Eskom	Report	Technology

Title: **TECHNICAL EVALUATION CRITERIA FOR THE INTEGRATED PHYSICAL SECURITY SYSTEM**

Unique Identifier:	**240-170000257**
Alternative Reference Number:	**<n/a>**
Area of Applicability:	**Engineering**
Documentation Type:	**Report**
Revision:	**2**
Total Pages:	**100**
Next Review Date:	**n/a**
Disclosure Classification:	**Controlled Disclosure**

Compiled by	Functional Responsibility	Authorized by
Donald Moshoeshoe	**Cornelius Naidoo**	**Nelson Luthuli**
Engineer – PTM&C	**Telecomms T&S CoE Manager**	**Senior Manager - PTM&C (Acting)**
Date: 22/06/2022	Date: 18/7/2022	Date: 19 July 2022

PCM Reference: **PTM&C**

SCOT Study Committee Number/Name: **Part 16 – DC & Auxiliary Supplies**

Content

Tables

1. Introduction

This document contains the technical evaluation criteria for the design, supply, installation, testing and commissioning of an integrated security system at Eskom substations. This system may comprise of the Integrated Alarm System with Intruder Detection, CCTV system, Integrated Access Control System (IACS), Public Address (PA) System, System Integration, Intrusion Pre-detection system, IT Infrastructure and PSIM (Physical Security Information Management) System.

Note: There might be projects where the scope of work includes only a subset of the systems mentioned above. In these instances the scope of work shall clearly indicate the excluded subsystems.

2. Supporting clauses

2.1 Scope

This document contains the technical evaluation criteria to be used for evaluating the tender submissions for the design, supply, installation, testing and commissioning of an integrated security system at Eskom substations. The detailed scope of work is included in the scope of work document, 240-170000258.

2.1.1 Purpose

The purpose of this document is to define the technical evaluation criteria for the design, supply, installation, testing and commissioning of an integrated security system at Eskom Substations.

2.1.2 Applicability

This document shall apply to Eskom Substations.

2.2 Normative/informative references

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

2.2.1 Normative

[1] 240-48929482: Tender Technical Evaluation Procedure

[2] 240-86738968: Specification for Integrated Security Alarm System for Protection of Eskom Installations and its subsidiaries

[3] 240-91190304: Specification for CCTV Surveillance with Intruder Detection

[4] 240-102220945: Specification for Integrated Access Control System (IACS) for Eskom Sites

[5] 240-170000258: Scope of work for Integrated Security System

[6] 240-83684419: PTM&C Technology Development

[7] 240-78980848: Specification for Non-Lethal Energized Perimeter Detection System (NLEPDS) Electrical Components

[8] 240-170000098: Security Public Address Systems for Substations and Telecoms High Sites

[9] 240-170000096: Physical Security Integration Standard

[10] 240-139282493: Security Lighting for Eskom Applications

[11] 240-170000691 Standard for Intrusion Pre-detection System used at Eskom sites

2.2.2 Informative

None.

2.3 Definitions

2.3.1 General

Definition	Description
PSIM	PSIM (Physical Security Information Management system) is a category of software that provides a platform and applications created by middleware developers, designed to integrate multiple unconnected security applications and devices and control them through one comprehensive user interface.

2.3.2 Disclosure classification

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

2.4 Abbreviations

Abbreviation	Description
CCTV	Closed Circuit Television
DVR	Digital video recorder
IACS	Integrated Access Control System
IT	Information technology
NLEPDS	Non-Lethal Energized Perimeter Detection System
NVR	Network video recorder
OEM	Original Equipment Manufacturer
PA	Public address
PSIM	Physical security information management
TET	Technical Evaluation Team

2.5 Roles and responsibilities

As per 240-48929482: Tender Technical Evaluation Procedure.

2.6 Process for monitoring

Not applicable.

2.7 Related/supporting documents

Not applicable.

3. Tender Technical Evaluation Criteria

a) The assessments are performed to assess the tenderer's capability to enter into a contract with Eskom with respect to a specific product or service and meet Eskom's requirements.

b) This report and any actions that are listed or recommended as a result of the assessments are by no means a confirmation or guarantee that any contract will be entered into by Eskom.

c) Any actions undertaken by the tenderer as a consequence of this report is for the tenderer's account. Any liability for the said actions undertaken by the tenderer is not transferrable to Eskom in any way.

d) The assessment team has no authority or responsibility in the decision taken by Eskom with respect to contracting for a product or service.

e) Any statements, intentions and/or actions expressed by the assessment team during the assessment and after the assessment should not be interpreted as the awarding of a contract and does not constitute any liability to Eskom with regards to contract placement or post-contract performance guarantees.

f) The technical evaluation method has three sub-categories: Mandatory Criteria Evaluation, Desktop Evaluation and Practical Evaluation. The detailed methodologies for scoring in each sub-category are provided in sections 3.1 to 3.3 below.

g) Tenderer's that do not achieve the minimum threshold for each of the sub-categories will not be evaluated further.

3.1 Mandatory Criteria Evaluation

This evaluation exercise is performed by the Eskom evaluating representatives. This part of the technical evaluation starts when submissions are opened for the first time. The Eskom evaluating representatives will peruse the tender submissions to ensure that the Mandatory criteria are met. Submissions that receive a "No" on any of the Mandatory criteria will not be able to proceed to the Desktop Evaluation and therefore will fail the technical evaluation.

Table 1: Mandatory Criteria Evaluation

Item	Criteria	Comply	Comments
1	**Technical schedules**		
1.1	Alarm: System: Submission of Technical Schedules A/B from the Technical specification 240-86738968 (Written in English)		
1.2	CCTV System: Submission of Technical Schedules A/B from this standard, 240-170000257, Annex A (related to technical specification 240-91190304) (Written in English)		
1.3	IACS System: Submission of Technical Schedules A/B from this standard, 240-170000257, Annex B (related to technical specification 240-102220945) (Written in English)		
1.4	PA System: Submission of Technical Schedules A/B from the Technical specification 240-170000098 (Written in English)		
1.5	Intrusion Pre-detection system: Submission of Technical Schedules A/B from the Technical specification 240-170000691 (Written in English)		
1.6	System Integration: Submission of Technical Schedules A/B from the Technical specification 240-170000096 (Written in English)		
1.7	IT Infrastructure and PSIM: Submission of the Technical Schedule from the Microsoft Excel spreadsheet, titled “Consolidated spreadsheet PSIM Evaluation Criteria rev2.14 Update1”, sheet “Master Evaluation Criteria” that are part of the tender pack documents issued by Eskom. The overview of the scoring on the Microsoft Excel spreadsheet is listed in this standard, 240-170000107, Annex C. All schedules must be written in English.		
1.8	Supplier Services and Organisation Experience: Compliance with Technical Schedules A/B from this standard, 240-170000257, Annex D.		
2	**PSIRA registration**		
2.1	Submission of PSIRA registration certificate.		
	Threshold	**Compliance to all of the above**	

3.2 Desktop Evaluation

Submissions that obtain a minimum pass mark of 60% for the Desktop Evaluation (Table 2) shall proceed to the Practical Evaluation.

a) The evaluation process for the desktop evaluation will involve the evaluation of individual systems as listed in Table 2, that is the Alarm System (with Intruder Detection) (10%), CCTV (15%), IACS (10%), PA system (5%), Intrusion pre-detection (10%), System Integration (15%), IT Infrastructure and PSIM system (20%), Supplier Services and Organisational Experience (5%) and System Design Report (10%).

b) The Desktop Evaluation shall comprise scoring of the Technical Schedules A/B from the different specifications and the Annexures in this document. The details are listed in Table 2.

c) The Technical Schedules A/B use a default weight of 1 for each scored item. Critical items are assigned higher weights. For example, a weight of 3 indicates that the item will count the same as three items with weight 1.

d) Each item will be assigned a score by the Eskom evaluation team based upon the tendered response and cross-checked with the supporting documents provided. The scoring shall follow section 3.4, Table 4.

e) The scoring method for the IT Infrastructure and PSIM evaluation shall follow the method stated in the Technical Schedule in the Microsoft Excel spreadsheet, "Consolidated spreadsheet PSIM Evaluation Criteria rev2.14 Update1", sheet "Master Evaluation Criteria" that are part of the tender pack documents issued by Eskom.

f) Failure to submit responses to the Technical Schedules A/B will result in the tender scoring zero % for Desktop Evaluation.

g) For the Desktop Evaluation, tenderers are required to indicate compliance to the requirements listed in the Technical Schedules A/B that will be provided in the accompanying Microsoft Excel files and will be required to provide supporting evidence/documentation where applicable.

h) Tenderers are expected to state clearly, for each clause that requires a statement of compliance in the Technical Schedules A/B, either "Comply" or "Do not comply".

i) If a clause in the Technical Schedule A/B requires a statement of compliance and additional information e.g. a description etc., tenderers are requested to state clearly either "Comply – followed by Evidence and References in support of compliance – i.e. explanations, document reference (title, paragraph/page number).

j) Any deviations from the technical specifications should be indicated in the deviations schedules provided.

Table 2: Scoring criteria and weighting for each system for the Desktop Evaluation

	Technical Criteria Description	Criteria Weighting (%)	Criteria Sub Weighting (%)
1.	**Alarm System**	**10**	
1.1	Compliance with Technical Schedules A/B in the Technical specification 240-86738968. (Full compliance = 179 x 3 x weight = 537 points (i.e. 100%).		100
2.	**CCTV**	**15**	
2.1	Compliance with Technical Schedules A/B from this standard 240-170000257, Annex A (related to Technical specification 240-91190304). (Full compliance = 401 x 3 = 1203 points (i.e. 100%).		100
3	**IACS**	**10**	
3.1	Compliance with Technical Schedules A/B from this standard, 240-170000257, Annex B (related to Technical specification 240-102220945). (Full compliance = 335 x 3 = 1005 points (i.e. 100%).		100
4.	**PA System**	**5**	
4.1	Compliance with Technical Schedules A/B in the Technical specification 240-170000098. (Full compliance = 69 x 3 = 207 points (i.e. 100%).		100
5	**Intrusion Pre-detection System**	**10**	

5.1	Compliance with Technical Schedules A/B in the Technical specification 240-170000691. (Full compliance = 134 x 3 = 402 points (i.e. 100%).		100
6	**System Integration**	**15**	
6.1	Compliance with Technical Schedules A/B in the Technical specification 240-170000096 . (Full compliance = 90 x 3 = 270 points (i.e. 100%).		100
7	**IT Infrastructure and PSIM**	**20**	
7.1	Compliance with the Technical Schedules from the Microsoft Excel spreadsheet, titled “Consolidated spreadsheet PSIM Evaluation Criteria rev2.14 Update1”, sheet “Master Evaluation Criteria” that are part of the tender pack documents issued by Eskom. The overview of the scoring on the Microsoft Excel spreadsheet is listed in this standard, 240-170000107, Annex C.		100

	Technical Criteria Description	Criteria Weighting (%)	Criteria Sub Weighting (%)
8	**Supplier Services and Organisation Experience**	**5**	
8.1	Compliance with Technical Schedules A/B from this standard, 240-170000257, Annex D. (Full compliance = 18 x 3 = 54 points (i.e. 100%)).		100
9	**System Design Report** The tenderer is required to produce and submit a System Design Report covering at a minimum the following (refer to Annex B of 240-170000258 for the report index):	**10**	
9.1	Overview of the overall design and detailing each of the different components (sub-systems)		15
9.2	System architecture (Logical and Physical designs) including the integration of the different components (sub-systems).		35
9.3	Cause and Effect matrix of the overall system to be provided.		10
9.4	Schematics displaying the location of each component's (sub-systems) sensor (e.g. CCTV, alarm contacts, etc)		20
9.5	Equipment list of all the different components (sub-systems)		10
9.6	Equipment Data Sheets		10
	TOTAL:	**100**	
T	**Threshold** *(minimum 60% to qualify for practical evaluation)*	**60**	

Note: The scoring criteria and weighting is Table 2 above should be applied where the project scope includes all the system listed. For projects with only a subset of security systems listed, the weighting method depicted in Annex F shall be used for evaluations.

3.3 Practical evaluation

A threshold of 70% is required for the tenderer to pass the Practical (Demonstration) Evaluation (Table 3).

a) The purpose of testing at this phase is to test whether the equipment proposed is capable of meeting the specifications. To this end, equipment needs to be demonstrated to meet the functional requirements. These tests need not be carried out on site. They may be carried out on equipment already installed on a 3rd party site by the tenderer or setup at the local OEM's or Tenderer test facilities for demonstration purposes.

b) The evaluation of the demonstration will be based on the requirements listed in the 'Demonstration Evaluations' schedule listed in Annex E of this document.

c) During the demonstration, the tenderer shall demonstrate how the different functional and technical requirements have been incorporated in the system design (refer to 'Demonstration Evaluation' in Annex E).

d) The Tenderer shall use the offered equipment/system to demonstrate how Eskom's requirements are met. The test system shall be configured so as to represent the architecture envisaged for the complete solution.

e) It is the responsibility of the tenderer to have complete demo units and test instruments available. The tenderer will be responsible to do all testing and programming required by Eskom.

f) The tenderer will be required to setup a demonstration system comprising of the following system components:

1) Alarm System (including the pre-detection system)

2) CCTV

3) IACS

4) PA Systems

5) Intrusion pre-detection system

6) Integration of systems (Alarm system, CCTV system, IACS, PA system, pre-detection system, IT and PSIM systems)

7) IT Infrastructure and PSIM

g) Each item will be assigned a score by the Eskom evaluation team based upon the tendered response and cross-checked with the supporting documents provided. The scoring shall follow section 3.4, Table 4.

h) The total score for the Practical evaluation will be expressed as a percentage of the maximum possible score from each of the different systems listed in Table 3 below. The weighted percentages (listed in Table 3) of each of the different systems will be added to obtain an overall score out of a 100%. This score value will be recorded in Table 3.

i) The scoring method for the IT Infrastructure and PSIM evaluation shall follow the method stated in the sheet labelled “System Demo” from the Microsoft Excel spreadsheets, titled “Consolidated spreadsheet PSIM Evaluation Criteria rev2.14 Update1” that are part of the tender pack document issued by Eskom.

j) The tenderer will be informed in advance to arrange and facilitate for the practical evaluation to take place.

Note: Eskom will conduct only one evaluation per OEM equipment submitted in the tender. Where multiple Tenderers use the same OEM for equipment, only one practical evaluation will be conducted. All the Tenderers using that OEM’s equipment will receive the same score for the Practical Evaluation.

Table 3: Scoring criteria for Practical Evaluation

	Technical Criteria Description	**Criteria Weighting (%)**	**Criteria Sub Weighting (%)**
1	Alarm System	**10**	
1.1	Testing of the Alarm System will follow section 1 in Annex E from this standard, 240-170000257 and calculated out of 100%. Full compliance = 20 x 3 = 60 points (i.e. 100%).		100
2	CCTV	**15**	
2.1	Testing of the CCTV System will follow section 2 in Annex E from this standard, 240-170000257 and calculated out of 100%. Full compliance = 42 x 3 = 126 points (i.e. 100%).		100
3	IACS	**15**	

	Technical Criteria Description	Criteria Weighting (%)	Criteria Sub Weighting (%)
3.1	Testing of the IACS System will follow section 3 in Annex E from this standard, 240-170000257 and calculated out of 100%. Full compliance = 12 x 3 = 36 points (i.e. 100%).		100
4	PA System	**5**	
4.1	Testing of the PA System will follow section 4 in Annex E from this standard, 240-170000257 and calculated out of 100%. Full compliance = 7 x 3 = 21 points (i.e. 100%).		100
5	Intrusion pre-detection system	**10**	
5.1	Testing of the Intrusion pre-detection System will follow section 5 in Annex E from this standard, 240-170000691 and calculated out of 100%. Full compliance = 19 x 3 = 57 points (i.e. 100%).		100
6	System Integration	**20**	
6.1	Testing of the Integrated System will follow section 6 in Annex E from this standard, 240-170000257 and calculated out of 100%. Full compliance = 54 x 3 = 162 points (i.e. 100%).		100
7	IT Infrastructure and PSIM	**20**	
7.1	Testing of the IT Infrastructure will follow the sheet “System Demo” from the Microsoft Excel spreadsheet, titled “Consolidated spreadsheet PSIM Evaluation Criteria rev2.14 Update1” that is part of the tender pack documents issued by Eskom. The overview of the scoring on the Microsoft Excel spreadsheet is listed in this standard, 240-170000107, Annex C.		100
8	Supplier Services & Organisation Experience	**5**	
8.1	Testing of the Supplier Services & Organisation Experience will follow section 7 in Annex E from this standard, 240-170000257 and calculated out of 100%. Full compliance = 6 x 3 = 18 points (i.e. 100%).		100
	TOTAL:	**100**	
	Threshold *(minimum 70% to pass the practical evaluation)*	**70**	

Note: The scoring criteria and weighting is Table 3 above should be applied where the project scope includes all the system listed. For projects with only a subset of security systems included in the scope, the weighting method depicted in Annex F should be used for evaluations.

3.4 Scoring Method

Each item will be assigned a score by the Eskom evaluation team based upon the tendered response/demonstrated functionality and cross-checked with the supporting documents provided (where applicable). The scoring method is depicted in Table 4 below:

Table 4: Scoring method for integrated security system

Criteria	Score
Fully compliant • Meet technical requirement(s) AND; • Cross-checked with the supporting documents provided (where applicable) AND; • No foreseen technical risk(s) in meeting technical requirements	3
Partially compliant (minor deviation) • Does not meet all the technical requirement(s) AND/OR; • Unacceptable technical risks(s) AND/OR; • Unacceptable exceptions AND/OR; • Unacceptable conditions. • No supporting documents provided.	1
Non-compliant (major deviation) • Totally deficient or non-responsive	0

4. Authorisation

This document has been seen and accepted by:

Name and surname	Designation
Tony Sheerin	Manager – Project Planning and Support

5. Revisions

Date	Rev	Compiler	Remarks
June 2022	2	R Moshoeshoe	Included requirements for Intrusion pre-detection system
June 2021	1	R Moshoeshoe	First issue

6. Development team

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

- Tejin Gosai

7. Acknowledgements

Not Applicable

Annex A – Technical Schedules A/B for the CCTV

(related to technical specification 240-91190304)

TECHNICAL SCHEDULES A & B FOR

SPECIFICATION FOR CCTV SURVEILLANCE WITH INTRUDER DETECTION STANDARD IN ACCORDANCE WITH ESKOM STANDARD 240-91190304

Schedule A: Purchaser's specifications

Schedule B: Guarantees, compliance and technical particulars of equipment offered

The clauses and numbering in this table are not necessarily the verbatim clauses as per 240-91190304. Therefore it is OBLIGATORY on the TENDERER to review the applicable clauses in 240-91190304 in order to provide an informed response.

