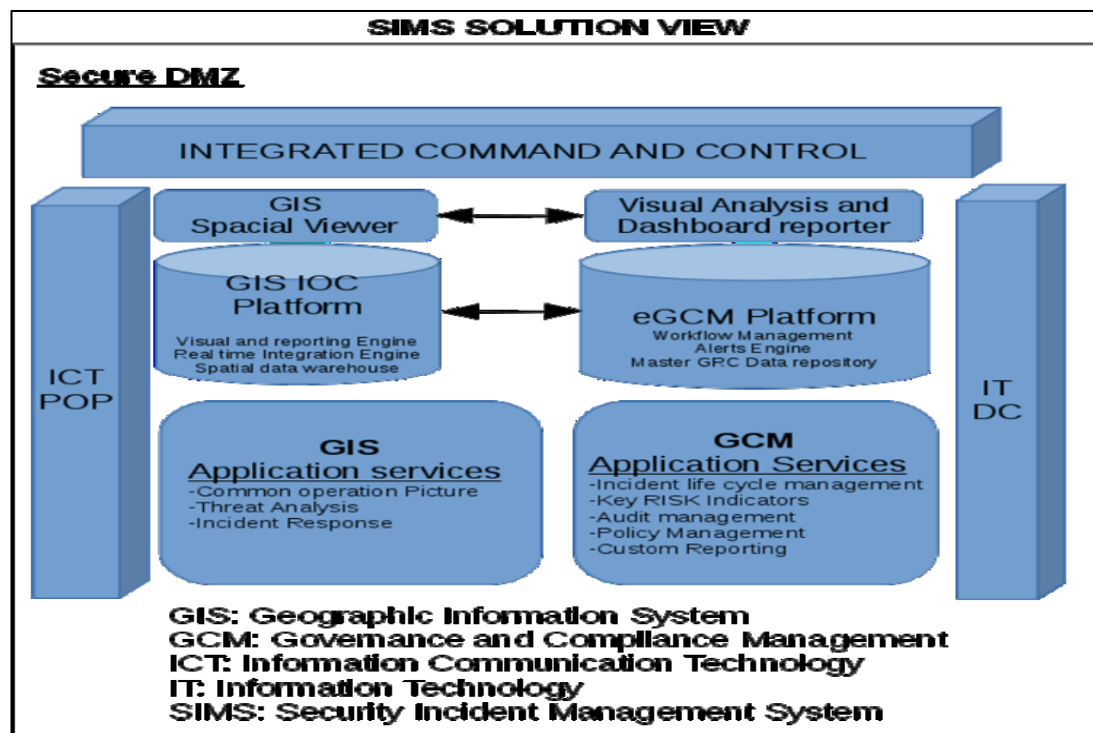
### Controlled Disclosure

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

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/30.

	<b>Group IT Business Requirement Specification (BRS)</b> DEM_2412993 & 2425114 Tx and ET Security Monitoring System	Template Identifier	240-83570075	Rev	6
		Authorisation Date	9 November 2018		
		Review Date	December 2021		

The alarms from the PSIM or individual Physical security systems will integrate with the SIMS (Security Information Management System), see Figure 9. This will ensure integration into the proposed Cybersecurity solution within Eskom, whereby the workflow of incident response and investigations can be monitored and managed on a strategic security level. This SIMS will also be integrated to the SIEM/ SOC, which is responsible for reporting and management of all Information Security alarms and alerts with the Eskom Group IT Division.



**Figure 9: SIMS (Security Information Management System) Solution Overview**


## 8.6 Information/data requirements

- The information that will be populated can be used as an input to system integration and/ or migration purposes.
- Once the architectural design is completed and approved, Table 8 will adopted for the classification criterion to decide which components of data and technology can be outsourced.
- Final approval will be obtained from the Cloud Committee.

### Controlled Disclosure

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

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/30.

