Eskom	Guideline	Group Investigations and Security

Title: **Guideline for Outcome-Based Contracts**

Document Identifier: **559-348635181**

Alternative Reference Number: **Not applicable**

Area of Applicability: **Eskom Holdings SOC Ltd**

Functional Area: **Security**

Revision: **1**

Total Pages: **47**

Next Review Date: **April 2028**

Disclosure Classification: **Controlled Disclosure**

Compiled by	Supported by	Functional Responsibility	Authorised by
K Moloi	M Mthimunye	R Govender	T Kulu
Senior Advisor	Middle Manager	Senior Manager	General Manager
Security Solutions Physical	National Security Control Centre	Security Solutions Physical	Group Investigation and Security
Date: 15/05/2025	Date: 16/05/2025	Date: 16/05/2025	Date: 16/5/2025

Content

Appendix

Tables

1. Introduction

The current security contracts have demonstrated significant shortcomings, particularly in terms of accountability and performance. Eskom is experiencing substantial losses due to theft, vandalism, and other security breaches, yet there is no clear mechanism to hold service providers accountable for these failures. This lack of accountability stems from the fragmented nature of existing contracts, where guarding services and technology maintenance are often handled by separate entities, leading to a "*blame game*" when incidents occur.

The OBC model addresses this issue by providing a turnkey solution where a single service provider is responsible for guarding and technology. This ensures that all risks are transferred to the service provider, who is incentivised to deliver results because their performance is directly tied to predefined outcomes. For example, the service provider will be held accountable and penalised accordingly if there are losses due to security breaches.

Conversely, if the service provider performs well and achieves the desired outcomes, they will be rewarded through performance-based incentives. This creates a win-win situation where Eskom benefits from improved security, and the service provider is motivated to deliver high-quality services. The OBC model shifts the focus from lowest-cost bidding to value-based procurement. Instead of simply selecting the cheapest option, Eskom will evaluate tenderers based on their ability to deliver value for money. This includes their technical capability, financial stability, innovation, and track record in delivering similar projects. By focusing on value propositions, Eskom can ensure that it selects a service provider who is not only capable of meeting the current requirements but also adaptable to future challenges.

2. Supporting Clauses

2.1 Scope

This document covers all outcome-based contracts for physical security services in Eskom Holdings Limited and all its subsidiaries. For operational stakeholders participating in the security contract lifecycle, procurement teams, security service providers, and security contract managers, it acts as a reference.

2.1.1 Purpose

The purpose is to evaluate value propositions of qualified security service providers to deliver comprehensive turnkey services for Eskom facilities, with a strong emphasis on innovation and technology integration. The goal is to enhance security outcomes, reduce reliance on physical guarding, and ensure cost-effectiveness while maintaining the safety and protection of Eskom's assets, personnel, and operations.

2.1.2 Applicability

This document shall apply throughout Eskom Holdings Limited and all its subsidiaries.

2.1.3 Effective Date

Two weeks after it has been approved.

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] ISO 9001 Quality Management Systems.

[2] Scope of Work Statements for Guarding Contracts – Guideline Document - 559-970769434.

[3] Specification for Integrated Security Alarm System for Protection of Eskom Installations and Its Subsidiaries (240-86738968)

[4] Standard for Intrusion Pre-Detection Systems Used at Eskom Sites (240-170000691)

[5] Physical Security Integration Standard (240-170000096)

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

[7] Security Public Address Systems for Substations and Telecoms High Sites (240-170000098)

[8] Specification for CCTV Surveillance with Intruder Detection (240-91190304)

[9] Security Public Address Systems for Substations and Telecoms High Sites (240-170000098)

[10] Technical Evaluation criteria for integrated physical security systems (240-170000257)

2.2.2 Informative

None.

2.3 Definitions

2.3.1 General

Definition	Explanation
Outcome-Based Contract	An outcome-based contract is a type of agreement where the payment and evaluation are tied to the achievement of specific, measurable results rather than just the completion of the task or delivery of service.
Guarding Service	The deployment of trained security personnel to protect people, assets, infrastructure and operations from security threats, unauthorised access, theft, vandalism, and other risks.
Access Control System	An access control system (ACS) is a security framework designed to regulate and monitor entry to the physical or digital environment based on predefined authorisation levels.

Definition	Explanation
Intrusion Detection System	An intrusion detection system (IDS) is a security mechanism designed to monitor, detect, and respond to unauthorised access or suspicious activities within a protected area.
Centralised Monitoring	Centralised monitoring refers to the practice of aggregating and overseeing data from various security systems such as surveillance cameras, access control systems, intrusion detection systems, and alarm systems from multiple sites into a single, unified control centre.
Surveillance System	An integrated network of hardware and software designed to continuously monitor, record, and analyse activities within a specified area. It typically incorporates devices such as cameras, sensors, and sometimes advanced analytical tools, all coordinated to provide real-time situational awareness.
Ad-hoc Review	An informal or unplanned evaluation of a document, project or process that is conducted as needed, rather than as part of a scheduled or structured review cycle. It is usually initiated in response to a specific issue, request or concern that arises unexpectedly.