When completing the Schedule B and the References section, The Tenderer is required to state clearly, for each clause that requires a statement of compliance, with one of the following options:

Comply – Confirmation of FULL Compliance to all clauses of the applicable section of the Technical Standard. No deviations

Partially Comply – Confirmation of PARTIAL Compliance and that FULL Compliance is not possible. Deviations taken.

Do Not Comply - Conformation of Non-Compliance to ALL requirements in the applicable section

Reference to evidence in the form of datasheets, equipment manuals, drawings, hyperlinks shall be included in the References section if required.

Where there are any deviations taken from the clauses in the applicable section, these should be indicated under the References and Deviations section.

	Description	Schedule A	Schedule B (Supplier's statements of compliance)	References/ Statement (supporting evidence) & Deviations
3.6	Installation			
3.6(a)	To ensure quality workmanship and sound installation practice, it is imperative that the contractor adheres to the specifications and standards supplied by Eskom.	Comply		
3.6(b)	Only contractors with experience in CCTV and alarm system installations shall do installations. To this end the tenderer shall provide a CV of relevant experience and references.	Comply and provide supporting evidence		

3.6l	All installers shall adhere to the OHS Act (Occupational Health and Safety Act) of 1970 when installing the system. Contractors and sub-contractors shall meet the requirements specified by Eskom Health and Safety specifications	comply		X
3.6(d)	All equipment shall have a mechanical earth connected to the site earth according to Eskom standards.	comply		X
3.6(e)	All equipment shall be designed and specified for a minimum realisable operational life 10 years under the prevailing environmental conditions unless otherwise agreed to by Eskom during the tender evaluation stage.	comply and provide the design MTBF (Mean Time Between Failures)		
3.6(f)	Consideration must be given for the minimum working and electrical clearances of overhead equipment – see Eskom Specification 34-3–4 - Substations, Section 2: Generic Substation Design [–] - section 4.5.1.2	comply		X
3.6(g)	All equipment shall be labelled in accordance with the design diagrams, with durable, weather resistant labels.	comply		X
3.6(h)	Cable and wiring marking shall be in accordance with Eskom standard 240-64636794, Standard for Wiring and Cable Marking in Substations.	comply		X
3.6(i)	All cables and wires shall be marked with a unique identification, at all terminations, in accordance with the cabling and wiring diagrams supplied.	comply		X
3.6(j)	All of the splices and connections shall be mechanically secure and shall provide electrical contact without stress on connections and terminals.	comply		X
3.6(k)	Any hole which insulated conductors pass through shall be provided with a smooth, rounded bushing, or shall have smooth, rounded surfaces upon which the insulated conductors may bear.	comply		X
3.6(l)	Wireways shall be smooth and free from sharp edges, burrs, fins, or moving parts that may damage wiring.	comply		X
3.6(m)	All internal wiring connections shall be made with a solder lug or pressure terminal connector	comply		X

3.6(n)	A terminal lug shall be arranged such that in any position it cannot contact the metal enclosure, non-energized accessible metal parts or other electrical circuits. Alternatively the shank of the lug shall be provided with insulation equivalent to that of the conductor.	comply		
3.6(o)	Terminal blocks shall be in accordance with Eskom standard 240-70413291, Specification for Electrical Terminal Blocks.	comply		
3.6(p)	The CCTV installation shall be signed off as accepted by Eskom's appointed Project Engineer for the security system installation.	comply		
3.7	System Level			
3.7.1	System Overview			
3.7.1.1	On site			
3.7.1.1(g)(i)	On site different subsystems will communicate with various controllers (DVR, Alarm panel, PA controller etc.) using a combination of hardwired contacts and communication busses (RS232, Ethernet, proprietary protocols etc.). These controllers will communicate with each other as necessary to create a system which can meet the functional requirements set forth in this document.	comply		
3.7.1.1(g)(ii)	At manned sites there may also be a security monitoring station on site from which CCTV and alarms can be viewed.	comply		
3.7.1.1(g)(iii)	The security equipment cabinet shall also serve as the point of power distribution for the security equipment which may need a variety of combination of AC and DC power at various voltage levels.	comply		
3.7.1.2	Eskom Local OT Security Server			
3.7.1.2(i)	All sites with CCTV systems will communicate with a Local OU Security Server. This server shall be owned and hosted by Eskom. VMS server software will be housed here as well as other server related equipment such as alarm base stations.	comply		
3.7.1.2(ii)	If necessary due to budget/resource availability, the server can be hosted at a third party	comply		
3.7.1.3	Local Security Control Centre			

3.7.1.3(i)	The Local Security Control Centre shall be responsible for responding to alarms from sites and managing incidents on site using the CCTV data from site. Ideally the Local Security Control Centre should be an Eskom manned centre, but budget and resource restraints may necessitate that the control centre be provided by a third party. Network security between any 3rd parties and the Eskom Network shall be designed and controlled by Eskom.	comply		
3.7.1.3(ii)	The Security Control Centre shall use approved VMS client software to connect to the Eskom OT Security Server, thereby receiving all alarm signals from the various sites (black screen monitoring). The Local Control Centre shall also be able to receive video on demand from the sites via the OT Security Server.	comply		
3.7.1.3(iii)	The connection between the Local OT Security Server and the Local Security Control Centre shall be a dedicated link (e.g. a Diginet line / microwave link). There may also be a backup links directly between the Local Security Control Centre and sites if this is deemed necessary.	comply		
3.7.1.4	National Security Control Centre			
3.7.1.4(i)	Eskom intends to establish an Eskom National Security Control Centre from which selected security incidents can be managed and monitored. A communication link would be established from the local OU security servers to the National Control Centre server via the Eskom corporate LAN. Selected signals or events would then be directed to the National Security Control Centre. It shall be possible to escalate events from the Local Security Control Centre to the National Security Control Centre.	comply		
3.7.1.5	Engineering and Operational Access			
3.7.1.5(i)	Eskom engineers shall be able to connect to the Local OT Security Server remotely from the Eskom Engineering (OT) LAN to perform maintenance and administrative tasks on the system.	comply		

3.7.1.5(ii)	Members of Eskom Group Security shall be able to connect to the OT security server remotely from the Eskom corporate network in order to perform operational tasks (check up-time of systems, confirm sites are being armed etc.) and investigations (view footage and alarm logs etc.).	comply		
3.7.1.5(iii)	This remote access shall be restricted to those who have explicitly been granted access rights.	comply		
3.7.3	Warrantee and Certification			
3.7.3(a)	All equipment installed shall be subject to the OEM warrantee	comply & provide OEM agreement letter		
3.7.3(b)	Contractor shall provide proof that technicians have been trained and certified to install and configure the CCTV equipment specified.	comply & provide training certificates for technicians		
3.7.3(c)	There shall be an agreement from the OEM that the OEM supports the tender offering and will continue to support the product if the tenderer defaults.	comply & provide OEM support agreement		
3.7.4	General Physical Requirements			
3.7.4.1	Environmental conditions			
3.7.4.1(a)	Ambient air temperature: -25 °C to +55 °C (installed indoors); or -25 °C to +70 °C (installed outdoors, within enclosures).	comply and provide reference		
3.7.4.1(b)	Altitude: < 2 500 m	comply and provide reference		
3.7.4.1(c)	Pollution: Location in urban areas with industrial activities and without special precautions to minimize the presence of sand or dust (conditions as per classes 3C2 and 3S2 in IEC 60721-3-3[12]).	comply and provide reference		
3.7.4.1(d)	Relative humidity (24h average): 98%	comply and provide reference		
3.7.4.1(e)	All outside equipment Including fasteners and supports should be corrosion resistant and appropriate for the environment on site	comply and provide reference		
3.7.4.1(f)	After fabrication, metal surfaces including doors and removable covers shall be prepared and finished with corrosion protection.	comply and provide reference		

3.7.4.1(g)	Paint work damaged during transport and delivery shall be made good as per manufacturer repair specification at no cost to Eskom. If site re-painting is necessary, the equipment and labels shall be carefully masked and any overpaint which occurs in spite of the masking must be removed. If the damage is not repairable, Eskom reserves the right to return the equipment.	comply		
3.7.4.1(h)	All nuts, bolts and washers use for the construction to be stainless steel. Screws can be cadmium plated.	comply		
3.7.4.1(i)	Further environmental protection may be needed e.g. Equipment installed at a coal power station or in a mining area will need added dust protection.	comply		
3.7.4.1(j)	Convection cooled (fan-less) equipment are strongly preferred. If fans are used, they shall be speed controlled and the electronics shall be isolated and conformal coated to protect against dust ingress.	comply and provide reference		
3.7.5	General Electrical Requirements			
3.7.5(a)	The expected life of equipment under conditions specified (section 3.7.4.1 above) shall be a minimum of 10 years.	comply and provide the design MTBF (Mean Time Between Failures)		
3.7.5(b)	All power cable shall be appropriately sized to ensure voltage drops along cable runs remain within the operating specifications of the equipment being powered.	comply		
3.7.5 (c)	All equipment shall be effectively protected against overvoltage due to lighting strikes or switching surges by strategically placed surge arrestors	comply		
3.7.5(d)	Descriptive cable markings shall be used as agreed to with Eskom. These shall be reflected on the drawings.	comply		
3.7.5(e)	Cable selection and routing shall always be done in such a way that operation of equipment is not affected by electrical interference. This may be achieved by separating power and communications cables, shielding of cables, or a combination of the two.	comply		
3.7.5(f)	Equipment shall not be affected by electrostatic discharges that are applied directly to the equipment or to metal objects in the proximity of the equipment: All electronic equipment shall be a class 2 device as specified in IEEE 1613-2009, 8 Electrostatic discharge tests[24]	comply and provide reference		

3.7.6	Cable routes in control plant / equipment rooms:			
3.7.6(a)	Auxiliary power cables shall be laid in the control room power rack, away from communication cables. No conduit is needed on the rack.	comply		
3.7.6(b)	Communications cables should use the control plant room communications rack. No conduit is needed on the rack.	comply		
3.7.6(c)	Where cable racks are not available, cables may be routed along the wall or in PVC sleeves in the cable trench, at Eskom's discretion.	comply		
3.7.6(d)	Where security cables are routed along the walls, they shall be in metal or plastic conduit.	comply		
3.7.6(e)	Auxiliary power and communication cables shall be in separate conduit.	comply		
3.7.6(f)	In substations, security cables shall not be routed in the ceiling.	comply		
3.7.6(g)	If fibre optic leads are used they should be protected usi19unctiogue tubing when entering and exiting cable trays or panels.	comply		
3.7.6(h)	Regional or site specific requirements may supersede the above cable route requirements.	comply		
3.7.7	Outdoor Cables and Trenching in Substations			
3.7.7(a)	Security cable should share control cable or lighting trenches where possible, where this is not possible, security cable trenches shall be dug.	comply		
3.7.7(b)	The security cables shall enter the control plant room through the same path as control cables.	comply		
3.7.7(c)	Security cable trenches shall be 0,5 m deep	comply		
3.7.7(d)	All cables shall be armoured or laid in appropriately sized plastic conduit (e.g. HDPE, Kabelflex, whether in cable trenches or dedicated security trenches. The appropriate bends and connectors must be used for the conduit, according to manufacturer's instructions.	comply		
3.7.7(e)	Security systems communication cables and auxiliary power cables shall not be laid in the same conduit unless using fibre communication or DC power.	comply		

3.7.7(f)	Drilled holes in junction boxes shall be kept to a minimum and shall be appropriately sealed to prevent water ingress.	comply		
3.7.7(g)	Care shall be taken when working with fibre optic cable so as to ensure the fibre is not damaged during installation or maintenance.	comply		
3.7.7(h)	The stone layer shall be removed far enough from the cable trench excavation as illustrated in 6. The trench soil shall not be placed on top of any yard stone.	comply		
3.7.7(i)	After the cables have been laid, the trenches must be backfilled with the original soil in layers not exceeding 300mm and properly compacted. Once the backfill is completed, the stone shall be replaced appropriately.	comply		
3.7.8	Security Cabinet			
3.7.8(i)	The security cabinet/panel shall contain all the control equipment of the intruder detection and the surveillance system (digital video recorder (DVR), communication equipment, public address (PA) etc.). The cabinet shall be housed within a suitable access controlled equipment room.	comply		
3.7.8(a)	The cabinet shall comply to Eskom Standard 240-6072564“, "Specification for Standard (19 inch) Equipment Cabin”ts". The Cabinet shall be a freestanding standard equipment cabinet (600 x 600). For servers, a freestanding server cabinet shall be provided.	comply		
3.7.8(b)	Cabinet shall be designed so as to limit dust ingress which could affect effective operation of equipment.	comply		
3.7.8(c)	All points of cable entry shall be through glands so as to secure the cables.	comply		
3.7.8(d)	Access to the inside of the cabinet shall be restricted and controlled by means a physical lock to which only authorized security personnel and Eskom employees from the Risk Department shall have access. Cabinet shall be alarmed for tempering and remain armed when main alarm system is disarmed. This is subject to regional requirements.	comply		
3.7.8(e)	Cabinet design shall take into consideration airflow and heat distribution. Equipment shall be laid out such that units that generate the most heat are at the top.	comply		

3.7.8(f)	There shall be a dedicated Aux power supply distribution module with a suitably sized incomer isolator and suitably sized load MCBs per piece of equipment	comply		
3.7.8(g)	The incomer supply DB MCB for this module must be correctly sized to protect the incomer cable in order to prevent nuisance trips.	comply		
3.7.8(h)	Cables shall be neatly routed in trunking.	comply		
3.7.8(i)	Cable ties or similar shall be used for cable management.	comply		
3.7.8(j)	Where possible equipment in the security cabinet shall be 19 inch rack	comply		
3.7.8(k)	Equipment or connection accessed regularly shall be accessible from the front of the panel or shall be wired to a terminal rack accessible from the front.	comply		
3.7.8(l)	Equipment shall be suitably earthed to the cabinet, and the cabinet shall be earthed to the substation earth.	comply		
3.7.8(m)	Eskom shall approve the layout design before the cabinet is populated.	comply		
3.7.9	Backup Power Supply			
3.7.9(i)	The responsible Eskom DC design engineer shall be consulted on a per site basis to determine which power supply system will be used and to allocate connection MCB's on the main Distribution Board.	comply		
3.7.9(ii)	The supply shall include a battery backed up UPS for all security system devices.	comply		
3.7.9(iii)	The standing time for backup power is 12 hours at sites within 200kms of a responsible Eskom DC section, 18 hours at sites more than 200kms from a responsible Eskom DC section.	comply for 12 hours		
3.7.9.1	Option A: 220V DC			
3.7.9.1(a)	The security system shall be powered by 220V supplied from the site's DC supply. In the event of a power failure the system will be supplied by the substation's battery and / or generator backup.	comply		
3.7.9.1(b)	The security system shall be supplied by an appropriately sized supply cable and MCB from the site's DC panel.	comply		
3.7.9.1c)	The MCB used on the AC/DC panel shall be clearly labelled 'Security'.	comply		

3.7.9.1(d)	Power will be distributed through the panel so as to isolate the supply of the subsystems by means of appropriately sized MCBs. At a minimum the following will be on separate supply circuits:			
	i. Intruder detection system	comply		
	ii. Perimeter Cameras	comply		
	iii. DVR, Indoor cameras and PTZ	comply		
	iv. Perimeter detection system (if separate from perimeter cameras)	comply		
	v. Other security related equipment such as motorized gates or electric fences.	comply		
3.7.9.2	Option B: 220V AC			
3.7.9.2(a)	Alternatively the security system shall be powered by 220V AC supplied from the site's AC supply with an appropriately sized Uninterruptable Power Supply. With this option, the requirements above shall still be complied with.	comply		
3.7.9(f)	CCTV system batteries in addition to UPS batteries are not recommended. If CCTV system batteries are unavoidable then individual subsystems that have their own battery backup, these shall not be fed by the UPS. This is to prevent the UPS from charging these batteries in the event of a power failure (See figures 10 and 11). Any CCTV system batteries used shall provide backup for the time specified in section e) above.	comply		
3.7.9(g)	The system shall have a power failure intruder detection indication that shall be sent through to the security control room should the AC supply be interrupted.	comply		
3.7.9(h)	The system may have an additional power failure alarm indication that shall be sent through to Eskom network control via SCADA should the AC supply be interrupted.	comply		
3.7.10	Communication			
3.7.10(a)	A connection from the site to the Eskom local OT security server shall provide the means of communication to the control centre for, alarms and live viewing.	comply		
3.7.10(b)	The connection shall also be used for remotely configuring equipment and downloading of recorded footage	comply		

3.7.10(c)	The communication link between the site and the security control room shall be by means of a dedicated and secure communication medium between the sites and the security control room.	comply		
3.7.10(d)	Communication shall take place over Eskom's telecommunications network if at all possible.	comply		
3.7.10(d)(i)	When specifying a new site Eskom Telecoms will be consulted to determine the feasibility of using (or establishing) an Eskom Telecoms link to the site.			
3.7.10(d)(ii)	Eskom Telecoms will be consulted before going out on tender and communications available shall be stated at tender phase.			
3.7.10(d)(iii)	The priority and risk at the site shall be taken into account when deciding whether or not to increase bandwidth available for security			
3.7.10(e)	Though the Eskom telecommunication network is preferred, 3rd party communications infrastructure may be used if necessary.			
3.7.10(f)	The communication medium will be fibre (2Mbps bandwidth) where possible and satellite or microwave where fibre is not installed.	comply		
3.7.10(g)	As a last resort, if a higher bandwidth connection is not possible, GPRS may be used for communications provided equipment is specified and configured to be operated over the lower bandwidth.			
3.7.10(i)	The connection from the security equipment to the Eskom Telecoms network shall be Ethernet	comply		
3.7.10(j)	Eskom to provide all IP addresses to be used for on-site LAN.			
3.7.12	Time Synchronisation			
3.7.12(a)	In order accurately analyse recordings of incidents, and for providing reliable evidence, recorded footage needs to be time stamped with an accurate date and time stamp.	comply		
3.7.12(b)	The preferred method of time synchronization is using GPS. If a site has a GPS time signal, it should be used for the security system.	comply		