	<b>Group IT Business Requirement Specification (BRS)</b> DEM_2412993 & 2425114 Tx and ET Security Monitoring System	Template Identifier	240-83570075	Rev	6
		Authorisation Date	9 November 2018		
		Review Date	December 2021		

Classification of data / information	Data / Information type	Confidentiality of information (refer to previous page for quick reference)	Confidentiality level of information (refer to previous page for quick reference)	Availability of data	Migration of data
Select from the following list: <ul style="list-style-type: none"> <li>• Use &amp; re-use (information flow)/ usage patterns</li> <li>• Information security/ risk associated with the disclosure</li> <li>• Document and record management</li> <li>• Governance &amp; legislative requirements</li> <li>• Life cycle stages</li> <li>• Add own type if not one of the above</li> </ul>	For example, financial, HR, GIS etc.	Select from the following list: <ul style="list-style-type: none"> <li>• Public domain / non classified</li> <li>• Controlled disclosure</li> <li>• Confidential</li> <li>• Secret</li> <li>• Top secret</li> </ul>	Select from the following list: <ul style="list-style-type: none"> <li>• Low</li> <li>• Medium</li> <li>• High</li> <li>• Very high – secret</li> <li>• Very high – top secret</li> </ul>	Refer to section 9.5 (in the disaster recovery section the business will advise how long they can be without data) to source the information	Is migration of data required? If so, describe the source of data.


**Table 8: Process for Classifying the Sensitivity of Technology and Information**

Table 8 will be supported by the “Classification Taxonomy” depicted in Table 9. Table 9 provides a guideline to be adopted for classifying information and data according to its unique level of sensitivity. This classification will then be presented at the Cloud Committee for approval.

### **Controlled Disclosure**

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

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/30.

	<b>Group IT Business Requirement Specification (BRS)</b> DEM_2412993 & 2425114 Tx and ET Security Monitoring System	Template Identifier	240-83570075	Rev	6
		Authorisation Date	9 November 2018		
		Review Date	December 2021		

<b>Non-Business / Personal Data</b>	<ul style="list-style-type: none"> <li>Data does not belong to the organisation.</li> <li>Data is not encrypted.</li> <li><b>Data can not be tracked nor revoked using AIP.</b></li> </ul>
<b>Public Data</b>	<ul style="list-style-type: none"> <li>Business data specifically prepared for public consumption.</li> <li>Data is not encrypted.</li> <li><b>Data can not be tracked nor revoked using AIP.</b></li> </ul>
<b>General Data</b>	<ul style="list-style-type: none"> <li>Business data, not meant for public consumption.</li> <li>Can be shared by internal employees, business guests and external partners as needed.</li> <li>Data is not encrypted.</li> <li><b>Data can not be tracked nor revoked using AIP.</b></li> </ul>
<b>Confidential Data</b>	<ul style="list-style-type: none"> <li>To be used for sensitive data that will cause business harm if over-shared.</li> <li>Recipients are trusted and get full delegation rights, i.e. the ability to remove the "encryption".</li> <li><b>Data is protected using AIP encryption; with Full Control Usage Rights.</b></li> <li>Owners can track and revoke access.</li> </ul>
<b>Highly Confidential Data</b>	<ul style="list-style-type: none"> <li>Very sensitive business data, which would certainly cause harm if over shared.</li> <li>Recipients do not get delegation rights, i.e. rights to modify or remove the "encryption".</li> <li><b>Data is protected using AIP encryption; with Reviewer Usage Rights.</b></li> <li>Owners can track and revoke access.</li> </ul>

**Table 9: Data Sensitivity Classification Taxonomy**

## 8.7 Define the legal requirements.

This is not a legal requirement but safety compliance. This BRS is supported by the OHS act legal compliance as safety of the Eskom employees and contractors is very crucial to Eskom.

## 8.8 Intellectual Property

All the data related intellectual property belongs to Eskom. Eskom to own coded integration as a perpetual licence.