2.4 Abbreviations

Abbreviation	Explanation
OBC	Outcome-Based Contract
PSIRA	Physical Security Industry Regulation Act
CCTV	Closed-Circuit Television
PTZ	Pan Tilt Zoom
IACS	Integrated Access Control System.
AI	Artificial Intelligence.
LPR	License Plate Recognition.
UPS	Uninterrupted Power Supply.

2.5 Roles and Responsibilities

Security contract managers, procurement team, service providers and other related operational stakeholders involved in safeguarding Eskom assets and its personnel shall ensure that they implement these guidelines when dealing with Eskom outcome-based contracts.

2.6 Process for Monitoring

To guarantee compatibility with Eskom's security long-term strategic objectives, the process monitoring will be carried out using a systematic and ongoing improvement methodology. Frequent evaluations will be conducted to monitor adherence to contractual duties, identify areas for improvement, and boost overall effectiveness. Ad-hoc reviews will be carried out as needed to address emerging challenges and reduce risk, in addition to planned assessments. The line division managers will be responsible for process monitoring.

2.7 Related/Supporting Documents

Not applicable.

3. Scope of work

Service providers will be required to deliver an integrated solution:

3.1 Physical Guarding Services

- Provide trained and certified security personnel for 24/7 guarding at Eskom facilities.
- Ensure compliance with PSIRA Regulations and Eskom's Security Standards.
- Compliance in respect of Firearm Standards.
- Supporting evidence in terms of contractual obligation, e.g., proof of armoured vehicles.
- Implement a robust command-and-control structure for effective coordination and incident management.

3.2 Technology Integration

Propose and implement technology-driven solutions to reduce reliance on physical guarding.

Examples Include:

3.2.1 Surveillance Systems: Advanced CCTV cameras (a combination of different camera types, e.g., thermal, optical, PTZ, etc.) with AI-based analytics for real-time threat detection.

3.2.2 Access Control Systems: Automated access control systems (e.g., biometric scanners, license plate recognition) with multi-factor authentication on restricted areas.

3.2.3 Drones: For perimeter surveillance and rapid response to incidents.

3.2.4 Intrusion Detection Systems: Motion and or vibration sensors, thermal imaging, and other advanced detection technologies.

3.2.5 Fogging Unit: A device used to release dense fog when the alarm is triggered to reduce visibility to prevent intruders from seeing or stealing valuables

3.2.6 Centralised Monitoring: A centralised control room for real-time monitoring and response coordination.

3.3 Innovation and Continuous Improvement

- Service providers must submit a technology roadmap outlining how to introduce and scale innovative solutions over the contract period.
- Proposals must include measurable outcomes (e.g., reduction in guarding personnel, improved incident detection rates, incident management and avoiding reoccurrence, and cost savings).

4. Outcomes-Based Performance Metrics

Service providers will be evaluated and remunerated based on the achievement of the following outcomes specific to the Security Department's risk:

Metric	Target	Measurement Method	Tolerance Level
• Incidents relating to loss or damage of property during deployment to the Eskom facility	• High-impact sites (e.g., Eskom network-critical facilities): 0 incidents (zero tolerance). • Low-impact sites (e.g., non-critical facilities): ≤ 2 minor incidents per month (with corrective actions implemented).	• Daily incident reports reviewed by the site manager. • Monthly audit of incident logs. • Verification through client feedback and Eskom facility reports.	• High-impact sites: Zero tolerance for any incidents. • Low-impact sites: Minor incidents (e.g., non-critical property damage) allowed, provided corrective actions are taken within 24 hours.
• All security incidents are detected, recorded, and a correct response is rendered	• High-impact sites: 100% detection, recording, and correct response (zero tolerance for failures). • Low-impact sites: ≥ 95% detection, recording, and correct response (minor delays allowed, provided they are resolved within 1 hour).	• Review of incident logs and response reports. • Eskom feedback on incident handling.	• High-impact sites: Zero tolerance for missed incidents or incorrect responses. • Low-impact sites: Minor delays (e.g., < 1 hour) allowed, provided they are documented and resolved promptly.
• Compliance with regulatory and legislative requirements (PSIRA, FCA, NKP, 2.2.1, CIPA, etc.)	• High/low impact Sites: 100% compliance (zero tolerance for non-compliance).	• Monthly audits of compliance documentation. • Review of training records and certifications (e.g., PSIRA licenses). • External regulatory body inspections and reports.	• High/Low impact sites: Zero tolerance for non-compliance.