3.7.12(c)	At a single site, all cameras shall be time synced to within 1s of each other. This time syncing may be provided by the DVR or other timing device.	comply		
3.7.12(d)	Different sites shall be synchronised so that the difference between the times at different sites is less than 10s. This synchronisation may happen via an NTP clock or the central video management system (VMS).	comply		
3.7.12(e)	The central NTP clock or VMS system shall get its time from a GPS signal.	comply		
3.8	Intruder Detection System			
3.8.1	Indoor Detection			
3.8.1(a)	There shall be intruder detection in all buildings and rooms which the risk assessment indicates should be protected. At substations this will include all rooms of the relay house and switch rooms.	comply		
3.8.1I(b)	The sensors shall be placed so as to detect intrusion through any door or window leading into the building or by which access can be gained into the secured area.	comply		
3.8.1(c.)	Intruder detection may be in the form of movement detection (e.g. passive infrared sensors (PIRs), video analytics); door and window detection (e.g. Reed switches), or some combination of sensors.	comply		
3.8.1(d)	Intruder detection shall be located as to detect unauthorised entry through any door or window in the building.	comply		
3.8.1(e.)	Battery rooms holding lead acid batteries are a zone 2 hazardous location with specific rules governing work in the room. For this reason battery rooms shall not have CCTV or alarm equipment installed inside, but rather a door contact installed on the outside of all doors and windows to detect unauthorised entry.	comply		
3.8.2	Alarm System Operation			
3.8.2(a)	The alarm system shall meet the requirements of Eskom specification 240-867389–8 - Standard for Security Alarm Systems for Protection of Eskom Installations and its Subsidiaries [3]. In addition, the alarm system shall support the following when integrated with the CCTV:	comply		

3.8.2(b)	When an alarm is generated by the alarm system, the CCTV system shall detect the alarm and know what zone was triggered in ordered to trigger the relevant cameras for that zone.	comply		
3.8.2(c)	The alarm system shall receive trigger signals from CCTV video analytics in addition to triggers from the site's traditional security sensors.	comply		
3.8.2(d)	For redundancy alarm signals shall be sent to the Local OT security server through the CCTV system (to the VMS) and well as through the alarm system (to the alarm base station).	comply		
3.8.2(e)	The intruder detection system shall be able to control relay contacts which can be connected to the gate motor for opening and closing the gate.	comply		
3.8.2(f)	Should the intruder detection system be triggered at night, the site's LED floodlights shall be activated for a period of 15 minutes. Night can be determined by a means of day/night sensor or a clock timer. See section 3.8.3 below for more details.	comply		
3.8.2(g)	When the alarm is deactivated, a signal shall be sent through to the security control room identifying the employee who disarmed the site.	comply		
3.8.2(h)	Alarm system activation / deactivation shall be confirmed by means of audio sound over the speaker system as well as indicator LED(s) visible from inside the relay house and from the outside the gate of the site.	comply		
3.8.2(i)	Activation/deactivation of the intruder detection system shall activate/deactivate perimeter detection and internal building protection whether the detection is on the cameras or alarm sensors.	comply		
3.8.2(j)	Each activation / deactivation of the alarm system shall be date and time stamped and recorded by the alarm system.	comply		
3.8.2(k)	The system shall use remote controls to activate and deactivate the system as specified by 240-86738968 or per the technology already being used in the region.	comply		
3.9	Yard			
3.9.1	Yard overview			

3.9.1(a)	The main outdoor area to be covered by the CCTV and intruder detection system shall be along the perimeter of the site yard within the boundary fence.	comply		
3.9.1(b)	There shall be a thorough analysis of the site's layout before installing any cameras and perimeter detection to ensure that the entire site perimeter has been covered. Once installed, the entire system will be tested to ensure that this intended coverage has been achieved (See sections 3.16.–0 - Indoor Intruder Detection Tests and 3.16.12 -Camera Functional Test).	comply and provide proposed camera location schematics/diagrams		
3.9.1(c)	The intention is for the perimeter detection system to detect when an intruder crosses the boundary of the site and the camera system to be used to verify that a person has crossed the boundary. The perimeter detection can be provided by video analytics, either as part of the camera / DVR, or as an add-on feature to the camera system. See Section 3.9.3.	comply		
3.9.1(d)	One or more PTZ cameras shall be installed so as to view the majority of the yard. The intention of the PTZ system is to automatically track intruders, providing information to the security monitoring centre which can be used to deter the intruder and guide armed response. At smaller, lower risk sites, the PTZ may be omitted to save costs. At other sites it may prove more feasible to use strategically placed fixed cameras instead of the PTz.	comply		
3.9.1(e.)	A fixed camera shall be positioned so as to have a clear view of the main entrance gate. The intention of the gate camera is to recognise people and vehicles entering the site.	comply		
3.9.1(f)	To prevent damage to the camera and ensure good picture quality, cameras shall not be placed in a direction such that they will be exposed to intense beams of light from the floodlights or direct sunlight.	comply		
3.9.1(g)	Visible notification shall be placed at entrances and on the outside of the perimeter fence of the premises to notify persons entering the premises, that they may be subjected to CCTV surveillance. At substations the date of placement of such notices shall be recorded in the substation logbook.	comply		
3.9.2	Perimeter Camera System Layout			

3.9.2 (a)	The installation of fixed cameras shall be done primarily to cover the inside perimeter of the site yard.	comply		X
3.9.2 (b)	The purpose of the perimeter cameras is detection (See section 3.9.1 for a discussion of camera purpose). Perimeter cameras shall provide control room operators a method to confirm when an alarm is generated that an intruder has breached / approached the perimeter.	comply		X
3.9.2 (c)	At selected sites it may be appropriate for the cameras field of view to cover the outside perimeter of the fence, supporting detection before the perimeter is breached. This will depend on detection method used and the likelihood of false alarms from movement just outside the perimeter.	comply		X
3.9.2 (d)	There shall be a thorough analysis of the site's layout before installing any cameras and perimeter detection to ensure that the entire site perimeter has been covered. This must include mapping each camera's field of view and range of view on the site layout drawings to ensure that the perimeter is 100% covered.	comply and provide proposed camera location schematics/diagrams		
3.9.2 (e)	The view of the camera shall be free of any hindering obstacles such as walls, trees or buildings.	comply		X
3.9.2 (f)	The installation of cameras shall be done so as not to hinder existing vehicle accessibility paths to the installed power plant.	comply		X
3.9.2 (g)	The recommended arrangement of cameras within a generic substation yard is illustrated in Figure 12. Achieving coverage of the yard fence need not always be by means of a camera installed parallel to the yard fence. This is especially the case where the layout of the yard is not square. The requirement is only to have visuals of all enclosing fences of the yard, be it a parallel visual along the span of fence or at an angle facing.	comply		X
3.9.2 (h)	Where it is possible to obtain visuals at an angle of the fence, it shall be ensured that there is no obstacle between the camera and the face of the fence being monitored.	comply		X
3.9.2 (i)	Perimeter cameras shall be arranged so that the dead spot of each camera is covered by the field of view of another camera as shown in Figure 12.	comply		X

3.9.2 (j)	Should there be obstacles or poor visuals, additional cameras shall be installed to cover the span of fence.	comply		
3.9.3	Perimeter Detection System			
3.9.3 (a)	Alarms shall be generated by a perimeter detection system.	comply		
3.9.3(b)	The use of microwave beam detection is strongly discouraged due to the prevalence of nuisance alarms.	comply		
3.9.3 (c)	The perimeter detection can be provided by 'video analytics', either built into, or as an addition to, thermal perimeter cameras. Other detection methods (or combination of detection methods) may be used if they are able to meet the functional requirements specified here.	comply and provide supporting documentation		
3.9.3(d)	If Video analytics is used it should be 'advanced video analytics', able to analyse the footage, not simply video motion detection which only looks for changes in the picture. See Annex A for the distinction between the two.	comply		
3.9.3(e)	Edge' video analytics is preferred over server/DVR based video analytics. Edge video analytics happens on board the camera or on a device connected to each camera. Each camera therefore has a dedicated processor analysing its footage. Server or DVR based analytics uses one processor to analyse the feeds from a number of cameras, increasing the chance of poor performance. See Annex A for more information.	comply		
3.9.3(f)	The perimeter detection system shall create an 'invisible wall' which encapsulates the entire perimeter of the yard, so that there are no areas where an intruder may enter the site undetected.	comply		
3.9.3(g)	There shall be no 'dead spots' in the invisible wall. Where a method of detection has an inherent dead spot, the dead spot of each device shall be covered by another device (e.g. Cameras with overlapping fields of view).	comply		

3.9.3(h)	The perimeter detection method should be divided into zones matching the areas covered by the perimeter cameras. This shall enable the operators at the security control room to determine which area has been disturbed and which visual to use from the camera covering that section of fence where the incident occurred. Zone names must be the same on site as in the video management system at the security monitoring centre. These zones and zone names shall be reflected on the site layout provided with the system documentation.	comply and provide supporting documentation		
3.9.3(i)	The perimeter detection system must generate an alarm when a human enters the monitored zone. It must be able to detect a person who is walking upright, walking hunched over, crawling or running.	comply		
3.9.3(j)	The system must not be triggered by changes in light, movement of trees, small vibrations of the camera pole, animals including birds, vehicles driving past the protected siyte, weather conditions such as rain and snow.	comply		
3.9.3(k)	The sensitivity of the perimeter detection system must be adjustable in order to configure the system to meet the conditions at specific sites.	comply		
3.9.3(l)	The system must be able to operate in all lighting and weather conditions.	comply		
3.9.3(m)	Nuisance alarms shall be limited to 7 nuisance alarms, per site, per 7 day period.	comply		
3.9.3.1	Poles			
3.9.3.1(a)	Where lighting poles, buildings, or other suitable structures exist on the site in appropriate positions, these may be used to mount the cameras. If no existing structure is available, the cameras shall be mounted on poles.	comply		
3.9.3.1(b)	Poles shall be steel reinforced 4.5m or 5.7m spun concrete poles according to Eskom drawings: D-DT-0010 or D-DT0011. Poles may be purchased on the Eskom ENC (Eskom National Contract) if one is in place at the time.	comply		
3.9.3.1 (c)	Poles to be installed as per manufacturer instructions so as to minimize vibration due to wind.	comply		

3.9.3.1(d)	To prevent theft of cameras, the poles shall not be placed directly next to the fence, and anti-climbing devices shall be considered.	comply		
3.9.3.1(e)	The pole shall be earthed via 50 x 3 mm earth tails, the earth tails shall be buried and welded to the base of the fence so as not to be easily visible. The join shall be painted the same colour as the fence to avoid theft of the copper earthing.	comply		
3.9.3.1(f)	The earthing shall conform to the latest revision of the general earthing standards of copper joints as per D-DT-5240, sheets 2 and 6 (Annex C and Annex D)	comply and provide supporting evidence		
3.9.3.1(g)	Holes required for the fixing of the sensors and cameras may be drilled on-site and shall be appropriately sealed to prevent water ingress. Drilling can be minimised by using equipment that clamp securely onto the poles.	comply		
3.9.3.1(h)	Prior to the installation of the support foundation, the stone layer shall be removed sufficiently far enough from where the foundation is to be cast.	comply		
3.9.3.1(i)	On completion of the installation, all excess soil shall be removed from the yard and the stone shall be replaced to cover the area surrounding the foundation.	comply		
3.9.3.1(j)	All cabling be routed through the foundation of the cement pole. Drilled holes shall be kept to a minimum and shall be appropriately sealed to prevent water ingress.	comply		
3.10.	CCTV Surveillance System			
3.10(i)	The subcomponents of the surveillance system primarily consist of fixed perimeter cameras, gate cameras, PTZ cameras, indoor cameras and the security and site lighting. It is recommended that when any design is done, that it be taken into consideration that should the equipment need upgrading, that the existing infrastructure shall be able to incorporate new technologies.	comply		
3.10.1	Camera Purpose			
3.10.1(i)	In order to test whether a camera is fit for purpose, it is essential that the purpose of this camera be defined.			

3.10.1.1	Each camera shall have a single, clearly defined purpose. The purpose should consist of a category (detection, observation, recognition or identification), an area to be covered and a range of distances from the camera.	comply and provide supporting documentation		
3.10.1.2	Lighting conditions in which the camera should operate should also be stated.	comply and provide supporting documentation		
3.10.2	General Camera Requirements			
3.10.2.1	General			
3.10.2.1(a)	Cameras should be IP cameras, exceptions should be obtained for installation of analogue cameras	comply		
3.10.2.1(b)	Before installation begins the camera layout, including expected fields of view and dead spots, shall be documented and signed off by an Eskom Engineer.	comply		
3.10.2.2	Cables			
3.10.2.2(a)	Choice of cables shall be based on camera manufacturer recommendations.	comply		
3.10.2.2(b)	Either fibre or electrical signals may be used for camera communication. Cost should be considered when choosing between Cat 5 and fibre communication cables. In high EMF environments CAT6 or fibre should be considered.	comply		
3.10.2.2(c)	Where electrical cables are used they should be unshielded twisted pair (UTP) cable, such as CAT5. UTP cabling is cost efficient, has high noise immunity, lower loss per length than coax and allows for high quality long range transmission.	comply		
3.10.2.2(d)	For analogue cameras a UTP balun connector may be implemented for the cabling between the camera and the DVR. Cat5 is recommended over coaxial cable as it is thin and flexible cable making it easy to string between walls.	comply		
3.10.2.2(e)	Cable selection and routing shall always be done in such a way that operation of cameras is not affected by interference. This may be achieved by separating AC power cables from communication cables, shielding cables, or a combination of the two.	comply		
3.10.2.3	Installation			

3.10.2.3 (a)	The installation of the camera and brackets shall be as indicated in the manufacturer's guidelines.	comply and provide supporting documentation		
3.10.2.3(b)	Brackets used to secure the camera shall be robust and shall minimize vibration.	comply		
3.10.2.3(c)	Brackets shall be capable of being "lock tight" to reduce the possibility of accidentally moving.	comply		
3.10.2.3(d)	All brackets shall be "cable managed" so that cable entering the housing is enclosed within the bracket from the support to the housing, allowing no cable to be exposed.	comply		
3.10.2.3(e)	The cables shall be marked with at least the camera name and number.	comply		
3.10.2.3(f)	Dome and PTZ cameras shall be mounted with appropriate brackets which prevent the pole from being in the camera's field of view.	comply		
3.10.2.4	Manufacturer Specifications			
3.10.2.4(a)	Automatic Gain Control (AGC) shall be at least 30dB	comply		
3.10.2.4(b)	Back light compensation must be implemented.	comply		
3.10.2.4(c)	The camera's specified coverage distance shall be 10% further than is required by the site security design.	comply		
3.10.2.4(d)	Minimum Frames Frequency shall be 8 fps	comply		
3.10.2.4(e)	The lens shall be chosen to suit the application and the functional requirements of the site.	comply		
3.10.2.4(f)	If cameras are IP Cameras, they shall be ONVIF compliant.	comply and specify which open industry protocols are supported		
3.10.2.4(g)	Image Format shall be 1/3 inch or larger	comply		
3.10.2.4(h)	All cameras settings (except focal length and focus) shall be remotely configurable, either via the DVR, or directly using Ethernet.	comply		
3.10.2.4(i)	The camera shall provide a minimum horizontal resolution of 600 TV lines or 800 pixels.	comply		
3.10.2.4(j)	The signal to noise ratio shall be ≥ 52db.	comply		
3.10.2.4(k)	Camera shall implement wide dynamic range and white balance control functionality to compensate for bright areas.	comply		

3.10.2.4(l)	Camera shall have Wide Dynamic Range	comply		
3.10.3	General Requirements for Outdoor Cameras			
3.10.3(i)	Outdoor cameras shall meet all specifications listed in section 3.10.2 – General Camera Requirements	comply		
3.10.3.1	General			
3.10.3.1 (a)	As far as possible, outdoor cameras shall be positioned “North to South” in order to avoid sunlight on the lens. In some cases this is not possible; therefore all cameras shall have wide dynamic range (WDR) functionality.	comply		
3.10.3.2	Cables			
3.10.3.2(a)	The power cable shall be steel wire armoured cable.	comply		
3.10.3.3	Installation			
3.10.3.3 (a)	The camera shall be well protected from the elements and vandalism by mounting it within an appropriate housing.	comply		
3.10.3.3 (b)	The camera housing shall have an IP rating of at least 65.	comply and provide supporting documentation		
3.10.3.3 (c)	The camera housing shall have a sun visor and be steel constructed.	comply		
3.10.3.3 (d)	The camera housing shall be weather-proof, environmental, corrosion and vandalism resistant as well as UV resistant.	comply		
3.10.3.3 (e.)	Harsh environments such as coal power plants may require a harsh environment housing. Similarly cameras at coastal sites will need added corrosion protection.	comply		
3.10.3.3 (f)	If necessary, a junction box with a minimum rating of IP 65 may be installed on the camera support pole. The junction box shall be used to protect any connections and additional equipment necessary for the camera operation. Equipment housed in the junction box should be kept to a minimum; as much equipment as possible shall be housed in the equipment room / relay house.	comply		
3.10.3.3 (g)	If used, the junction box shall be mounted on the cement pole support, below the camera.	comply		

3.10.3.3 (h)	If used, the junction box shall be lockable (lock and key, not a panel key) and alarmed.	comply		
3.10.3.3 (i)	All openings of the housing and junction box, used as well as unused, shall be properly sealed to prevent any water or insects from entering the housing.	comply		
3.10.3.4	Manufacturer Specifications			
3.10.3.4(a)	outdoor cameras shall meet all requirements under 3.10.2.4 above	comply		
3.10.3.4 (b)	Camera sensor shall be protected from sun damage. Mechanical Shutters are susceptible to failure and will not be accepted.	comply		
3.10.4	Fixed Thermal perimeter cameras			
3.10.4.1	Introduction			
3.10.4.1(a)	The purpose of perimeter cameras is to provide confirmation of an intruder when an alarm is generated by the perimeter intruder detection system.	comply		
3.10.4.1(b)	Since the images from good thermal cameras are not affected by weather conditions (fog, rain, snow), or glare, it is preferred that the perimeter cameras be thermal. It is also preferred that these thermal cameras provide perimeter detection using 'video analytics', either built into, or as an addition to, the perimeter cameras.	comply		
3.10.4.2	Specifications			
3.10.4.2(i)	Thermal cameras shall meet all specifications listed in section 3.10–2 - General Camera Requirements,	comply		
3.10.4.2(ii)	Thermal cameras shall meet all specifications listed in section 3.10–3 - General Requirements for Outdoor Cameras.	comply		
3.10.4.2(iii)	If video analytics on the cameras is used as a method of intruder detection, the video analytics shall meet all specifications listed in 3.9–3 - Perimeter Detection System.	comply		
3.10.4.2(a)	Thermal perimeter cameras shall be installed along the perimeter of the site yard as described in section 3.9.2 above.	comply		
3.10.4.3	Manufacturer Specifications			
3.10.4.3(i)	Thermal cameras shall meet all requirements under section 3.10.2.4 above	comply		