# 9. REPORTING REQUIREMENTS


## 9.1 High level reporting requirements

- Ability for the system to contain a set of standard reports that can be generated.
- Ability for the system to allow for custom reports to be developed, accessed and generated from within the application.
- Both standard and custom reports should have capability of being scheduled to run at specific dates and times and/or recurring or as required.
- Ability for the system to e-mail reports from within the application.
- The reports are required to have an export/save functionality for at least the following file formats:
  - .xls &
  - .pdf

## Controlled Disclosure

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

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/30.

	<b>Group IT Business Requirement Specification (BRS)</b> DEM_2412993 & 2425114 Tx and ET Security Monitoring System	Template Identifier	240-83570075	Rev	6
		Authorisation Date	9 November 2018		
		Review Date	December 2021		

## 9.2 Detailed reporting requirements

The PSIM system, shall as a minimum, support the following reporting functions:

- Report on the login and logout actions of all workstation users. The report shall as a minimum contain the information listed in Table 3.
- Report on all site security alarm events. The report shall as a minimum contain the information listed in Table 4. The reporting function shall be able to display all security events in tabular and graphic format. It shall be possible to sort the tabular and graphical report information according to the criteria listed in Table 5. It shall be possible to search the report according to the criteria listed in Table 6.
- Report on all maintenance alarm events. The report shall as a minimum contain the information listed in Table 7. The reporting function shall be able to display all maintenance events in tabular and graphic format. It shall be possible to sort the tabular and graphical report information according to the criteria listed in Table 5. It shall be possible to search the report according to the criteria listed in Table 6.
- It shall be possible to display the report documents on the workstation display after logging into the system with the appropriate access rights.
- It shall be possible to generate a printable format document. It shall be possible to generate the report in either MS Word or Adobe PDF format.
- It shall be possible to export any tabular format data as MS Excel format for further processing by the maintenance manager.
- Report on communication infrastructure performance.


Workstation login and logout information	Description
User Name	User name of the operator that logged into the workstation
User ID number	User ID of the operator that logged into the workstation. Each user shall have a system wide unique ID.
Site ID number	Site ID defining which site the workstation is physically located on. Each site shall have a system wide unique site ID.
Workstation ID	Workstation ID identifying the workstation that was used to log in. Each workstation shall have a system wide unique workstation ID.
Date and time of login	The date and time when the user logged into the workstation
Date and time of logout	The date and time when the user logged out of the workstation
Login duration	The login duration on the workstation

**Table 3: Workstation user login and logout report information**

### Controlled Disclosure

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

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/30.

	<b>Group IT Business Requirement Specification (BRS)</b> DEM_2412993 & 2425114 Tx and ET Security Monitoring System	<b>Template Identifier</b>	<b>240-83570075</b>	<b>Rev</b>	<b>6</b>
		<b>Authorisation Date</b>	<b>9 November 2018</b>		
		<b>Review Date</b>	<b>December 2021</b>		


Security event information	Description
Security event unique number	Unique number identifying the event. This number shall be unique over all sites and the Eskom PSIM system over the lifetime of the system.
Security event criticality level	Criticality level of the security event.
Security event short description	Short description defining the security event in text.
Site ID number	Site ID number defining from which physical site location the alarm event originated from.
Sensor ID number	Sensor ID number defining from which physical sensor the alarm event originated from.
Security event routing information	<p>The event routing information shall contain all information defining the following:</p> <ul style="list-style-type: none"> <li>i.) Event date and time stamping, all critical flow points need to be time stamped. These shall include the start and the end time of events, duration before event is resolved, when the event transitions took place between operators and any point where the operator uses any communication devices to resolve the event.</li> <li>ii.) List of operators and managers the event was presented to.</li> <li>iii.) Any operator input relevant to the event.</li> </ul>
Operator action	All operator actions and feedback shall be logged including event specific notes.
Communication logging	<p>Where possible any interaction with any communication channels shall be logged, including the following:</p> <ul style="list-style-type: none"> <li>i.) Telephone numbers dialled</li> <li>ii.) Radio communication channels used</li> <li>iii.) E-mail messages sent and received</li> <li>iv.) SMS messages sent and received</li> </ul>

**Table 4: Security event report information**

### Controlled Disclosure

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

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/30.