3.10.4.3(ii)	Thermal cameras shall meet all requirements under section 3.10.3.4 above	comply		
3.10.4.3(iii)	Detector type shall be Uncooled micro bolometer	comply		
3.10.4.3(iv)	Thermal cameras must have Automatic Gain Control	comply		
3.10.4.3(v)	Resolution shall be at least 320 x 240	comply		
3.10.5	Fixed perimeter cameras – non thermal			
3.10.5(i)	Fixed cameras shall meet all specifications listed in section 3.7.4 – General Camera Requirements,	comply		
3.10.5(ii)	Fixed cameras shall meet all specifications listed in section 3.10–3 - General Requirements for Outdoor Cameras.	comply		
3.10.5(iii)	Fixed cameras shall be installed along the perimeter of the site yard as described in section 3.9.2 above.	comply		
3.10.5(iv)	If non thermal perimeter cameras are to be used, the design must explicitly address how the effects of weather will be mitigated.	comply and provide supporting documentation		
3.10.5.1	Manufacturer Specifications			
3.10.5.1(i)	fixed perimeter outdoor cameras shall meet all requirements under 3.10.2.4 above	comply and list any deviations		
3.10.5.1(ii)	fixed perimeter outdoor cameras shall meet all requirements under 3.10.3.4 above	comply and list any deviations		
3.10.5.1(iii)	Infrared shall Use 850 or 940nm wavelength. Distance covered must match application.	comply and provide supporting documentation		
3.10.5.1(iv)	The minimum sensitivity shall be 0.0002 lux for colour images and 0.00002 lux for monochrome images.	comply and provide supporting documentation		
3.10.6	PTZ camera			
3.10.6.1	Introduction			
3.10.6.1(i)	The purpose of the PTZ cameras is to track intruders in order to help response teams pinpoint the location of intruders. Intruder tracking can be automatic or manual.	comply		
3.10.6.2	Installation			
3.10.6.2(a)	One or more PTZ cameras may be installed within the yard depending on the risk and the layout of the site.	comply		

3.10.6.2(b)	The PTZ camera shall be positioned in the yard in such a way as to cover the majority of the critical points. Positioning shall be site dependent and shall be informed by the site PSD,	comply		
3.10.6.2(c)	In the case where there are no perimeter cameras, the perimeters and the critical points to be covered by the PTz.	comply		
3.10.6.2(d)	Where there are perimeter cameras the critical points to be covered by the PTZ are: cable trenches, Building Entrance,Gate entrances, Minisubs, RMUs or Metering Kiosks, Outdoor storage areas	comply		
3.10.6.2 (e.)	The PTZ camera unit shall be installed in one of the following manners:			
3.10.6.2 (e.)(i)	On a 7.2m or 9.1m Eskom approved cement pole (See D-DT-0011& D-DT0012 for guidance). The installation shall be done according to the latest revision of D-DT-0332 (LV and MV Foundation Pole Arrangement).	comply		
3.10.6.2 (e.)(ii)	A steel pole attached to a building. SANS 1431 grade 300WA or 4360 grade 43A steel shall be used.	comply and provide supporting documentation		
3.10.6.2 (e.)(iii)	A bracket attached to an already installed Eskom lighting mast.	comply		
3.10.6.3	Specification			
3.10.6.3(i)	PTZ cameras shall meet all specifications listed in section 3.10–2 - General Camera Requirements,	comply and list any deviations		
3.10.6.3(ii)	PTZ cameras shall meet all specifications listed in section 3.10–3 - General Requirements for Outdoor Cameras.	comply and list any deviations		
3.10.6.3(a)	The PTZ's zooming capabilities shall be powerful enough to meet the purpose of the PTZ	comply		
3.10.6.3(b)	The PTZ camera shall be remotely controllable by an operator to pan, tilt, zoom, focus, mobilize the iris, switch the camera on/off and place the camera in a pre-set position.	comply		
3.10.6.3(c)	The PTZ camera shall be controlled by a hardwired cable.	comply		
3.10.6.3(d)	If there are no perimeter cameras then the PTZ shall be able to see the perimeter by means of thermal imaging or a built in infrared spotlight.	comply		

3.10.6.3(e)	The PTZ shall have preset positions. When a preset position is chosen by the controller, the PTZ shall immediately go to that position.	comply		
3.10.6.3(f)	Preset positions shall include zoom level.	comply		
3.10.6.3(g)	It shall be possible to label the preset positions with a descriptive name.	comply		
3.10.6.3(h)	The PTZ shall be capable of having at least 10 pre-sets.	comply		
3.10.6.3(i)	Preset positions at each site shall include all gates, doors, various points on the perimeter boundary and high risk assets (trenches, transformers, rolls of cable).	comply		
3.10.6.4	Operation			
3.10.6.4(a)	It is preferable that the PTZ have built in analytics and be set to 'patrol' the yard during normal operation.	comply		
3.10.6.4(b)	If the PTZ does not have analytics then during normal operation it should be set to a useful 'home' position (e.g. gate).	comply		
3.10.6.4(c)	When an alarm triggers the PTZ shall zoom into the area where the alarm happened. If a person is detected, the PTZ shall follow the motion of that person.	comply		
3.10.6.4(d)	The control signals from an operator shall take preference over the patrol and tracking functions.	comply		
3.10.6.4(e)	Preset positions at each site shall include all critical points on the site.	comply		
3.10.6.5	Manufacturer Specifications			
3.10.6.5(i)	PTZ camera shall meet all requirements of section 3.10.2.4 above	comply and list any deviations		
3.10.6.5(ii)	The minimum Pan speed at which the PTZ camera can pan the full 360° shall be 6° per second	comply		
3.10.6.5(iii)	The Pan Range angle through which the PTZ can tilt shall be minimum 90º (-10º +80º)	comply		
3.10.6.5(iv)	Minimum Optical Zoom which the camera can zoom without reducing resolution shall be 3.2mm – 138.5mm (43x) (Site dependent)	comply		
3.10.6.5(v)	Minimum digital zoom that camera can zoom while decreasing the resolution shall be 16x	comply		

3.10.6.5(vi)	The minimum light sensitivity shall be 0.0007 lux for colour images and 0.000007 lux for monochrome images.	comply and provide supporting documentation		
3.10.7	Indoor Cameras			
3.10.7(i)	At substations, indoor cameras shall be installed in control plant rooms and switch rooms.	comply		
3.10.7(ii)	Indoor cameras shall meet all specifications listed in section 3.10.2 – General Camera Requirements	comply		
3.10.7.1	General			
3.10.7.1(a)	The camera field of view shall include the entrance to the room/building as the point of interest. Where there is more than one entrance, more indoor cameras may be necessary, as determined by the risk assessment.	comply		
3.10.7.1(b)	Indoor cameras may be dome, fixed or bullet cameras	comply		
3.10.7.1(c)	Indoor cameras shall have infrared lighting.	comply		
3.10.7.1(d)	The purpose of the camera shall be observation and / or identification in the case of forced entry depending on the site requirements.	comply		
3.10.7.1(e)	Backlight compensation with wide dynamic is particularly necessary for cameras looking at entrances.	comply		
3.10.7.2	Placement and Installation			
3.10.7.2(a)	Indoor cameras may be ceiling or wall mounted depending on the site.	comply		
3.10.7.2(b)	The camera shall be housed in a vandal proof housing with an IP rating of at least 51.	comply		
3.10.7.2 (c)	The camera field of view shall be adjustable via an adjustable bracket or built in manual pan-tilt mechanism.	comply		
3.10.7.3	Manufacturer Specifications			
3.10.7.3(i)	Indoor cameras shall meet all requirements listed in 3.10.2.4	comply and list any deviations		
3.10.7.3(ii)	Camera shall have day/night function to compensate for poor lighting conditions	comply		
3.10.7.3(iii)	Electronic shutters shall be used to compensates for moderate light changes in indoor applications without the use of auto iris lenses.	comply		
3.10.7.3(iv)	Camera shall have infrared.	comply		

3.10.7.3(v)	The minimum illumination shall be 0.0002 lux for colour images and 0 lux for monochrome images.	comply and provide supporting documentation		
3.10.8	Digital Video Recorder / Network Video Recorder			
3.10.8(i)	A Digital video recorder (DVR) or Network Video Recorder (NVR) shall be used to record relevant video footage as well as to allow access to live streaming footage from the security control room.	comply		
3.10.8(ii)	The DVR shall be integrated with the alarms from both the perimeter detection system and the indoor intruder detection system and shall connect to the Video Management System.	comply		
3.10.8(iii)	The DVR shall meet all specifications listed in section 3.7.4 – General Physical Requirements, and section 3.7–5 - General Electrical Requirements	comply and list any deviations		
3.10.8.1	DVR Functionality			
3.10.8.1(a)	In the event of an alarm being triggered (from camera or intrusion detection system) when the system is armed the system shall cater for the followi39unctionalityity:			
3.10.8.1(a)(i)	Record footage from relevant cameras.	comply		
3.10.8.1(a)(ii)	The footage recorded shall be for 5s second before the event triggered, the time of the actual event (however long motion is detected by the camera) and at least a 15 second post event time period. This recording shall be at the full resolution of the camera.	comply		
3.10.8.1(a)(iii)	Send a signal to the Security Control Room, including the zone that was triggered.	comply		
3.10.8.1(a)(iv)	Send short video clip / series of still pictures from the camera covering the zone where the alarm triggered to the security control room.	comply		
3.10.8.1(a)(v)	Allow for the security control room to remotely access the site in order to stream live footage from the system.	comply		
3.10.8.1(a)(vi)	Allow for the security control room to operate any PTZ cameras installed on site, including using pre-set positions.	comply		
3.10.8.1(a)(vii)	Allow for the controller to speak over the PA system or play a pre-recorded message on site.	comply		

3.10.8.1(b)	In the event of movement being detected when the system is not armed, the system shall: Record footage from relevant cameras for 5s second before the event, the time of the actual event (For however long motion is detected by the camera) and at least a 15 second post event time period. This recording shall be at the full resolution of the camera.	comply		
3.10.8.2	Compatibility:			
3.10.8.2(a)	The DVR shall be able to integrate with a wide range of cameras from different manufacturers.	comply		
3.10.8.2(b)	The DVR shall be ONVIF compliant. It must however be noted that ONVIF compliance does not guarantee compatibility between systems.	comply and specify which open industry protocols are supported		
3.10.8.2(c)	The DVR shall allow for simultaneous use of different model cameras with different resolutions.	comply		
3.10.8.3	Recording and streaming			
3.10.8.3(a)	It shall be possible to configure the DVR to record on any motion event or only when an alarm event is generated.	comply		
3.10.8.3(b)	Simultaneous recording on site and streaming to the security control room shall be possible.	comply		
3.10.8.3(c)	It shall be possible to stream video at a lower resolution and frame rate than the footage is recorded on site.	comply		
3.10.8.3(d)	Recording: Shall be such that identification can be achieved on cameras with identification as the purpose.	comply		
3.10.8.3(e)	All footage shall be time and date stamped	comply		
3.10.8.3(f)	It shall be possible to search events and recorded footage based on a combination of date, time, event and motion in a specific part of the camera's field of view	comply		
3.10.8.3(g)	The recording media shall be a removable, hot swappable and lockable.	comply		
3.10.8.3(h)	All footage shall be kept for a minimum of 30 days. To achieve this, the hard drive size should initially be calculated to be large enough to store 30 hours of continuous recording from all cameras.	comply		
3.10.8.3(i)	It shall be possible to 'flag' important footage so that it will not be overwritten.	comply		

3.10.8.3(j)	When the hard drive is full, the DVR shall continue to record by overwriting the oldest recordings first. Flagged footage shall not be overwritten.	comply		
3.10.8.4	Frame Rate			
3.10.8.4(a)	The frame rate shall be adjustable	comply		
3.10.8.4(b)	A frame rate of at least 25fps shall be achievable by the DVR	comply		
3.10.8.4(c)	Recommended frame rate for streaming video: 2-5 fps	comply		
3.10.8.4(d)	Recommended frame rate for recordings: 6fps or larger	comply		
3.10.8.5	Video Compression			
3.10.8.5(a)	Compression standards such as H. 264, MPEG4 or equivalent may be used for streamed video	comply and provide supporting documentation		
3.10.8.5(b)	A compression standards such as MJPEG or equivalent may be used for streamed video	comply and provide supporting documentation		
3.10.8.5(c)	Video compression shall be used appropriately such that the specified purpose of each camera (detection/observation/recognition/identification) can be achieved for recordings and streaming of footage	comply		
3.10.8.6	Time Sync			
3.10.8.6(a)	The DVR shall enable the syncing of time between sites, and between cameras as specified in section 3.7.12	comply		
3.10.8.7	Remote Connections			
3.10.8.7(a)	It shall be possible to remotely view live or recorded video over the network (with appropriate access rights).	comply		
3.10.8.7(b)	It shall be possible to configure all DVR settings over the network (with appropriate access rights).	comply		
3.10.8.7(c)	It shall be possible to download recordings on site or offsite.	comply		
3.10.8.8	Video Monitor			
3.10.8.8(a)	It shall be possible to plug a Video Monitor into the DVR (site specific)	comply		
3.10.8.9	Security			
3.10.8.9(a)	The DVR shall be password protected.	comply		

3.10.8.9(b)	The DVR shall cater for a minimum of 10 individual users with assigned access rights	comply		
3.10.8.9 (c)	There shall be a minimum of 2 access levels, one with limited access right, the other with full administrative rights	comply		
3.10.8.10	Hardware and I/O connections			
3.10.8.10(a)	The DVR shall have input contacts for connecting to alarm signals from the alarm system	comply		
3.10.8.10(b)	It is recommended that DVR have an 'error' output which will output a signal to the alarm system if there is an error with the DVr.	comply		
3.10.8.10(c)	DVR shall have an on off switch and status LED	comply		
3.10.8.11	System Logging:			
3.10.8.11(a)	The DVR shall keep a time stamped electronic log of the following:			
3.10.8.11(a)(i)	User who has logged in to make changes.	comply		
3.10.8.11(a)(ii)	Changes made	comply		
3.10.8.11(a)(iii)	System Errors	comply		
3.10.8.11(a)(iv)	Interruption of Camera feeds	comply		
3.11	Video Management System (VMS)			
3.11.1	Introduction			
3.11.2	Location and Architecture			
3.11.2(i)	In regions where an Eskom security control room for remote sites is not available, the security control shall be manned and hosted by a contractor. It is however imperative that Eskom still remains in control of the VMS infrastructure and is not locked into using one service provider indefinitely. For this reason a distributed architecture shall be used for the security network allowing for the VMS system to be used from multiple secure sites.	comply and provide supporting documentation		
3.11.2(ii)	The network infrastructure shall adhere to the principles laid out in the following Eskom Documents			
3.11.2(ii)(a)	240-554109–7 - Cyber Security Standard for Operational Technology	comply and provide supporting documentation		

3.11.2(ii)(b)	240-556835–2 - Definition of Operational Technology (OT) and OT / IT Collaboration Accountabilities	comply		
3.11.2.1	Hosting Server at a Third Party – Exceptional Case			
3.11.2.1	There may be cases where, due to budget, infrastructure or resource restraints, it is not feasible for the server to be hosted by Eskom. In such cases the VMS server may be hosted by a third party.	comply		
3.11.2.1 (a)	There shall be an agreement with the third party as to who owns the Servers, VMS software license, Configuration data, Recordings and Logs when the contract expires	comply		
3.11.2.1 (b)	There shall be a strategy for moving monitoring of sites to a different third party, or Eskom premises when the contract expires.	comply		
3.11.3	Network and Connections			
3.11.3(a)	The VMS shall connect to CCTV cameras and DVRs via the Eskom OT network, a third party network, or a combination of the two.	comply		
3.11.3(b)	The VMS shall be capable of a 'Client-Server' configuration. The server shall be housed at an Eskom site and the security control room shall connect to the server using client software, over a secure, dedicated link.	comply		
3.11.3(c)	Authorised Eskom employees using the client software shall be able to connect to the server via the Eskom Corporate Network.	comply		
3.11.3(d)	The VMS system shall be able to connect to a minimum of 500 sites and 4000 cameras. Not all installations will need this many connections, but it shall be possible to upgrade the system to accommodate these numbers.	comply and provide supporting documentation		
3.11.3(e)	The VMS design shall cater for failover and allow for a redundant architecture.	comply		
3.11.3(f)	The system shall allow for at least 5 simultaneous client connections.	comply		
3.11.3(g)	The frame rate and resolution of camera connections shall be reduced in order to provide smooth footage over the communication medium.	comply		
3.11.4	Features			

3.11.4(a)	The VMS shall be able to connect to a wide range of CCTV NVRs and DVRs.	comply and provide supporting documentation		
3.11.4(b)	Where there are already CCTV components installed, the VMS shall be compatible with the existing install base of CCTV equipment.	comply		
3.11.4(c)	The VMS system shall be ONVIF Compliant. It must however be noted that ONVIF compliance does not guarantee compatibility between systems.	comply and specify which open industry protocols are supported		
3.11.4(d)	The VMS shall be able to connect to cameras with a wide range of different resolutions (from CIF (352x240) to 5 Megapixel). Typically the higher resolutions will only be used when monitoring is on site.	comply		
3.11.4(e)	All security control room activities as described in section 3.12 Security Control Room, shall be possible using the VMS system.	comply		
3.11.4(f)	The VMS system shall allow for Access Control integration.	comply		
3.11.4(g)	The VMS shall be linked to an NTP/SNTP timeserver to synchronise the time on the VMS system.	comply		
3.11.4(h)	The VMS shall be able to operate as a time server to synchronise the times of downstream systems at remote sites.	comply		
3.11.4(i)	The VMS shall allow an administrator to make customizable reports on events, system status etc.	comply		
3.11.4(j)	The VMS shall allow the security control room operators to view whether a site is armed or disarmed.	comply		
3.11.4(k)	It shall be possible to draw up a list of all sites which are disarmed.	comply		
3.11.5	Network Security			
3.11.5(a)	The system shall comply with 240-55410927: Cyber Security Standard for Operational Technology which serves to guide the implementation of Cyber Security principles in the OT environment	comply and provide supporting documentation		
3.11.5(b)	All connections to the Eskom OT networks shall be firewalled as per 240-79669677: Demilitarised Zone (DMZ) Designs For Operational Technology	comply		

3.11.5(c)	All connections to the Eskom corporate network shall be firewalled and approved by Eskom Group It.	comply		
3.11.5(d)	Remote Access to the Eskom network shall adhere to 32-273: Information Security – IT/OT and Third Party Remote Access Standard.	comply		
3.11.5(e)	The Engineering design shall follow both IT and OT governance processes as per 240-55863502: Definition of OT and OT/IT Collaboration Accountabilities.	comply		
3.11.5(f)	The VMS shall allow for individual, password protected user rights.	comply		
3.11.5(g)	There shall be a minimum of the following 2 access levels:			
3.11.5(g) (i)	Level 1 shall provide viewing of footage only, with no ability to delete footage or view and change network settings.	comply		
3.11.5(g)(ii)	Level 2 shall provide full administrative rights.	comply		
3.11.5(h)	The system shall keep a time and date stamped log of all logon events	comply		
3.11.5(i)	The system shall keep a log of all administrative changes made on the system, including who made the change.	comply		
3.11.6	Video Recording and Streaming			
3.11.6(a)	The primary purpose of the VMS shall be to view live footage. Due to network constraints the primary place for saved recordings shall be on site. However, for investigation and training purposes, it shall be possible for the VMS to record footage which has been streamed to the security control room and to export that footage.	comply		
3.11.6(b)	The VMS shall support simultaneous recording and streaming of footage.	comply		
3.11.6©	The VMS shall support streaming at a wide range of resolutions, depending on the network bandwidth and the camera being connected to.	comply		
3.11.6(d)	The VMS shall enable different client workstations to stream from different cameras simultaneously.	comply		
3.11.6(e)	The VMS shall enable a continuous streaming ‘video wall’. This shall be customizable, allowing for resizable viewing panes.	comply		

3.11.6(f)	The VMS shall support recording and playback of files using H.264, MPEG and MJPEG video compression	comply and provide supporting documentation		
3.11.6(g)	The VMS shall be able to trigger recordings based on: Schedule, Manual trigger, alarm, event	comply		
3.11.6(h)	The VMS shall be able to stream and record using various frame rates (8fps - 25fps). Typically the higher frame rates will only be used for live footage when monitoring is on site.	comply		
3.11.6(i)	The VMS shall be able to use a wide range of different communication links to different sites. This will range from poor 3G connections, to high latency satellite, to fibres. It shall be possible to cater for different frame rates and resolutions per site depending on the bandwidth and cost of the communication medium.	comply		
3.11.6(j)	All recordings shall be electronically watermarked and show time and date.	comply		
3.11.6(k)	It shall be possible to search events and recorded footage based on a combination of date, time, event and motion in a specific part of the camera's field of view	comply		
3.11.6(l)	Playback in slow motion and at high speed shall be possible.	comply		
3.11.6(m)	The player shall allow for multichannel playback, which allows users to play recorded video from several cameras simultaneously. This is useful if tracking suspects moving on a site.	comply		
3.11.6(n)	The system shall be able to perform mass export of archived footage.	comply		
3.11.6(o)	It shall be possible to 'cut' footage to export only the portion of footage that is of interest	comply		
3.11.6(p)	As a guideline, the system shall cater for at least 7 days of continuous recordings from each of the security control room monitors, streaming from 5 of the highest frame rate and resolution cameras installed.	comply		
3.11.6(q)	It shall be possible to 'flag' important footage so that it will not be overwritten.	comply		
3.11.6(r)	When the hard drive is full, the oldest recordings shall be overwritten first. Flagged footage shall not be overwritten.	comply		
3.11.7	Event Management			
3.11.7	The VMS shall support the following event management functions			

3.11.7(a)	Support 'black screen monitoring': In normal state, no video is shown. When an alarm triggers at a site the controller sees a series of still images or a short video clip of the zone where the alarm was triggered. The controller can then choose to stream video from the site.	comply		
3.11.7(b)	Support an event queue to allow the management and acknowledgment of multiple alarm events.	comply		
3.11.7(c)	It shall be possible to look at a new event without having acknowledged a previous event.	comply		
3.11.7(d)	Support PTZ control including PTZ pre-set positions.	comply		
3.11.7(e)	Allow the transmission of voice from the controller to the PA system on site.	comply		
3.11.7(f)	Allow for the controller to control lights at the site.	comply		
3.11.7(g)	Allow controller to view the location of alarms and cameras on a site layout	comply		
3.11.7(h)	Allow controller to view the location and status of all sites on a map	comply		
3.11.7(i)	Enable comments from controller to be linked to an event.	comply		
3.11.7(j)	It shall be possible to 'escalate' incidents to another workstation running the client software e.g. another controller or an Eskom National Security Control Centre.	comply		
3.11.7(k)	Log events and actions for auditing purposes	comply		
3.11.7(l)	A highly recommended feature is the ability of the VMS system to 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).	comply		
3.11.8	Usability			
3.11.8	The VMS system shall have high usability (be 'user friendly'). Usability is a difficult thing to quantify but can be broadly defined as consisting of:			
3.11.8(a)	The system shall be easily learnable	comply		
3.11.8(b)	The system shall be highly efficient	comply		
3.11.8(c)	The system shall be easily memorable	comply		
3.11.8(d)	It shall be easy to recover from errors	comply		

3.11.8(e)	It shall be pleasant to use the design	comply		
3.11.8(f)	Before choosing a VMS system Eskom shall view a demonstration of the VMS product. The service provider shall be able to demonstrate all of the features specified above, this shall include administrative tasks as well as security control room tasks. The evaluator(s) shall use the system themselves as part of this demonstration rather than simply being shown the system in operation.	comply		
3.11.9	Hardware			
3.11.9(a)	Server shall meet Eskom IT requirements for servers including:			
3.11.9(a)(i)	An HP server may be used	comply		
3.11.9(a)(ii)	Server shall be 19” rack mountable	comply		
3.11.9(a)(iii)	The operating system shall be approved by Eskom IT	comply		
3.11.9(a)(iv)	Symantec antivirus shall be installed (can be provided by Eskom IT support)	comply		
3.11.9(a)(v)	Server shall connect to Eskom IT servers for antivirus and Windows security updates.	comply		
3.11.9(b)	Server shall meet with the VMS manufacturer’s hardware requirements.	comply		
3.11.9(c)	Server shall be housed in a secure, access controlled environment.	comply		
3.11.10	Training and Support			
3.11.10(a)	There shall be local support for the VMS product.	comply		
3.11.10(b)	There shall be product support in the closest City to the installation	comply		
3.11.10(c)	The tenderer shall provide Eskom with details of their support network as well as the service levels in terms of turnaround time to attend to technical problems.	Comply and to provide details of support network as well as the service levels in terms of turnaround time to attend to technical problems.		
3.11.10(d)	Operator and administrator training shall be provided	comply		
3.11.10(e)	Documentation on the hardware installation shall be provided	comply		
3.11.10(f)	Instruction manuals shall be provided	comply		
3.12	Security Control Room			

3.12.1	The CCTV surveillance shall be monitored by Eskom staff or an Eskom approved security company located within a secured central security control room.			
3.12.2	The security control room shall be equipped such that the security control room operators shall, for each site, be able to execute the following functions:			
3.12.2 (a)	Select each individual camera within the site to view footage from the respective camera.	comply		
3.12.2 (b)	Select a program to sequentially switch the cameras.	comply		
3.12.2 (c)	Operate the zoom, pan and tilt throughout the complete range of each PTZ camera installed.	comply		
3.15	Maintenance			
3.15.1	Introduction – Maintenance Contracts			
3.15.1(a)	All installations shall be accompanied by a 1 year maintenance contract.	comply		
3.15.1(b)	After this 1 year period one of the following must be in place:			
3.15.1(b)(i)	A maintenance contract with a supplier	comply		
3.15.1(b)(ii)	A maintenance plan for Eskom to do maintenance work.	comply		

Annex B – Technical Schedules A/B for the IACS

(related to technical specification 240-102220945)

TECHNICAL SCHEDULES A & B FOR

SPECIFICATION FOR INTEGRATED ACCESS CONTROL SYSTEM (IACS) FOR ESKOM SITES STANDARD IN ACCORDANCE WITH ESKOM STANDARD 240-102220945

Schedule A: Purcha'er's specifications

Schedule B: Guarantees, compliance and technical particulars of equipment offered

The clauses and numbering in this table are not necessarily the verbatim clauses as per 240-102220945. Therefore it is OBLIGATORY on the TENDERER to review the applicable clauses in 240-102220945 in order to provide an informed response.

When completing the Schedule B and the References section, The Tenderer is required to state clearly, for each clause that requires a statement of compliance, with one of the following options:

Comply – Confirmation of FULL Compliance to all clauses of the applicable section of the Technical Standard. No deviations.

Partially Comply – Confirmation of PARTIAL Compliance and that FULL Compliance is not possible. Deviations taken.

Do Not Comply - Conformation of Non-Compliance to ALL requirements in the applicable section

Reference to evidence in the form of datasheets, equipment manuals, drawings, hyperlinks shall be included in the References section if required.

Where there are any deviations taken from the clauses in the applicable section, these should be indicated under the References and Deviations section.

	Description	Schedule A	Schedule B (Suppl'er's statements of compliance)	References/ Statement (supporting evidence) if required & Deviations
5	Operational requirements			
5.1	General operational requirements			
5.1 (1)	The system shall be able to transfer data to SAP for Time and attendance data.			
5.1 (2)	Each user authorization shall be uniquely definable.	Comply with reference.		
5.1 (3)	Operator terminals shall be protected by terminal security such as password policy.	Comply with reference.		
5.1(4)	All actions on the system shall be traceable and auditable. These actions must be kept for a minimum period of 90 days.	Comply with reference.		

5.1 (5)	The system shall allow for an allocated employee number (unique number) to be changed when a contractor or visitor becomes a permanent employee with Eskom without having to re-register.	Comply		
5.1 (6)	Automatic disabling of a visitor/contractor on the required date.	Comply		
5.1 (7)	A visitor shall be disabled after leaving the site or designated place of visit/work	Comply		
5.1 (8)	The system shall have a full anti-pass back facility to control the flow of personnel from one zone to the other.	Comply with reference where applicable.		
5.1(9)	High risk areas access shall be granted only to personnel working in that area, additional access shall be automatically disabled as soon as that person leaves the area.	Comply		
5.1(10)	The system shall allow for overrides, interlocking and other functions as they become necessary to operate and optimize the system by the administrator at a remote location.	Comply		
5.1 (11)	The system shall be able to interface with existing software packages and therefore an open protocol software platform will be required.	Comply		
5.1 (12)	It shall be possible for the operator to bypass anti-pass back rules selectively such as one host having multiple visitors.	Comply		
5.1(13)	The system shall have lockdown functionality in emergency situations.	Comply		
5.1 (14)	System shall allow for online changes to be made.	Comply		
5.1 (15)	Real-time online debugging shall be possible.	Comply		
5.1 (16)	The system shall be either fail safe or fail secure, as required.	Comply		

5.1(17)	The application for change or update of access shall be completed on a standardised eForm.	Comply		
5.1 (18)	There shall be a dedicated “Master” station to assist in roll call in the event of an evacuation.	Comply		
5.1(19)	The system shall have a built in Fitness For Duty (FFD) program or interface to the FFD program.			
6	Access Control Models			
6.1(i)	The system shall be able to enforce access through the different types of controls such as:			
	1) Attribute-based Access Control (ABAC)	Comply		
	2) Discretionary Access Control (DAC)	Comply		
	3) History-Based Access Control (HBAC)	Comply		
	4) Identity-Based Access Control (IBAC)	Comply		
	5) Mandatory Access Control (MAC)	Comply		
	6) Organization-Based Access control (OrBAC)	Comply		
	7) Role-Based Access Control (RBAC)	Comply		
7	System architecture			
7.1	The system should have a distributed architecture with tiered model comprising Primary Servers, Regional Servers and Site Servers.			
7(1)	There shall be a primary server hosted at the main Security control centre which shall act as a single source for all Eskom’s card Holder data.	Comply		
7(2)	The primary server shall have redundancy with real time synchronisation with the secondary/ back-up server.	Comply		
7(3)	At regional level there shall be regional servers connected to the Primary server via the Eskom Telecoms IP network.			

7(4)	The regional servers shall have real time synchronisation of card holder information with the Primary server. These servers shall have a daily full server backup.			
7(5)	At site level (where applicable), there shall be site server(s) installed with various security end point devices. The sites server(s) shall be capable of operating in isolation if it loses connectivity to the regional sever to ensure business continuity.	Comply		
7(6)	Firewalls and servers shall be managed by Eskom to ensure confidentiality and integrity of information. Where a third-party is appointed for management of firewalls and servers, there shall be a non-disclosure agreement signed between Eskom and the third-party and Eskom shall be approached for approval of any planned upgrades or changes before they are implemented.	Comply		
8	Communication and network requirements			
8.1	General communication requirements			
8.1 (1)	Suppliers shall ensure that the system is capable of using Eskom's existing communication infrastructure.	Comply		
8.1 (2)	The network infrastructure shall adhere to the principles laid out in the following documents which will be made available to the contracted supplier:			
	a) **240-554109–7** - Cyber Security Standard for Operational Technology	Comply		
	b) **240-556835–2** - Definition of Operational Technology (OT) and OT / IT Collaboration Accountabilities	Comply		
	c) **32-1203** – Eskom Telecommunications User Requirements Specification	Comply		
	d) **240-941363–6** - IP Voice and Data Network Design Guideline.	Comply		

	e) **240-46264031** – Fibre Optic Design Standard – Part 2: Substations.	Comply		
	f) **IEC 62645** Nuclear Power Plants – Instrumentation and Control Systems – Requirements for Security Programme for Computer-based Systems.			
8.1(4)	The system shall allow IP to IP connection between the servers.	Comply		
8.1 (5)	The system shall allow multi-casting for distributing status information between servers.	Comply		
8.1 (6)	The servers shall be time synchronised.	Comply		
8.1 (7)	There shall be LAN points for servers with connectivity to IAC VLAN.	Comply		
8.1 (9)	Severs shall be configured with static IP addresses.	Comply		
8.1 (10)	All reader controllers shall have interface capabilities stipulated under section 4.1.3 of SANS 2220-2-4.	Comply		
8.1(11)	The System shall at minimum cater for Ethernet 10/100/1000 with auto negotiation, the supplier shall also indicate if their equipment supports the following I/O ports:			
	a) RS-232	Comply		
	b) RS-485	Comply		
	c) Wiegand in/out	Comply		
	d) TTL in/out	Comply		
	e) Modem (to provide alternative Comms where there is no network infrastructure installed).			
8.2	Supported communication standards			
8.2(1)	The system shall support open communication standards/protocols	comply		
8.3	Bandwidth requirements			

8.3 (a)	Bandwidth allocation for the system shall Comply with the requirements of Eskom Telecommunications User Requirement Specification (Unique identifier: 32-1203).	Comply		
9	Cyber security			
9(1)	The system shall Comply with Eskom' Cyber Security standard for Operational Technology (Unique identifier: 240-55410927).	comply		
9(2)	The system shall Comply with the requirements of Demilitarised Zone (DMZ) designs for Operational Technology (Unique identifier: 240-79669677).	comply		
9(3)	For nuclear sites the system shall Comply with site specific cyber security procedures and programs.			
10	Hardware requirements			
10.1	Server requirements			
10.1 (1)	The server shall Comply with the requirements of SANS 2220-2-2.	Comply with reference.		
10.1 (2)	There shall be a primary server where all the system configurations and event data is stored.	Comply		
10.1(3)	There shall be a redundant sever which is a mirror of the primary server	Comply		
10.1(6)	There shall be synchronization between field devices and server network such that transaction records are automatically uploaded from each reader to the relevant database.	Comply		
10.1(7)	The server shall automatically back up data, this data shall be stored for a minimum period of 36 months.	Comply		
10.1 (8)	There shall be LAN points for servers with connectivity to the IAC VLAN.	Comply		

10.1(9)	There shall be servers that handle administration at each site that can be diverted to a central server that is situated at the security control centre	Comply		
10.1(10)	The server shall be able to handle the automatic deletion of visitor and contractor account/profile after the expiry date.	Comply		
10.1(11)	The server shall be able to handle the deletion and removal of redundant account/profile based on information received from an administrator workstation.	Comply		
10.1(12)	Cabinets with minimum IP 65 rating shall be used for servers. These shall be housed inside the nearest restricted building such as guard house or access control building.	Comply		
10.1(13)	The server shall have 99.99 % availability.	Comply		
10.1 (14)	The server shall be of a modular design.	Comply		
10.1(15)	The server shall contain a real-time clock circuit synched with a GPS time clock, capable of maintaining and displaying real time (month, day, hour, minute and second).	Comply		
10.1(16)	Interface between the server and the peripheral devices (such as readers and reader controllers) shall be by means of a standard communications protocol.	Comply		
10.1(17)	The server shall allow entry to the system parameters by password only, and there shall be at least three levels of password to allow three levels of access.	Comply		
10.1 (18)	The server software shall maintain a real-time sequential record (on the hard disk) of reader events, alarm events and all operator programming events	Comply		

10.1 (19)	Server sizing shall be guided by factors such as number of estimated card holders, information retention period and storage for backups	Comply		
10.2	Registration stations			
10.2(1)	The Security Manager shall be the owner and main operator of the system responsible to provide any changes and permissions to the system.	Comply		
10.2 (2)	The registration facility shall enable the Security Manager to be able to register, disable, enable and change personnel details of employees, Visitors and other personnel onto the access control system for them to be able to gain access into the approved areas as approved by the security management team.	Comply with reference.		
10.2 (3)	A full audit-trail shall be provided for all registration transactions.	Comply		
10.2(4)	Registration shall be fingerprint protected – i.e. the access control administrator shall be required to fingerprint in order to login to the registration application.	Comply		
10.2(5)	The registration stations shall be integrated to the database where the access control data is kept.	Comply		
10.2 (6)	Permanent employees shall only be registered once authorization has been given.	comply		
10.2 (7)	Visitors shall only be authorised for registration when a valid identity document is produced and confirmation from the Eskom employee been visited has been received.	comply		
10.2 (8)	Contractors shall only be authorised for registration after producing a valid labour requisition form with start and end date captured and a valid identity document. There shall be automatic lockout after completion of the work related to the contract.	Comply		

10.2(9)	Permanent employee's access rights shall only be disabled on request from the Security and/or HR department.	comply		
10.2(10)	Visitors' access rights shall be disabled by the access control auto-disabling function at the end of the scheduled visiting time/period and/or at the return of the visitor access card in the drop box.	Comply		
10.2 (11)	Contractors' and sub-contractors access rights shall be disabled once the term that is recorded expires. A reminder shall be generated by the system 48 hours prior to disabling the access rights. This reminder shall be sent to HR department, affected contractors and project managers.	Comply		
10.2 (12)	The HR department shall notify the systems administrator to extend or terminate the access rights, the system shall generate automated reminders to the HR department and system administrators for access rights expiry dates.			
10.3	Client stations			
10.3(1)	The IACS shall use a client/server architecture	Comply		
10.3 (2)	The client stations shall be used by the operator to view alarm/events and manage the system. This client station shall have a standard Eskom desktop image loaded.	Comply		
10.3 (3)	The reception stations shall be used by the operator to manage visitors. This reception station shall have a standard Eskom desktop image loaded.	Comply		
10.3(4)	The software installed on the client stations shall cater for the following requirements:			
	a) Screen modification programs.	Comply		
	b) Menu modification programs	Comply		
	c) Keyboard modification programs	Comply		

	d) Colour modification programs	Comply		
	e) Icon menu modification programs	Comply		
	f) System monitor programs	Comply		
	g) Logbook reset program	Comply		
	h) Graphical font modification program	Comply		
	i) System message modification program	Comply		
10.4	Readers and reader controllers (for both outdoor and indoor use)			
10.4.1	General			
10.4.1 (1)	It shall be possible to assign to any reader an IN or OUT function in any geographic area or any combination of areas.	Comply		
10.4.1 (2)	It shall be possible for the operator to declare any reader as either card only, card plus biometrics, card plus PIN, or to switch from one state to the other.	Comply with reference.		
10.4.1 (3)	It shall be possible to attach an identifier to each reader to assist in identifying reader locations for record purposes.	Comply with reference.		
10.4.1 (4)	It shall be possible to assign to any reader a time and attendance function. This function shall be independent of the access control function. Time and attendance events shall be recorded sequentially in a separate record.			
10.4.1 (5)	It shall be possible for the processor software to enable or disable any reader at any time or to switch from one state to the other. The central processor shall generate a report showing which readers are currently enabled or disabled. There shall be an audit trail of the user who completed the change and authorization.	Comply		
10.4.2	Card readers			
10.4.2 (1)	Card readers shall Comply with requirements of SANS 2220-2-3.	Comply with reference.		