	<b>Group IT Business Requirement Specification (BRS)</b> DEM_2412993 & 2425114 Tx and ET Security Monitoring System	Template Identifier	240-83570075	Rev	6
		Authorisation Date	9 November 2018		
		Review Date	December 2021		

Event report sorting functions	Description
Sort event report according to event type	Sort all the events according to the event type.
Sort event report according to date and time	Sort all the events according to date and time.
Sort event report according to operator	Sort all the events according to the operator assigned to for resolution.
Sort event report according to event severity level	Sort all the events according to the event severity level.
Sort event report according to a specific site location	Sort all the events according to site location

**Table 5: Event report sorting functions**

Event report search functions	Description
Search event report and filter by event type	Search through the event report for all events associated with a specific event type.
Search event report and filter by date and time	Search through the event report according to a date and or time period.
Search event report and filter by operator	Search through the event report for all the events associated with a specific operator.
Search event report and filter by event severity level	Search through the event report for all events associated with a specific severity level.
Search event report and filter by site location	Search through the event report for all events associated with a specific site location.

**Table 6: Event report search functions**


Maintenance event information	Description
Maintenance event unique number	Unique number identifying the event. This number shall be unique over all sites and the Eskom PSIM system over the lifetime of the system.
Maintenance event criticality level	Criticality level of the Maintenance event.
Maintenance event short description	Short description defining the maintenance event in text.
Site ID number	Site ID number defining from which physical site

### Controlled Disclosure

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

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/30.



	<b>Group IT Business Requirement Specification (BRS)</b> DEM_2412993 & 2425114 Tx and ET Security Monitoring System	<b>Template Identifier</b>	<b>240-83570075</b>	<b>Rev</b>	<b>6</b>
		<b>Authorisation Date</b>	<b>9 November 2018</b>		
		<b>Review Date</b>	<b>December 2021</b>		

Maintenance event information	Description
	location the alarm event originated from.
Sensor ID number	Sensor ID number defining from which physical sensor the alarm event originated from.
Maintenance event routing information	<p>The event routing information shall contain all information defining the following:</p> <ul style="list-style-type: none"> <li>i.) Event date and time stamping, all critical flow points need to be time stamped. These shall include start and end time of the event, duration before the event is resolved, when the event transitions took place between operators and any point where the operator uses any communication devices to resolve the event.</li> <li>ii.) List of operators and managers the event was presented to.</li> <li>iii.) Any operator or maintenance manager input relevant to the event.</li> </ul>
Fault report field	A fault report field that may be used to provide a detailed account of the technical aspects of the maintenance fault.
Repair report field	A repair report field that may be used to provide a detailed account of how the fault was repaired.
Maintenance event action field	<p>All actions performed to resolve the maintenance event which shall include the following:</p> <ul style="list-style-type: none"> <li>i.) Technical personnel involved in resolving the maintenance event.</li> <li>ii.) Actions performed to resolve the maintenance event.</li> <li>iii.) Any special notes relating to the specific maintenance event.</li> </ul>

**Table 7: Maintenance event report information**

## 10. NON FUNCTIONAL REQUIREMENTS


### 10.1 User interface requirements

- Graphical user interface to be user friendly and have different overlays / layers to display different system data on one screen.
- User should not need to move between screens to get a status overview of all integrated systems
- All new systems will have to be evaluated by super users of current system on this functionality.

#### Controlled Disclosure

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

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/30.

	<b>Group IT Business Requirement Specification (BRS)</b> DEM_2412993 & 2425114 Tx and ET Security Monitoring System	<b>Template Identifier</b>	<b>240-83570075</b>	<b>Rev</b>	<b>6</b>
		<b>Authorisation Date</b>	<b>9 November 2018</b>		
		<b>Review Date</b>	<b>December 2021</b>		

## 10.2 Data Integrity, Confidentiality and Privacy

- 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:
  - Layer 2 (IEEE (Institute of Electrical and Electronics Engineers) 802.15.4g or IEEE P1901.2)
  - Layer 3 IPsec (IP Security)
  - Layer 4 DTLS (Datagram Transport Layer Settings)
  - Layer 7 (ANSI C12.22 or DLMS (Device Language Messaging Specification)/COSEM (Companion Specification for Energy Metering))
- 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).