10.4.2 (2)	A card reader shall accept cards presented to it through proximity, or long distance reading or remote controls linked to access cards such that systems can be armed/disarmed and access be granted without exiting the vehicles at sites located in risky areas.	Comply		
10.4.2 (3)	The reader shall use visual confirmation e.g. light-emitting diodes to show whether access was granted or denied. The response shall be within 100 milliseconds of presentation of the access card.	Comply		
10.4.2 (4)	If a PIN keypad is included in a card reader, access shall only be granted when the card and its associated PIN have been validated.	Comply		
10.4.2 (5)	The readers shall be capable of reading access cards and send data to an associated interface.	Comply		
10.4.2 (6)	A card reader shall be capable of indicating failures as well as an alarm condition.	Comply		
10.4.3	Biometric readers			
10.4.3 (1)	Biometric readers shall Comply with requirements of SANS 2220-2-5.			
10.4.3 (2)	A biometric device shall contain a sensor that recognizes a per'on's physical characteristics, such as the following:			
	a) fingerprints;			
	b) hand geometry (finger position and length);			
	c) retina patterns;			
	d) voice patterns; or			
	e) signature			
10.4.3 (3)	If a PIN keypad (from which a personal identification number can be entered) is used, access shall only be granted on validation of both the PIN and the measured physical characteristics.			

10.4.3 (4)	There shall be biometric readers capable of requesting biometric validation after presentation of the access card, after which it shall send data to an associated interface.			
10.4.3 (5)	The MTBF (mean time between failures) of biometric readers shall Comply with section 4.1.5 of SANS 2220-2-5.			
10.4.3 (6)	If a biometric reader is connected to a central processor, it shall be by means of standard communications protocol.			
10.4.3 (7)	The biometric device shall Comply with all relevant health and safety requirements and regulations.			
10.4.3 (8)	Markings for biometric readers shall Comply with section 5 of SANS 2220-2-5.			
10.4.4	Reader controllers			
10.4.4 (1)	Reader controllers shall Comply with requirements of SANS 2220-2-4.	Comply with reference.		
10.4.4 (2)	A reader controller shall be used where a reader cannot be connected directly to a central processor.	Comply		
10.4.4 (3)	Construction of reader controllers shall Comply with section 4.1.1 of SANS 2220-2-4.	Comply with reference.		
10.4.4 (4)	The MTBF (mean time between failures) (guaranteed by the supplier) of a reader controller (assessed in accordance with IEC 60050-191 and IEC 60300 (all relevant parts)) under normal operating conditions shall be at least 8 000 h.	Comply with reference.		
10.4.4 (5)	A site server shall be used to control all reader controllers for a site.	Comply		
10.4.4 (6)	The reader/door controller must keep a local copy of the access control lists and logs, so that stand-alone operation is possible for a defined time in the event of a communications failure.	Comply		
10.6	Access cards			

10.6 (1)	Access cards shall Comply with the requirements of SANS 2220-2-6.	Comply with reference.		
10.6 (2)	Access shall be available in the formats below:			
	a) swipe cards	Comply		
	b) contact cards	Comply		
	c) passive proximity cards	Comply		
	d) active proximity cards	Comply		
10.6 (3)	Access cards shall be Eskom's approved corporate identity template and be made of a durable material that can display the following information, as required:			
	a) an ID photograph;	Comply		
	b) Employee number (unique number);	Comply		
	c) a company logo;	Comply		
	d) name and other information of bearer (e.g. vehicle permit information).	Comply		
10.6 (4)	Card printers shall be used to print the employee details and card layout directly to the cards before issuing.	Comply		
10.6 (5)	The standard card format shall at minimum have 128 Bit Encryption.	Comply with reference.		
10.6 (6)	The cards shall have support for random ID, each card shall have a unique serial number printed on the card.	Comply		
10.6 (7)	Dimensions of access cards shall Comply with section 4.1.2 of SANS 2220-2-6.	Comply with reference.		
10.6 (8)	An ACS card encoder shall be used to encode cards by loading the required information regarding the card owner before issuing of the card. Any attempt to change the code shall destroy the card.	Comply		
10.6 (9)	A photograph of the card holder shall be captured using a digital HD camera before issuing the card.	Comply		

10.6 (10)	The card shall be water resistant and resistant to wear and tear caused by extended use.	Comply		
10.6 (11)	The location of the contacts and the microchip shall not cause surface irregularities on the back of the card or in the magnetic strip area.	Comply		
10.6 (12)	It shall be possible to print a list of all card numbers and their cardholder names which conform to a combination of specific and non-specific parameters.	Comply		
10.6 (13)	When so required, the central processor shall be able to provide a print-out of all activities of a card.	Comply		
10.7	Barriers			
10.7 (1)	A barrier shall be one of the following devices intended to prevent unauthorized access to a controlled area:			
	a) an access booth;			
	b) a door (with door closer or monitor or both);			
	c) a vehicle boom;			
	d) a vehicle gate;			
	e) a vehicle stopper;			
	f) a turnstile.			
10.7 (2)	A barrier shall at minimum, consist of the following components:			
	a) a physical barrier;	Comply		
	b) a detection unit, this can be used to detect an object in the path of the barrier which could obstruct the barrier movement;	Comply		
	c) an interface to a control unit operated manually or by some access control facility;	Comply		
	d) a barrier status device, and	Comply		
	e) a tamper protection device.	Comply		

10.7 (3)	The mean time between failures (MTBF) of a barrier shall be such that, under normal operating conditions, there are at least 100 000 operations with specified maintenance and 50 000 operations without maintenance	Comply with reference.		
10.7 (4)	When an access booth is tested in accordance with section 6.3 of SANS 2220-2-7, the mechanism shall be activated by the access control system and an override switch. In the case of a power failure, the outside door of the booth shall unlock automatically, and the inside door shall lock automatically. The booth shall have a preset timer to relock the door if the booth was not used within 30 s after a door has been unlocked.	Comply		
10.7 (5)	A panic/emergency alarm facility shall be provided on the inside of the booth, to allow any person trapped inside the booth to initiate an alarm.	Comply		
10.7 (6)	If a booth malfunctions, it shall be possible to unlock the door from the outside with an emergency key override.	Comply		
10.7 (7)	A barrier shall have the necessary potential free contacts to indicate status (open/closed).	Comply		
10.7 (8)	A cubicle shall be so constructed that it is possible to anchor the booth to a solid base by means such as expanding bolts.	Comply		
10.7 (9)	A class 4 or class 5 access control system using an access booth shall have a system to detect when more than one person is using the booth. In such a case, access shall not be granted.	Comply		
10.7 (10)	The operating mechanism of the access booth shall have a locked cover equipped with a tamper protection switch.	Comply		
10.7 (11)	Turnstiles and booms			

10.7 (11)(a)	Turnstiles shall Comply with section 4.7 of SANS 2220-2-7.	Comply with reference.		
10.7 (11)(b)	A vehicle boom shall consist of the following components:	Comply		
	i. an enclosure for the operating mechanism;	Comply		
	ii. a boom;	Comply		
	iii. detector loops;	Comply		
	iv. a warning device;	Comply		
	v. a mechanical crank;	Comply		
	vi. an operating mechanism;	Comply		
	vii. a boom rest (for a boom longer than 4 m).	Comply		
10.7 (11) C)	The boom shall be activated by electronic means such as a reader controller.	Comply		
10.7 (11)(d)	The enclosure of an operating mechanism for a boom shall at minimum Comply with the requirements of class IP45 of SANS 60529.	Comply with reference.		
10.7 (11) e)	There shall be provision for single and double height turnstiles.	Comply		
10.7 (11)(f)	A drop box shall be used for visitors to capture the card on exit.	Comply		
10.7 (11)(g)	Vehicle barriers with ground loop sensors shall be installed.	Comply		
10.7(11) (h)	At vehicle entrances dual height gooseneck pedestals with rain covers for biometric readers shall be installed.	Comply		
10.7 (11)(i)	Detector loops shall be so constructed that they can be buried in a road to detect vehicle movement. The boom shall close only after the vehicle has moved over the loop. The boom shall lower 30 s after it has been raised. The sensitivity of the detector loops shall be adjustable.	Comply		
10.7 (11)(j)	Each boom shall incorporate a warning device such as lights or a siren, to indicate when the boom is in operation (opening or closing).	Comply		

10.7 (11)(k)	In case of a power failure, it shall be possible to mechanically raise and lower the boom.	Comply		
10.7 (11)(l)	The bearings of the boom shall be self-lubricating and maintenance free.	Comply with reference.		
11	Integration requirements			
11.1	General			
11.1(i)	The IACS shall be adaptable to cater for future integration requirements that Eskom will stipulate and at minimum it shall be integratable with the following systems:			
	1) Intrusion Detection system	Comply		
	2) Electric Fence system	Comply		
	3) Intercom and Public Address systems	Comply		
	4) CCTV system	Comply		
	5) Security Lighting system	Comply		
	6) Guard Tour system	Comply		
	7) Fire Detection system	Comply		
12	Buildings access control			
12 (1)	All entry points into buildings shall be secured by the Access Control system.	Comply		
12 (2)	Where viable, windows should be protected by burglar proofing, apart from areas where HV Regulations require otherwise.			
12(3)	All non-automated doors shall be fitted with a suitable grade security lock.			
12 (4)	In the administration buildings all offices shall have security gates installed on the doors, a suitable key control system shall be introduced to manage access to offices and the safekeeping of duplicate keys.			
13	Reporting			

13(i)	The Integrated Access Control System shall have Reporting capability. The system should have a set of standard off the shelf reports. The system must allow for custom development of reports. The business requirement is to build a set of custom reports that are specific to the Eskom environment and these reports should be a standard set of reports for any Eskom site nationally. Both standard and custom reports should have capability of being scheduled to run at specific dates and times and/or recurring. The system is required to contain functionality for reports to be e-mailed from within the application. The reports are required to have an export / save functionality for at least xls, csv, and pdf file formats.	Comply with reference.		
13.1	Attendance Register			
13.1 (1)	A field labelled “Flexible time” should be added to the report			
13.1(2)	A field labelled “Leave” must be added to the report as this is currently contained in the manual attendance register form. This should integrate with SAP so leave is automatically filled in.			
13.1 (3)	A filed labelled “Leave Type” must be added to the report to enable Management viewing the report to understand whether a person is on their Annual leave or sick leave etc.			
13.2	Visitor reports			
13.2 (1)	Visitor reports should cater for the requirements in Table 4 of 240-102220945	Comply		
13.2.1	Visitor/Host registration information			
13.2.1.1	The system shall cater for information fields depicted in Table 5 and Table 6 of 240-102220945 on information forms and databases to facilitate the ACS searches.	Comply		
13.3	Additional Reports			

13.3(i)	The system shall cater for additional reports as required by Eskom including but not limited to Access Denied Reports and Alarms reports	Comply		
13.4	Graphical User Interface Requirements			
13.4.1	Functional GUI Requirements			
13.4.1(1)	The GUI must implement a role-based access and privilege model so that classes of users can be given access to functions appropriate to their assigned organisational responsibilities.	Comply		
13.4.1(2)	The GUI should primarily contain floor plan views per site. Alarms page / window should form part of screen to allow the user both graphical and data alarms to select from.	Comply		
13.4.1(3)	The GUI must cater for utilising photos as the background where icons can be mapped onto it. E.g. a picture of a zone with icons of readers and controllers mapped over the picture.	Comply		
13.4.1(4)	The GUI must cater for importing drawing files of various types such as CAD files.	Comply		
13.4.1(5)	The GUI must cater for multiple floor levels – as required for buildings with more than a single floor.	Comply		
13.4.1(6)	The GUI should have the capability to display more than 1 screen (floor plan) at a time (split screens).	Comply		
13.4.1(7)	The GUI must cater for 3 dimensional models and views with related controls to navigate through the model.	Comply		
13.4.1(8)	The GUI must include a zoom function which allows for both zoom in and zoom out on floor plan views and 3 dimensional views.	Comply		
13.4.1(9)	The GUI must allow for colours to be configurable for the layouts	Comply		

13.4.1(10)	The system must cater for integration of various modules into this GUI. Readers, controllers, access points, cameras, intrusion detection system and other security related hardware devices must be mapped/displayed on the GUI. The user should be able to select from a drop down list of various components to get a dynamic view of the same. E.g. if “Readers” were selected then the floor plan should only display the readers on that floor	Comply		
13.4.1(11)	All icons mapped on the GUI must be linked with the actual hardware devices installed in the field/building/site. The linking of this must include details such as the state of the device, the alarm state if any and last person that has accessed that point if it is a reader. There must be capability of using a pop-up screen to view this status.	Comply		
13.4.1(12)	The level of detail should be at a door level, i.e. the operator does not have to have a view of the server, and converter connected to the door. The alarm should bring up details of what the hardware /tamper alert is.	Comply		
13.4.1(13)	The GUI should contain different icon types/styles for different equipment e.g. camera, reader, controller.	Comply		
13.4.1(14)	The GUI must have colour coding for hardware items depicted, i.e. use colour coding to indicate the status of hardware items.	Comply		
13.4.1(15)	Alarms must be 3 colours:	Comply		
	a) Red for high priority	Comply		
	b) Yellow for medium priority	Comply		
	c) Blue for low priority	Comply		
13.4.1(16)	The GUI must display all access points that are open e.g. doors, turnstiles especially in the case of an evacuation. A separate colour code should be used for this. Text should be displayed as well indicating emergency.	Comply		

13.4.1(17)	A flashing GUI icon should be used when a hardware failure occurs or an alarm is triggered at any specific point. The flashing should not stop until the alarm / failure has been acknowledged / opened.	Comply		
13.4.1(18)	A hardware failure or alarm should have an audible alarm sound together with the flashing icon.	Comply		
13.4.1(19)	The GUI should have a configurable threshold of the number of unacknowledged alarms and an automatic escalation via the e-mail / SMS gateway.	Comply		
13.4.1(20)	The GUI should have manual and automated methods of SMS and emailing alarms, especially for high priority alarms.	Comply		
13.4.1(21)	The GUI must allow for clicking on the icons (cameras, readers, controllers, power supply etc.) that have been mapped on the interface. The system must then respond by opening details of the linked camera/reader/controller/power supply etc.	Comply		
13.4.1(22)	Access to live and recorded camera footages must be possible from the camera links on the GUI.	Comply		
13.4.1(23)	The GUI should have an emergency contact list that the operators can quickly access in order to attend to an alarm.	Comply		
13.4.1(24)	On acknowledging/opening an alarm the GUI should display procedures to attending to the alarm.	Comply		
13.4.1(25)	The GUI should have the ability to capture sticky notes / comments to alarms and escalations.	Comply		
13.4.1(27)	GUI must show different zones and the number of people in each zone should be listed in the zone.	Comply		
13.4.1 (28)	Alarms should be displayed in real-time with the icons.	Comply		
13.4.1 (29)	Linked readers/controllers/power supplies etc. must open within 100 milliseconds requesting it to open.	Comply		

13.5	Databases			
13.5.1	General database requirements			
13.5.1 (1)	Database shall provide for regular reports and specific database queries, these should be viewable both locally (onsite) and also retrievable remotely from security control centre(s).	Comply		
13.5.1 (2)	Copies of reports from the database shall be kept for at least three years or as long as required for legal proceedings.	Comply		
13.5.1 (3)	The system shall allow for Logbook entries with the following as minimum features:			
	a) Alarm logbook for alarmed events generated by the system or peripheral devices	Comply		
	b) System logbook for all actions performed on the system	Comply		
	c) Event logbook for all events generated by the peripheral devices or by programs that are started up automatically in the background	Comply		
	d) Access logbook from all the readers	Comply		
	e) Time logbook for all time management related readings received from all the readers	Comply		
	f) Trend logbooks	Comply		
	g) Error logbook which is used for system errors as well for unauthorized access requests	Comply		
	h) Visitor logbook	Comply		
	i) Video logbook	Comply		
13.5.1 (4)	Database reports shall provide for the following functions:			
	a) Time and Attendance	Comply		
	b) Personnel tracking (Individual's historical movements to and from the various access points)	Comply		
	c) Date and time movements of Individuals or groups through the system	Comply		
13.5.2	Database structure			

13.5.2 (1)	The database shall allow for the following information to be included:			
	a) Eskom employee number (unique number)	Comply		
	b) Access ID (this shall be generated automatically by the system)	Comply		
	c) Full names and surnames	Comply		
	d) ID Number	Comply		
	e) Selection of access levels whereby the level where access is required is selected at the registration facility	Comply		
13.5.2 (2)	The employee status shall be either of the following:			
	a) Eskom employee	Comply		
	b) Sub-contractor	Comply		
	c) Visitor	Comply		
	d) Contractor	Comply		
	e) Security services	Comply		
	f) Vendor (to be used for regular visitor)	Comply		
14	Alarms			
14 (1)	The system alarms shall Comply with Specification for Integrated security Alarm system for protection of Eskom installations and its subsidiaries (240-86738968).	Comply		
14 (2)	2) Where access control and alarm monitoring are carried out on the same central display screen, the central display screen shall:			
	a) Serve as a logged message output device and an opera'or's screen;	Comply		
	b) Be capable of being used as an alarm display terminal;	Comply		
	c) Be able to view the alarm display and other displays concurrently ; and	Comply		
	d) While the screen is being used by the operator for card or system programming, allow logging to occur.	Comply		

14 (3)	Error messages shall cause a beep tone to be sounded. The message shall stand until the error is acknowledged by the operator. All events printed on the printer shall include the time of the event to the nearest second, and details of the event.	Comply		
14 (4)	System shall have the following alarms capabilities:			
	a) Alarm handling screen	Comply		
	b) Graphics associated with alarms	Comply		
	c) Alarm classification	Comply		
	d) Report back facility why the alarm occurred	Comply		
	e) Logging of all transactions in the alarm logbook	Comply		
15	Power supply			
15 (1)	The power unit of an access control system shall Comply with the requirements of SANS 2220-1-7.	Comply with reference.		
15 (2)	All backup supplies shall Comply with 240-53114248, Thyristor and switch mode chargers, AC/DC to DC/AC converters and inverter/uninterruptable power supplies standard.	Comply with reference.		
15 (4)	There shall be an intelligent power supply that monitors incoming power, battery status and only supply power to the servers.	Comply		
15 (5)	There shall be a backup battery that ensures at least 12 hours autonomy.	Comply with Reference		
15 (6)	The system shall still operate in the event of a main power failure.	Comply		
15 (7)	Each system or subsystem shall have a dedicated circuit breaker and supply circuit.	Comply		
15 (8)	There shall be UPS with sufficient capacity to support all ACS equipment for a minimum of 8 hours.	Comply		

15(9)	Electro-magnetic radiation from the UPS shall not affect the operation of other electronic equipment in the equipment room	Comply		
15 (10)	The battery system shall be maintenance free with a 5 year guarantee.	Comply		
16	Cabling requirements			
16 (1)	Cables shall Comply with the requirements of Eskom's Standard for Wiring and Cable marking in Substations (240-64636794).	Comply		
16 (2)	Terminal blocks shall be in accordance with Eskom standard 240-70413291, Specification for Electrical Terminal Blocks.	Comply		
16 (3)	All wiring shall be concealed inside trunking or conduit. No exposed wiring will be accepted except at sites where suitable cable trays are installed.	Comply		
16(4)	Cabling in roof or floor voids shall be installed in cable trays. Where cable trays are not available or viable, conduit will be acceptable.	Comply		
16 (5)	Cabling in trays shall be tied off at a maximum of 1.5m interval.	Comply		
16 (6)	Data and low voltage (0-48V DC/AC) cable installations shall be separated from mains power installations by a minimum of 500mm.	Comply		
16 (7)	Where data and low voltage cabling has to cross power cabling, this shall always be at 90° angles.	Comply		
16 (8)	Cabling in manholes shall be kept above the manhole floor level to avoid water contact.	Comply		
16 (9)	Cable shall be handled with care and not pulled with excessive force that may cause internal damage.	Comply		
16 (10)	The installer must adhere to the drawings and specifications at all times. Where a discrepancy exists between a drawing and these specifications, the higher of the two standards is to be followed.	Comply		

16 (11)	The installation contractor shall provide detailed as built drawings indicating cable routes, installation locations and unique equipment identifiers on completion of each logical section of an installation.	Comply		
16 (12)	Cables are not to be bent at a radius of less than four times the diameter of the cable or tighter than specified by the manufacturer.	Comply		
16(13)	There shall be no cables running next to devices that may cause electro-magnetic interference.	Comply		
16 (14)	Tensioning of cables shall not exceed 10kg.	Comply		
16 (15)	Correct wiring schematic shall be followed.	Comply		
16 (16)	All wiring shall be terminated with bootlace ferrules of the appropriate size and colour to match the cable.	Comply		
16(17)	All bootlace ferrules shall be properly crimped and shall have good mechanical and electrical connection.	Comply		
16(18)	A dedicated ferrule crimper when crimping bootlace ferrules shall be used. The use of side-cutters, pliers or other tools for crimping is not acceptable.	Comply		
16 (19)	No short circuits shall be caused when cutting cables.	Comply		
16 (20)	Where cables are laid in trenches, they shall be armoured.	Comply		
16 (21)	Trenches shall be 600 mm deep measured from average ground level to the top of the upper sleeve or cable.	Comply		
16 (22)	Where any power reticulation work has been undertaken, contractors shall make provision to submit an approved reticulation certificate issued by an authorised electrical Contractor.	Comply		
16 (23)	With respect to site cabling, no cable joints shall be accepted between buildings and control room.	Comply		

17	Physical requirements			
17.1	Tamper protection			
17.1 (1)	Tamper protection for the electrical components of the IACS shall be in accordance with section 4.10 of SANS 2220-2-1	Comply with reference.		
17.2	Ingress protection			
17.2 (1)	The enclosures for the electrical and electronic circuits shall, unless otherwise specified, provide protection of class IP65 in accordance with SANS 60529.	Comply with reference.		
17.3	Safety			
17.3(i)	The mechanical construction of any part of the system shall be such that injury caused by mechanical instability or by moving parts, protruding or sharp edges is prevented.	Comply		
18	Environmental requirements			
18.1	General			
18.1 (1)	Access cards shall Comply with environmental requirements of 4.2 of SANS 2220-2-6.	Comply with reference.		
18.2 (2)	Biometric readers shall Comply with environmental requirements of 4.2 of SANS 2220-2-5.			
18.2 (3)	Servers/central processors shall Comply with environmental requirements of 4.2 of SANS 2220-2-2.	Comply with reference.		
18.2 (4)	Card readers shall Comply with environmental requirements of 4.2 of SANS 2220-2-3.	Comply with reference.		
18.2 (5)	Barriers shall Comply with environmental requirements of 4.8 of SANS 2220-2-7.	Comply with reference.		
18.3	EMC requirements			
18.3 (1)	Signal, voltage and electromagnetic radiation levels in readily accessible areas shall not be dangerous.	Comply with reference.		
18.3 (2)	System and its components shall Comply with requirements of SANS 61000-1-2.	Comply with reference.		
18.4	Earthing			

18.4 (1)	The Earthing of the system shall Comply with Eskom's earthing standards below:			
	a) 240 – 56872313 – Radio Station Earthing and Bonding.	Comply		
	b) 240 – 56356396 – Earthing and Lightning Protection Standard.	Comply		
	c) TST41-8–7 - Transmission Substation Design Earthing Standard	Comply		
19	Labelling and numbering			
19 (1)	Terminal boxes and terminals shall be numbered and labelled accordingly in line with the approved labelling standards specific to area of applicability.	Comply		
19 (2)	Numbering and labelling of system components shall be executed in such a way that it can be guaranteed that a maintenance artisan can trace wiring (cores) with the as-built information only.	Comply		
19(3)	Labelling at power stations, excluding nuclear power stations shall Comply with requirements of Plant Labelling and Equipment Description Standard (240-71432150).	Comply		
19 (4)	Labelling at Transmission sites shall Comply with requirements of Standard for Labelling of Secondary Plant Equipment (240-62362652).	Comply		
20	Markings			
20 (1)	Markings for access cards shall Comply with section 5 of SANS 2220-2-6.	Comply with reference.		
20(2)	Markings for biometric readers shall Comply with section 5 of SANS 2220-2-5.			
20(3)	Markings for servers/central processors shall Comply with section 5 of SANS 2220-2-2.	Comply with reference.		
20 (4)	Markings for card readers for shall Comply with section 5 of SANS 2220-2-3.	Comply with reference.		

20(5)	5) Markings for barriers shall Comply with section 5 of SANS 2220-2-7.	Comply with reference.		
21	Inspections and methods of tests			
21(1)	Inspections and methods of test for servers/central processors shall comply with section 6 of SANS 2220-2-2.	Comply		
21(2)	Card reader inspections and methods of tests shall comply with section 6 of SANS 2220-2-3.	Comply		
21(3)	Inspection and tests methods for biometric readers shall comply with section 6 of SANS 2220-2-5.	Comply		
21(4)	Inspection and methods of tests for reader controllers shall comply with section 6 of SANS 2220-2-4.	Comply		
21(5)	Inspections and methods of tests for access cards shall comply with section 6 of SANS 2220-2-6.	Comply		
21(6)	Inspections and methods of tests for barriers shall comply with section 6 of SANS 2220-2-7.	Comply		
22	Miscellaneous requirements			
22.1	Spares			
22.1(1)	The contractor shall provide a priced spares breakdown for each item of equipment.	Comply with reference.		
22.1(2)	The supplier shall indicate explicitly any licence conditions for associated software, what the duration of the licence is, and whether periodic payments would have to be made.	Comply with reference. Specify.		
22.1(3)	The supplier shall provide a recommended list of spares that Eskom should hold. The quantity of such spares will be a function of the installed base and MFBF figures.	Comply with reference. Specify.		
22.1(4)	There shall be provision for direct replacement spares to be obtained from the manufactures.	Comply with reference. Specify. Provide details of OEMs.		

22.1(5)	There shall be a formal OEM support and agent agreement letter provided by the supplier for local availability of spares and repair services.	Comply with reference. Specify.		
22.1(6)	There shall be a provision for Eskom to Establish contracts with external companies to facilitate the repairs of faulty equipment.	Comply with reference. Specify.		
22.1(7)	There shall be a provision to keep portable (non-strategic) spares in strategic stores and dispatched when required.	Comply with reference. Specify minimum spares holding.		
22.1(8)	There shall be provision to keep critical spares at minimum levels as identified by the custodians in the critical spares stores.	Comply with reference. Specify.		
22.1(9)	For emergency replacements where it could be difficult to wait for the spares to be dispatched, there shall be a provision to keep the spares at local stores.	Comply with reference. Specify.		
22.1(10)	There shall be provision to channel the spares from grids and other stake holders via an identified stores custodian who will exchange the faulty spare for the working one	Comply		
22.1(11)	Lead time to replace a spare shall be a day, at maximum.	Comply		
22.1(12)	Suppliers shall notify Eskom before they discontinue or modify any part of the system to allow procurement arrangements for the installed spares base.	Comply		
22.3	Training			
22.3(1)	Training courses for Eskom technicians shall be provided in the Republic of South Africa.	Comply		

22.3(2)	Courses shall be structured on a modular basis by individual equipment, such that a series of modules may be run consecutively to meet the needs of a particular group of trainees	Comply with Reference. Provide the course curriculum and accreditation information.		
22.3(3)	Unless the training needs to be provided in a specialized facility in South Africa, it is desirable that courses be conducted at various Eskom centres around the country	Comply		
22.4	Warranty			
22.4(1)	Suppliers shall state the warranty period on all offered equipment and the terms thereof.	Comply with Reference.		
22.4(2)	It is a requirement that the supplier accepts that on-site fault investigation shall be carried out by Eskom technicians with the warranty remaining intact.	Comply		
22.4(3)	The supplier shall indicate explicitly whether the equipment is limited in any way by licences and/or software maintenance agreements. In addition, the supplier shall include in the price the cost of all features, capabilities and capacities (i.e. will one have to pay for extra licences when either scaling up the deployment, or to get full functionality.	Comply with Reference.		
22.4(4)	The supplier shall indicate available options and costs for maintenances, upgrades, etc. of the offered equipment. In addition, the supplier shall furnish Eskom with technology roadmaps for the offered equipment.	Comply with Reference.		
22.5	Support contract & Repairs requirements			
22.5(1)	The supplier shall provide a repair service for faulty units, subunits and modules removed from site by Eskom technicians.	Comply		

22.5(2)	Within the contracted repair turnaround time, the supplier shall return to Eskom either the repaired item or a replacement thereof	Comply		
22.5(3)	Repaired items shall be warranted against a repetition of the same fault for a period of three months from the date of return.	Comply		
22.5(4)	The turnaround time for the repair and return service shall be thirty (30) calendar days.	Comply		
22.5(5)	The contractor shall provide a 24 h standby service.	Comply with Reference. Contact details and response footprint.		
22.5(6)	The contractor shall provide a technical assistance and support service for second and third line maintenance locally.	Comply with Reference. Contact details and response footprint.		
22.5(7)	The contractor shall provide software updates, patches and/or firmware when they become available.	Comply		

Annex C – Technical Schedules A/B for IT Infrastructure & PSIM

The details of the Technical Schedule for the Desktop Evaluation for IT Infrastructure & PSIM are listed in the Microsoft Excel spreadsheet, titled "Consolidated spreadsheet PSIM Evaluation Criteria rev2.14 Update1", sheet "Master Evaluation Criteria", listed in Table C.1 below.

Table C.1: List of evaluation criteria and weighting for each system for the IT Desktop Evaluation

Evaluation criteria	Evaluation Score	Weight
Section–1 - General Technical Questions		10%
Section–2 - PSIM Software Questions		5%
Section–3 - Security		10%
Section–4 - Mobility		5%
Section–5 - System Integration		10%
Section–6 - Performance & Capacity Management		10%
Section–7 - Data Management		10%
Section–8 - System Implementation Strategy		5%
Section–9 - System Reporting & Analytics		10%
Section –0 - System Maintenance, Support & Lifecycle Management		5%
Section –1 - End user training		3%
Section –2 - Geospatial Capability		5%
Section –3 - Operating Systems		2%
Section –4 - License Management		5%
Section –5 - Company Profile		5%
Desktop Evaluation Total – Minimum 60% threshold		100%

The details of the Technical Schedules for the Practical Evaluations for the IT Infrastructure & PSIM are listed in the Microsoft Excel spreadsheet, titled "Consolidated spreadsheet PSIM Evaluation Criteria rev2.14 Update1", sheet "System Demo"", listed in Table C.2 below.

Table C.2: List of evaluation criteria and weighting for the IT Practical Evaluation

Evaluation criteria	Evaluation Score	Weight
System Demo		100%
Practical Evaluation (Demo) Total – Minimum 70% threshold		100%

Annex D – Technical Schedules A/B for Supplier Services & Organisation Experience

TECHNICAL SCHEDULES A & B FOR

SUPPLIER SERVICES & ORGANISATION EXPERIENCE FOR AN INTEGRATED SECURITY SYSTEM

Schedule A: Purcha'er's specifications

Schedule B: Guarantees, compliance and technical particulars of equipment offered

This document provides a schedule of compliance with regard to the Integrated Security System including other applicable Eskom specifications to be provided for this project. It cross-references all the relevant works information clauses requiring a response from Tenderers and assists Tenderers in providing a comprehensive proposal.

When completing the Schedule B and the References section, The Tenderer is required to state clearly, for each clause that requires a statement of compliance, with one of the following options:

Comply – Confirmation of FULL Compliance to all clauses of the applicable section of the Technical Standard. No deviations.

Partially Comply – Confirmation of PARTIAL Compliance and that FULL Compliance is not possible. Deviations taken.

Do Not Comp–y - Confirmation of Non-Compliance to ALL requirements in the applicable section.

Reference to evidence in the form of datasheets, equipment manuals, drawings, hyperlinks shall be included in the References section if required.

Where there are any deviations taken from the clauses in the applicable section, these should be indicated under the References and Deviations section.

Item	Description	Schedule A	Schedule B	References/ Statement (supporting evidence) if required & Deviations	Comments
1	Supplier Services & Organisation Experience				
1.1	Supplier Services	At minimum the Tenderer shall provide the following services as part of system(s) life cycle management:			
1.1.1	There shall be provision for direct replacement spares for faulty equipment for all the different equipment in the Integrated Security System	Indicate compliance and provide a list of all spares items for each type of equipment in the Integrated Security System			
1.1.2	There shall be a formal OEM and agent agreement for local availability of spares and repair services.	submit a formal OEM and agent agreement for local availability of spares and repair services.			

1.1.3	Suppliers shall notify Eskom in writing before they discontinue or modify any part of the system to allow procurement arrangements for the installed spares base.	Indicate compliance			
1.1.4	Spares for the components of the disparate systems shall be available 10 years even after the model has been discontinued.	Indicate compliance and provide a formal letter.			
1.1.5	A 5 years pro-rata warranty is required.	Indicate compliance and provide a formal letter.			
1.1.6	Repaired items shall be warranted against a repetition of the same fault for a period of three months from the date of return.	Indicate compliance and provide a formal letter.			
1.1.7	All the components of the system shall have a minimum of two years guarantee.	Indicate compliance and provide a formal letter.			
1.2	Organisation Experience				
1.2.1	Tenderer must submit company organogram, indicating team composition(s).	submit company organogram, indicating team composition(s)			
1.2.2	List of similar projects must be provided	Submit list of similar projects & customer contact details			
1.2.3	CVs for the company and staff must be submitted with the following experience / competencies :				
1.2.3(i)	Experience in design and installation of Alarms system	submit relevant CV showing the required experience in design and installation of Alarm Systems			
1.2.3(ii)	Experience in design and installation CCTV Systems, maintenance & associated communication network system fault finding	submit relevant CV showing the required experience in design and installation of CCTV Systems			

1.2.3(iii)	Experience in design and installation of Access Control Systems (IACS)	submit relevant CV showing the required experience in design and installation of Access Control Systems (IACS)			
1.2.3(iv)	Experience in design and installation of PA Systems	submit relevant CV showing the required experience in design and installation of PA Systems			
1.2.3(v)	Experience in design and installation of Intrusion pre-detection Systems	submit relevant CV showing the required experience in design and installation of Intrusion pre-detection Systems			
1.2.3(vi)	Experience in design and installation of an Integrated Security System	submit relevant CV showing the required experience in design and installation of an Integrated Security System			
1.2.3(vii)	Experience in design and installation of the IT Infrastructure and PSIM	submit relevant CV showing the required experience in design and installation of IT Infrastructure and PSIM			
1.2.4	Project Lead Engineer that is professionally registered (Pr Eng/Pr Tech) with ECSA (Engineering Council of South Africa) that will sign off the entire design.	submit relevant CV with the ECSA certificate and ECSA professional number			
1.2.5	Experience in providing training on all the components in the Integrated Security System	submit relevant CV showing the required experience in training for this system.			