## 10.3 Device and Platform Integrity

- A basic tenet of security design is to ensure that devices, endpoints, and applications cannot be compromised easily and are resistant to cyber-attacks.
- The routers we choose should therefore be tamper-resistant mechanical designs and use IE (Industrial Ethernet).
- Routers should even have if possible a physical lock and key mechanism as well as be ruggedized where necessary.
- This makes it extremely difficult for any rogue entity to open or uninstall the device.
- Platforms should generate software and NMS alerts if the router door or chassis is opened.

### Controlled Disclosure

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

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/30.

	<b>Group IT Business Requirement Specification (BRS)</b> DEM_2412993 & 2425114 Tx and ET Security Monitoring System	Template Identifier	240-83570075	Rev	6
		Authorisation Date	9 November 2018		
		Review Date	December 2021		

- Additionally, each router motherboard should be equipped with a dedicated security chip where possible that provides:
  - Secure unique device identifier (802.1AR)
  - Immutable identity and certifiable cryptography
  - Entropy source with true randomisation
  - Memory protection and image signing and validation
  - Tamper-proof secure storage of configuration and data

#### 10.4 Access Control Requirements

- 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 centralised AAA server.


#### 10.5 Threat Detection and Mitigation

- 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).
- 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.
- 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.
- 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.

### Controlled Disclosure

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

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/30.

	<b>Group IT Business Requirement Specification (BRS)</b> DEM_2412993 & 2425114 Tx and ET Security Monitoring System	Template Identifier	240-83570075	Rev	6
		Authorisation Date	9 November 2018		
		Review Date	December 2021		

- 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).
- An important aspect of threat detection is the use of syslog and netflow information from network devices.
- 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.

## 10.6 Archiving requirements

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 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

## 10.7 Disaster recovery requirements

- 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.
- Traditionally GIT run Production and DR as a backup, but the future is High-Availability configurations.
- New Simmerpan Data Centre is recommended for Production Site and MegaWatt Park for DR site.

## 10.8 Business continuity requirements

By implementing as a minimum of a Production environment with DR as a fail-over, would imply that BCP is addressed.

## 10.9 Data Centers

PSIM will be housed in an Eskom-owned Data Centre which will form part of the Core Data Network

## 11. TRAINING


Training for System Users is required and the supplier will come and do the on-site training for all the identified users.

Tx number of System Users to be trained:

### Controlled Disclosure

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

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/30.

	<b>Group IT Business Requirement Specification (BRS)</b> DEM_2412993 & 2425114 Tx and ET Security Monitoring System	Template Identifier	240-83570075	Rev	6
		Authorisation Date	9 November 2018		
		Review Date	December 2021		

- Tx number of Users are 13 National Key Points (NKPs) and the total number to be trained is x15 Guards per NKP.
- Zero Control has x10 Security Guards to be trained.
- Additional Grid Securities are x5 per Grid (total Grid x9), x45 Guards to be trained.

ET number of System Users to be trained:


- The recommended number to be trained for pilot is x8.
- ET has identified the overall number of System Users to be trained in the near future once the system is being rolled out to all site, as per the table below:

Business Area	Role	User	Operator	Configuration
Eastern cape	Ops Manager	1		
	Senior Supervisors	4		
	Field Staff	24		
KZN	Ops Manager	1		
	Senior Supervisors	4		
	Field Staff	22		
Gauteng	Ops Manager	1		
	Senior Supervisors	4		
	Field Staff	18		
North West	Ops Manager	0		
	Senior Supervisors	2		
	Field Staff	10		
Free State	Ops Manager	1		
	Senior Supervisors	4		
	Field Staff	21		
Western Cape	Ops Manager	1		
	Senior Supervisors	4		
	Field Staff	25		
Northern Cape	Ops Manager	1		
	Senior Supervisors	3		
	Field Staff	14		
Mpumalanga	Ops Manager	1		
	Senior Supervisors	8		
	Field Staff	35		
Limpopo	Ops Manager	1		
	Senior Supervisors	4		
	Field Staff	17		
NMC (network management centre)		15	10	
Other (Engineering/SHEQ etc.)		5		5

### Controlled Disclosure

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

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/30.

	<b>Group IT Business Requirement Specification (BRS)</b> DEM_2412993 & 2425114 Tx and ET Security Monitoring System	Template Identifier	240-83570075	Rev	6
		Authorisation Date	9 November 2018		
		Review Date	December 2021		

## 12. CORPORATE, DIVISIONAL AND DEPARTMENTAL PLAN ALIGNMENT

### 12.1 System Integration requirements

The Security Monitoring System needs to integrate with the following applications/systems:

- PSIM – To integrate all the physical security elements into a single management platform if required.  
Refer to **Figure 4**
- GIT SOC (Security Operations Center) / SIEM (Security Incident and Event Management System) – To report information related security alerts and to integrate the physical security alerts as well as the logical security alerts into a single platform.
- SIMS (Security Incident Management System) – To integrate both physical security alerts and logical security alerts to the Cyber Security iSOC (integrated SOC). Refer to **Figure 9**
- Access Control System – To provide strong identity mechanisms to people and devices authenticating to the proposed solution. Refer to detail in **Section 10.4**
- AD (Active Directory Services) – For AAA (Authentication, Accounting and Authorisation) services.
- Federated CA (Certificate Authority) – For cryptography related services required for certificate-based authentication.
- IDS (Intrusion Detection System) and IPS (Intrusion Prevention System) – For intrusion detection and prevention services.


### 12.2 Strategic alignment

SIS	Supported (Y/N)	How
Provide reliable, predictable and affordable electricity in line with the approvals and regulatory model by NERSA.	Y	<p>None interruption of power supply due Security technologies that will deter criminals.</p> <p>The required security monitoring system will assist to mitigate against the significant increase in criminal incidents at the various Telecommunications and Transmission sites where copper cables, batteries, chargers as well as copper conductors have been targeted and stolen. Financial Losses due to crime will decrease (rand value and material will decrease).</p>
Ensure and maintain a financially viable	Y	Lack of a unified security strategy in Eskom,

### Controlled Disclosure

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

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/30.

	<b>Group IT Business Requirement Specification (BRS)</b> DEM_2412993 & 2425114 Tx and ET Security Monitoring System	Template Identifier	240-83570075	Rev	6
		Authorisation Date	9 November 2018		
		Review Date	December 2021		

SIS	Supported (Y/N)	How
and sustainable company.		which results in duplication of effort and costs related to Physical, Information and Cyber Security initiatives across the organization. An integrated security system is required that is formed by a combination of human resources, procedures and technology successfully integrated within a single framework capable of providing the required level of protection against incidents that would otherwise cause damage to the facility and the assets within it.
Consolidate socio-economic contribution to ensure alignment to national transformation imperatives.		
Reduce the impact on the environment.		
Ensure that company structure is responsive to changing energy landscape.		
Submit annual strategic documents and report on progress.		
Conduct reporting in line with regulatory model, with profit and loss for each licensee.		

### 12.2.1 Define the Divisional Focus areas / mandates


Transmission has a mandate to reliably control, maintain, plan, expand and provide access to an interconnected transmission system and to trade energy, influence customer demand and effect opportunities in the SADC region.

### Controlled Disclosure

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

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/30.



	<b>Group IT Business Requirement Specification (BRS)</b> DEM_2412993 & 2425114 Tx and ET Security Monitoring System	Template Identifier	240-83570075	Rev	6
		Authorisation Date	9 November 2018		
		Review Date	December 2021		

## 12.2.2 Define the Departmental Focus areas / mandates

### Telecommunications Mission Statement:


To enable Eskom's Vision through the provisioning of superior, and sustainable, Mission Critical Telecommunications Services. Together building the powerbase for sustainable growth and development.

### Grids:

To ensure Customer Satisfaction by providing a sustainable Transmission Network through operating, maintaining and restoring the Power Network.

## 13. REFERENCES


The following documents have been referenced or used to compile this Business Requirements Specification including Process Control Manual.

Number	Name	Location
240-91252315	Standard for Bullet-resistant Guard facilities	<a href="https://hyperwave.eskom.co.za/240-91252315">https://hyperwave.eskom.co.za/240-91252315</a>
240-66963836	Process Control Manual for Manage Security Control	<a href="https://hyperwave.eskom.co.za/240-66963836">https://hyperwave.eskom.co.za/240-66963836</a>
240-155981330	Physical security protection of Transmission installations	<a href="https://hyperwave.eskom.co.za/240-155981330">https://hyperwave.eskom.co.za/240-155981330</a>
240-55714363	Coal Fired Power Stations Lighting and Small Power Installation Standard	<a href="https://hyperwave.eskom.co.za/240-55714363">https://hyperwave.eskom.co.za/240-55714363</a>
Physical Security High Design (Ezzard)	 Physical Security High-Level Design.ppt	SharePoint (working document)
240-56296995	Standard for records retention periods	<a href="https://hyperwave.eskom.co.za/240-56296995">https://hyperwave.eskom.co.za/240-56296995</a>
EPSUIP-606-253	Generic Design Specification for control centres	
EPSIUP-606-262	Generic concept Design for control centres	
EPSUIP-606-256	PISM system functional Specification	

### Controlled Disclosure

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

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/30.


	<b>Group IT Business Requirement Specification (BRS)</b> DEM_2412993 & 2425114 Tx and ET Security Monitoring System	Template Identifier	240-83570075	Rev	6
		Authorisation Date	9 November 2018		
		Review Date	December 2021		

Number	Name	Location
240-86738968	Integrated security alarm system for protection of Eskom installations and its subsidiaries	<a href="https://hyperwave.eskom.co.za/240-86738968">https://hyperwave.eskom.co.za/240-86738968</a>
240-91190304	Specification for CCTV surveillance with intruder detection	<a href="https://hyperwave.eskom.co.za/240-91190304">https://hyperwave.eskom.co.za/240-91190304</a>
240-102220945	Specification for integrated access control system (IACS)	<a href="https://hyperwave.eskom.co.za/240-102220945">https://hyperwave.eskom.co.za/240-102220945</a>
240-170000098	Security public address systems for substations and telecoms high sites	<a href="https://hyperwave.eskom.co.za/240-170000098">https://hyperwave.eskom.co.za/240-170000098</a>
240-170000096	Physical security integration standard (site level integration)	<a href="https://hyperwave.eskom.co.za/240-170000096">https://hyperwave.eskom.co.za/240-170000096</a>
240-100183119	Standard for fences in Eskom Transmission Substations Unique Identifier:	<a href="https://hyperwave.eskom.co.za/240-100183119">https://hyperwave.eskom.co.za/240-100183119</a>
240-76368574	High security mesh fencing Unique identifier:	<a href="https://hyperwave.eskom.co.za/240-76368574">https://hyperwave.eskom.co.za/240-76368574</a>
240-78980848	Non-Lethal Fence Specification: Unique identifier	<a href="https://hyperwave.eskom.co.za/240-78980848">https://hyperwave.eskom.co.za/240-78980848</a>
240-139282493	Security lighting for Eskom applications: Unique identifier :	<a href="https://hyperwave.eskom.co.za/240-139282493">https://hyperwave.eskom.co.za/240-139282493</a>
240-86738968	Specification for integrated security alarm system for protection of Eskom Installations and its subsidiaries Unique Identifier:	<a href="https://hyperwave.eskom.co.za/240-86738968">https://hyperwave.eskom.co.za/240-86738968</a>

### Controlled Disclosure

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

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/30.