Annex E – Demonstration Evaluation

The purpose of testing at the tender phase is to test whether the equipment proposed is capable of meeting the specifications. To this end, each piece of equipment needs to be demonstrated to meet the functional requirements. These tests need not be carried out on site. They may be carried out on equipment already installed on a 3rd party site by the tenderer or setup for demonstration purposes. Below is the list of functionality and requirements that will be tested: For projects with only a subset of systems included in the scope of work, the evaluation shall be limited to only those systems that form part of the scope.

Item	Criteria	Compliant / Part Compliant / Non-compliant	Details if not fully compliant	Score
1	Alarms			
1.1	The controller or user interface system shall be able to configure all the alarms in the station.			
1.2	All the alarms shall be displayed visually on the user interface at the substation.			
1.3	Alarm conditions to be resettable and acknowledgeable.			
1.4	Alarmed zone(s) of the fence shall be viewable /highlighted on the user interface/ display screen.			
1.5	Demonstrate Battery low alarm			
1.6	Demonstrate Mains supply fail alarm			
1.7	The intrusion detection system for buildings (for which access is granted) shall disarm upon granting of access by the access control system and arm upon the exiting of the person who was granted access.			
1.8	The access control door and gates access control devices shall create an alarm if there are unauthorised access attempts.			
1.9	Alarm triggers - Demonstrate activation of the alarm via the following triggers:			
	a) Due to Camera video analytics alarm detection on the site zone(s)			
	b) Noise in the guarded zones			
	c) Alarm inputs from electric fence			
	d) Alarm inputs from infrared sensors			
	e) Alarm inputs from microwave beams			
	f) Alarm inputs from panic buttons			

	g) Alarm input from pre-detection sensor(s) (e.g. fibre optic sensors)			
	h) Alarm inputs from access control points.			
	i) System should be able to be armed both manually and via a remote control.			
1.10	Pre Detection System			
	a) Demonstrate the pre-detection system, trigger the system and check all alarms on the user interface system			
	b) Demonstrate the pre-detection system zones and trigger the system on a specific zone. Check if the alarm corresponds to the zone on the user interface system			
	c) Demonstrate the configurability of the sensitivity of the pre-detection system.			
2	CCTV Note: For each of the camera tests conducted, details including Camera make & Model, Comms medium used, Camera location, Camera resolution, light conditions for the test, evident obstructions, and potential causes of the nuisance alarms should be recorded as per Annex F of the technical standard (240-91190304). The CCTV tests shall comprise of the system components including camera, DVR/NVRs, monitoring client stations etc. to reflect the proposed system.			
2.1	Demonstrate that a person is detected by a camera when walking 20m away from the camera			
2.2	Demonstrate that a person is detected by a camera when hunched 20m away from the camera			
2.3	Demonstrate that a person is detected by a camera when crawling 20m away from the camera			
2.4	Demonstrate that a person is detected by a camera when running 20m away from the camera			
2.5	Demonstrate that the camera does not result in nuisance alarm when a shadow passes within its coverage area			
2.6	Demonstrate that the camera footage is recorded			

2.7	Demonstrate that the camera records 5s before triggering and 15s after movement stops			
2.8	Demonstrate that the recorded camera footage is sufficient to confirm an intrusion			
2.9	Demonstrate that the camera records 5s before triggering and 15s after movement stops			
2..10	Demonstrate that time & date are displayed correctly on a recorded footage. (For each recorded footage document details including % Screen height, resolution achieved, Frame rate, Depth of colour as per Annex F of the technical standard (240-91190304))			
2.11	Demonstrate PTZ camera live streaming			
2.12	Demonstrate that the PTZ camera is able to perform automatic Tracking (A person shall run and walk across various areas of the site with a focus on strategic areas.)			
2.13	Demonstrate that the PTZ camera is able to zoom as required. (A person shall run and walk across various areas of the testing area/site)			
2.14	Demonstrate that the PTZ camera is able to perform live viewing both onsite and offsite (State the Comms medium used for off-site live viewing)			
2.15	NRV/DVR Tests Note: For all the NVR/DVR tests list NDVR Make and Model, Number of Connected Cameras , Comms Medium used as per Annex F of the technical standard (240-91190304)			
	a) Demonstrate that the NVR/DVR Records for 5s second before the event, the time of the actual event and 15s seconds after motion stops			
	b) Demonstrate that the NVR/DVR Sends short video clip / series of still pictures from the camera covering the zone where the alarm triggered to the security control room.			

	c) Demonstrate that the quality of the clip received at the control room is such that the controller can clearly identify whether the intruder detection was triggered by a human.			
	d) Demonstrate that the Control room is able to stream footage from site			
	e) Demonstrate that the Control room is able to operate PTZ			
	f) Demonstrate that the Control room is able to access PTZ present positions			
	g) Demonstrate that the DVR can simultaneously record and stream footage			
	h) Demonstrate that the DVR is able to trigger recordings based on ,manual trigger and alarm			
	i) Demonstrate that its possible to search recorded events based on date and time			
	j) Demonstrate that Playback in slow motion is possible			
	k) Demonstrate that Playback at high speed is possible			
	l) Demonstrate that All cameras on site can be synced to within 1 second of DVR time			
2.16	Video Management System (VMS)			
	a) Demonstrate that the Operator can select each camera at the site			
	b) Demonstrate that the Operator can sequentially switch between cameras			
	c) Demonstrate that the Operator can operate PTZ through full range			
	d) Demonstrate that PTZ can be controlled using pre-set positions			
	e) Demonstrate that Operator can start recordings of live footage			
	f) Demonstrate that the Operator can view recorded footage			
	g) Demonstrate that the Operator can view the location and status of the site on a map			
	h) Demonstrate that in normal state, no video is shown.			

	i) Demonstrate that if Alarm triggers at a site: controller sees a series of still images or a short video clip of the triggered zone.			
	j) Demonstrate that the controller can choose to stream video from the site.			
	k) Demonstrate that there is an event queue to allow the management and acknowledgment of multiple alarm events.			
	l) Demonstrate that All cameras on site can be synced to within 1 second of DVR time			
	m) Demonstrate that the Controller can enter comments and link them to the event			
	n) Demonstrate that It is possible to 'escalate' incidents to another workstation running the client software			
	o) Demonstrate that the VMS can simultaneously record and stream footage			
	p) Demonstrate that the recordings are electronically watermarked			
3	IACS Note: The IACS tests shall comprise of the system components including card readers, biometric readers, controllers, servers, client stations etc. to reflect the proposed system.			
3.1	Demonstrate Login to Client station with preconfigured username and password			
3.2	Demonstrate changing of card reader LED when an access card is presented to show the unlocked and locked status			
3.3	Demonstrate that a door is locked automatically when it is closed.			
3.4	Demonstrate that once an alarm has been acknowledged, it is cleared from the alarm summary page and returned to normal			
3.5	Demonstrate a door forced alarm when a door is forced open without presenting a valid card			
3.6	Demonstrate a remote operation (opening) of a door from a workstation			

3.7	Demonstrate the start-up of motor upon access granted on a valid card/biometric reader through a registered finger			
3.8	Demonstrate granting of access when any of the enrolled fingers is placed on the biometric reader sensor			
3.9	Demonstrate how the GUI displays opened and closed access points differently			
3.10	Demonstrate how the GUI displays an alarm when there is hardware failure			
3.11	Demonstrate logs for alarms, system logs, events, access logs and error logs.			
3.12	Demonstrate sequential record all Operator Configuration events			
4	PA System			
4.1	Demonstrate the siren alarm			
4.2	Configure the siren alarm			
4.3	The PA system broadcast functionality shall be done locally			
4.4	The PA system broadcast functionality shall be done remotely			
4.5	The manual broadcast shall be tested			
4.6	The configuration of parameters shall be tested using the user interface.			
4.7	Demonstrate faults on the PA system which are displayed on the user interface.			
5	Intrusion pre-detection system			
5.1	Demonstrate zoning capability for alarm monitoring and fault finding			
5.2	Demonstrate system components can be synchronized with a real-time clock with minimum accuracy of 250ms.			
5.3	Demonstrate mechanism to reduce/eliminate false alarms			
5.4	Demonstrate that the system alarms for the following conditions both locally and remotely			
	1. Intrusion pre-detection alarms			
	2. Equipment fail alarm (health check, mains supply fail, battery low)			
	3. Tamper detection			

5.5	Demonstrate that each alarm has the following details			
	1. Type of event (System, Incident, or Administrative).			
	2. Date and time of the event in format CCYY/MM/DD; hh:mm:ss.			
	3. Name/identification of the reporting device.			
	4. Location of the reporting device in the form of GPS coordinates.			
5.6	Demonstrate that the system resume its normal non-alarm condition within 10s after restoration from an alarm state			
5.7	Demonstrate that the detection range and sensitivity of the detectors shall be configurable.			
5.8	Demonstrate that the system shall sustain the alarm state until the controller has acknowledged a receipt of the intrusion alert on the Data Monitoring System.			
5.9	Demonstrate that there shall be a graphical user interface (GUI) with site zones and aggregation of the system data.			
5.10	Demonstrate that the system shall be configurable remotely			
5.11	The system shall allow a system administrator with the appropriate user-level authorization and two-way factor authentication to remotely configure it including arming/on, disarming/off and setting changes.			
5.12	The status of the field units/sensors shall be periodically and automatically checked and reported to the control monitoring/viewing stations. The frequency of these reporting shall be configurable.			
5.13	Transactions shall be recorded in a database with different level of administrative rights (write, read only etc).			
5.14	Database reports shall be capable of being exported and transmitted electronically in different formats (e.g., MS excel, PDF, etc).			
6	System Integration			

6.1	Cause & effect matrix: Demonstrate activation of the perimeter flood lights on the user interface system by simulating a breach on either the physical perimeter fence or virtual perimeter fence by smart cameras/beams/etc.			
6.2	Cause & effect matrix: Demonstrate activation of the substation flood lights on the user interface system by simulating:			
	a) a breach on the physical perimeter fence or virtual perimeter fence by smart cameras/beams/etc.			
	b) the outdoor sensor triggers.			
	c)the camera outdoor protected area triggers			
	d) the indoor sensor triggers			
6.3	Cause & effect matrix: Demonstrate activation of the control room lights on the user interface system by simulating:			
	a) the indoor sensor triggers.			
	b) camera indoor protected area triggers			
6.4	Cause & effect matrix: Demonstrate activation of the switch room lights on the user interface system by simulating:			
	a) the indoor sensor triggers.			
	b) camera indoor protected area triggers			
6.5	Cause & effect matrix: Demonstrate activation of any other room lights on the user interface system by simulating:			
	a) the indoor sensor triggers.			
	b) camera indoor protected area triggers			
6.6	Cause & effect matrix: Demonstrate activation of the DVR/NVR record footage on the user interface system by simulating:			
	a) a breach on the physical perimeter fence or virtual perimeter fence by smart cameras/beams/etc.			
	b) the outdoor sensor triggers.			
	c)the camera outdoor protected area triggers			

	d) the indoor sensor triggers			
	e) camera indoor protected area triggers			
	f) authorised access			
6.7	Cause & effect matrix: Demonstrate activation of the alarm signals (text and video) sent to Security Control Centre on the user interface system by simulating:			
	a) a breach on the physical perimeter fence or virtual perimeter fence by smart cameras/beams/etc.			
	b) the outdoor sensor triggers.			
	c)the camera outdoor protected area triggers			
	d) the indoor sensor triggers			
	e) camera indoor protected area triggers			
6.8	Cause & effect matrix: Demonstrate activation of the PTZ tracking sent to Security Control Centre on the user interface system by simulating:			
	a) a breach on the physical perimeter fence or virtual perimeter fence by smart cameras/beams/etc.			
	b) the outdoor sensor triggers.			
	c)the camera outdoor protected area triggers			
6.9	Cause & effect matrix: Demonstrate activation of the recorded message on the PA System on the user interface system by simulating:			
	a) a breach on the physical perimeter fence or virtual perimeter fence by smart cameras/beams/etc.			
	b) the indoor sensor triggers			
	c) camera indoor protected area triggers			
6.10	Cause & effect matrix: Demonstrate that the PA System Security Control operated if the alarm was verified using the user interface system by simulating:			
	a) a breach on the physical perimeter fence or virtual perimeter fence by smart cameras/beams/etc.			
	b) the outdoor sensor triggers.			

	c) the indoor sensor triggers			
	d) camera indoor protected area triggers			
6.11	Cause & effect matrix: Demonstrate activation of the triggered Alarm System Zones on the user interface system by simulating:			
	a) a breach on the physical perimeter fence or virtual perimeter fence by smart cameras/beams/etc.			
	b) the outdoor sensor triggers.			
	c)the camera outdoor protected area triggers			
	d) the indoor sensor triggers			
	e) camera indoor protected area triggers			
6.12	Cause & effect matrix: Demonstrate activation of the Alarm Zone events sent to Security Control on the user interface system by simulating:			
	a) a breach on the physical perimeter fence or virtual perimeter fence by smart cameras/beams/etc.			
	b) the outdoor sensor triggers.			
	c)the camera outdoor protected area triggers			
	d) the indoor sensor triggers			
	e) camera indoor protected area triggers			
6.13	Cause & effect matrix: Demonstrate activation of the Indoor Siren on the user interface system by simulating:			
	a) the indoor sensor triggers			
	Cause & effect matrix: Demonstrate activation of the Strobe light on the user interface system by simulating:			
	a) a breach on the physical perimeter fence or virtual perimeter fence by smart cameras/beams/etc.			
	b) the outdoor sensor triggers.			
	c)the camera outdoor protected area triggers			
	d) the indoor sensor triggers			
	e) camera indoor protected area triggers			

6.14	System Security			
	a) Demonstrate that access level can be set for user to only be able to perform operator tasks and prohibited from deleting footages, and prohibited from changing network settings.			
	b) Demonstrate that the user with configured access rights can view a time and date stamped log of all logon events			
	c) Demonstrate that the user with configured access rights Can view a log of all administrative changes made on the system, including who made the change.			
6.15	Events Log			
	a) Demonstrate that any alarm and fault triggered is logged in an easily viewable format that is date and time stamped.			
	b) Demonstrate that the events log can be sent electronically and in a Microsoft Excel format. format			
7	Supplier Services & Organisation Experience			
7.1	When the supplier is performing the practical/demonstration, are the supplier's people knowledgeable on the following systems/equipment:			
7.1.1	Alarm Systems/ Equipment			
7.1.2	CCTV Systems/ Equipment			
7.1.3	IACS Systems/ Equipment			
7.1.4	PA Systems/ Equipment			
7.1.5	Integrated Security Systems/ Equipment			
7.1.6	IT Infrastructure and PSIM Systems/ Equipment			

Annex F – Weighting and scoring criteria for Security projects with varying scope (Desktop evaluation)

	Technical Criteria Description	Criteria Weighting (%)	Criteria Sub Weighting (%)	System included in scope? (if yes = 1, if no =0)	Total Score (%)
1.	Alarm System	**10% = T1**		**Y1 = (1 or 0)**	
1.1	Compliance with Technical Schedules A/B in the Technical specification 240-86738968. (Full compliance = 179 x 3 x weight = 537 points (i.e. 100%)).		100		
2.	CCTV	**15% = T2**		**Y2 = (1 or 0)**	
2.1	Compliance with Technical Schedules A/B from this standard 240-170000257, Annex A (related to Technical specification 240-91190304). (Full compliance = 402 x 3 = 1206 points (i.e. 100%)).		100		
3	IACS	**10% = T3**		**Y3 = (1 or 0)**	
3.1	Compliance with Technical Schedules A/B from this standard, 240-170000257, Annex B (related to Technical specification 240-102220945). (Full compliance = 335 x 3 = 1005 points (i.e. 100%)).		100		
4.	PA System	**5% = T4**		**Y4 = (1 or 0)**	
4.1	Compliance with Technical Schedules A/B in the Technical specification 240-170000098. (Full compliance = 69 x 3 = 207 points (i.e. 100%)).		100		
5	Intrusion pre-detection system	**10% = T5**		**Y5 = (1 or 0)**	

5.1	Compliance with Technical Schedules A/B in the Technical specification 240-170000098. (Full compliance = 135 x 3 = 405 points (i.e. 100%)).		100		

	Technical Criteria Description	Criteria Weighting (%)	Criteria Sub Weighting (%)	System included in scope? (if yes = 1, if no =0)	Total Score (%)
5	System Integration	**15% = T6**		**Y6= (1 or 0)**	
5.1	Compliance with Technical Schedules A/B in the Technical specification 240-170000096 . (Full compliance = 90 x 3 = 270 points (i.e. 100%)).		100		
6	IT Infrastructure and PSIM	**20% = T7**		**Y7 = (1 or 0)**	
6.1	Compliance with the Technical Schedules from the Microsoft Excel spreadsheet, titled "Consolidated spreadsheet PSIM Evaluation Criteria rev2.14 Update1", sheet "Master Evaluation Criteria" that are part of the tender pack documents issued by Eskom. The overview of the scoring on the Microsoft Excel spreadsheet is listed in this standard 240-170000107, Annex C.		100		
7	Supplier Services and Organisation Experience	**5% = T8**		**Y8 = (1 or 0)**	
7.1	Compliance with Technical Schedules A/B from this standard, 240-170000257, Annex D. (Full compliance = 17 x 3 = 51 points (i.e. 100%)).		100		
8	System Design Report The tenderer is required to produce and submit a System Design Report covering at a minimum the following:	**10% = T9**		**Y9 = (1 or 0)**	
8.1	Overview of the overall design and detailing each of the different components (sub-systems)		15		

	Technical Criteria Description	Criteria Weighting (%)	Criteria Sub Weighting (%)	System included in scope? (if yes = 1, if no =0)	Total Score (%)
8.2	System architecture (Logical and Physical designs) including the integration of the different components (sub-systems).		35		
8.3	Cause and Effect matrix of the overall system to be provided.		10		
8.4	Schematics displaying the location of each component's (sub-systems) sensor (e.g. CCTV, alarm contacts, etc)		20		
8.5	Equipment list of all the different components (sub-systems)		10		
8.6	Equipment Data Sheets		10		
Totals		**Tot1 =** T1 + T2 + T3 + T4 + T5 + T6 + T7 + T8 + T9		**Tot2** = (Y1xT1)+(Y2xT2) +(Y3xT3) +(Y4xT4) + (Y5xT5) + (Y6xT6) + (Y7xT7) + (Y8xT8) + (Y9xT9)	**T3** = (Tot2/Tot1) x100
Threshold	**Threshold: Total score (T3) has to be greater or equal to (≥)70% for Tenderers to be deemed technically compliant.**				