	<b>Group IT Business Requirement Specification (BRS)</b> DEM_2412993 & 2425114 Tx and ET Security Monitoring System	Template Identifier	240-83570075	Rev	6
		Authorisation Date	9 November 2018		
		Review Date	December 2021		

#### 14. DOCUMENT ACKNOWLEDGEMENT

By signing this document, the people listed record their agreement on the contents of this document.

*Disclaimer: Formal governance processes will need to be followed prior to obtaining approval for the implementation of the business requirements specification and the initiation of a project plan.*

Name	Role	Signature	Date
Julie Cheerkoot	Business Subject Matter Expert		
Nonhlanhla Nsibande	Business Requestor		
Mulalo Ratsiku	Group IT BPM Business Analyst		
Ezzard De Lange	Group IT Solution Architect		
Themba Notununu	Group IT Business Relationship Manager		

#### 15. DOCUMENT APPROVAL

By signing this document, the people listed record their approval on the contents of this document.


*Disclaimer: Formal governance processes will need to be followed prior to obtaining approval for the implementation of the business requirements specification and the initiation of a project plan.*

Name	Role	Signature	Date
Harish Mohabir	Senior Business Manager / Business Sponsor		
Isabel Fick	Senior Business Manager / Business Sponsor		
Diane Small	Group IT Business Process Manager		
Carlos Betencourt	Group IT Portfolio Manager		

#### Controlled Disclosure

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

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/30.

	<b>Group IT Business Requirement Specification (BRS)</b> DEM_2412993 & 2425114 Tx and ET Security Monitoring System	<b>Template Identifier</b>	<b>240-83570075</b>	<b>Rev</b>	<b>6</b>
		<b>Authorisation Date</b>	<b>9 November 2018</b>		
		<b>Review Date</b>	<b>December 2021</b>		

DEM\_2412993 BRS\_F Tx Central Grid Access Control System Project DEM\_2425114 BRS\_F ET Security Monitoring System - For Sign-Off - Message (HTML)

File Message

Ignore X Delete Reply Reply All Forward More Meeting Protect Message Tracking Move OneNote Rules Actions Mark Unread Categorize Follow Up Translate Find Related Select Zoom

Delete Respond Protection Show Move

This message was sent on 2020/07/07 08:42 PM.  
Reply Totals: Approve 8; Reject 0

Recipient	Response
Julie Cheerkoot	Approve: 2020/07/09 12:27 PM
Nonhlanhla Nsiband	Approve: 2020/07/13 09:31 AM
Ezzard De Lange	Approve: 2020/07/09 11:01 AM
Themba Notununu	Approve: 2020/07/09 11:51 AM
Diane Small	Approve: 2020/07/09 05:09 PM
Carlos Betencourt	Approve: 2020/07/09 10:54 AM
Isabel Fick	Approve: 2020/07/09 04:22 PM
Harish Mohabir	Approve: 2020/07/08 12:25 PM

Click on a photo to see social network updates and email messages from this person.

10:32 AM 2020/07/13

DEM\_2412993 BRS\_F Tx Central Grid Access Control System Project DEM\_2425114 BRS\_F ET Security Monitoring System - For Sign-Off - Message (HTML)

File Message

Ignore X Delete Reply Reply All Forward More Meeting Protect Message Tracking Move OneNote Rules Actions Mark Unread Categorize Follow Up Translate Find Related Select Zoom

Delete Respond Protection Show Move Quick Steps

This message was sent on 2020/07/09 05:24 PM.  
Reply Totals: Approve 1; Reject 0

Recipient	Response
Mulalo Ratsiku	Approve: 2020/07/09 05:25 PM

Click on a photo to see social network updates and email messages from this person.

05:27 PM 2020/07/09

### Controlled Disclosure

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

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/30.