• Mandatory technology availability and equipment compliance.	• High-impact sites: 99% availability; failures rectified within 2 hours. • Low-impact sites: 95% availability; failures rectified within 6 hours.	• Daily system uptime reports. • Maintenance logs and response time records.	• High-impact sites: Zero tolerance for extended downtime (> 2 hours). • Low-impact sites: Minor downtime (< 6 hours) allowed, provided it does not recur frequently.
• Achieve Overall customer satisfaction with security services of at least 90% per month.	• High-Impact Sites: ≥ 95% satisfaction per month. • Low-Impact Sites: ≥ 85% satisfaction per month.	• Monthly customer satisfaction surveys. • Site Manager/ Supervisor to compile and submit a customer service report to the Security Manager.	• High-impact sites: Zero tolerance for satisfaction below 95%. • Low-impact sites: Satisfaction levels between 85-95% are acceptable, provided improvement plans are implemented.

Key notes:

- **High-Impact Sites:** These are facilities where incidents could severely affect the Eskom network or operations. Zero tolerance is applied to ensure maximum reliability and security.
- **Low-Impact Sites:** These are facilities where incidents have a lower impact on operations. Minor tolerances are allowed, provided corrective actions are taken promptly.
- **Corrective Actions:** For low-impact sites, any incidents or failures must be accompanied by documented corrective actions to prevent recurrence.
- **Incentives:** The supplier may be eligible for a performance reward of up to 1% of the contract value for the relevant service period, provided such payment is approved by Procurement and complies with NT regulations.

5. Consequence Management Framework with Main Supplier Accountability

5.1 Main Supplier's Accountability for Service Partners

Accountability Clause:

The main supplier who signs the contract with Eskom will be held **fully accountable** for the performance, actions, and breaches of any service partners, subcontractors, or third-party vendors involved in delivering the services. This includes:

- Financial losses incurred due to non-performance or breaches by service partners.
- Compliance with all regulatory and legislative requirements.
- Adherence to the agreed-upon KPIs and service levels.
- Implementation of corrective actions and strategy changes as required.

5.2 Obligations of the Main Supplier

The Main Supplier must:

Ensure that all service partners comply with Eskom's requirements and the contract terms.

- Monitor and report on the performance of service partners regularly.
- Take immediate corrective action if service partners fail to meet the required standards.
- Bear all costs associated with breaches, losses, or penalties caused by service partners.

5.3 Consequence management framework (Security Departments must adapt according to their requirements and be guided by Eskom's Procurement departments and Eskom's SCM Policy).

5.3.1 Incidents Relating to Loss or Damage of Property

High-Impact Sites (Zero Tolerance):

- **First Breach:** Formal written warning, mandatory retraining, and recovery of losses by Eskom. The main supplier must ensure the service partner takes corrective actions.
- **Second Breach:** Financial penalty (5% of annual contract value), independent audit, and recovery of losses. The main supplier must replace the non-performing service partner.
- **Third Breach:** Termination of contract and recovery of all losses.

Low-Impact Sites (≤ 2 Minor Incidents/Month):

- **First Breach:** Verbal warning, corrective action within 24 hours, and recovery of losses. The main supplier must ensure the service partner implements corrective actions.
- **Second Breach:** Written warning, additional training, and recovery of losses. The main supplier must review the service partner's performance.
- **Third Breach:** Financial penalty (5% of annual contract value), performance review, and recovery of losses. The main supplier must replace the non-performing service partner.

5.3.2 All Security Incidents Detected, Recorded, and Correct Response Rendered

High-Impact Sites (Zero Tolerance):

- **First Breach:** Formal written warning, mandatory retraining, and recovery of losses. The main supplier must ensure that corrective actions are taken by the service partner.
- **Second Breach:** Financial penalty (5% of annual contract value), independent review, and recovery of losses. The main supplier must replace the non-performing service partner.
- **Third Breach:** Termination of contract and recovery of all losses.

Low-Impact Sites (≥ 95% Detection and Response):

- **First Breach:** Verbal warning, corrective action within one hour, and recovery of losses. The main supplier must ensure the service partner implements corrective actions.
- **Second Breach:** Written warning, additional training, and recovery of losses. The main supplier must review the service partner's performance.
- **Third Breach:** Financial penalty (5% of annual contract value), performance review, and recovery of losses. The main supplier must replace the non-performing service partner.

5.3.3 Compliance with Regulatory and Legislative Requirements

- **First Breach:** Formal written warning, immediate corrective action, and recovery of losses. The main supplier must ensure the service partner complies.
- **Second Breach:** Financial penalty (5% of annual contract value), independent audit, and recovery of losses. The main supplier must replace the non-compliant service partner.
- **Third Breach:** Termination of contract and recovery of all losses.

5.3.4 Mandatory Technology Availability and Equipment Compliance

High-impact Sites (99% availability, ≤ two hours downtime):

- **First Breach:** Formal written warning, immediate rectification, and recovery of losses. The main supplier must ensure the service partner rectifies the issue.
- **Second Breach:** Financial penalty (5% of annual contract value), independent review, and recovery of losses. The main supplier must replace the non-performing service partner.
- **Third Breach:** Termination of contract and recovery of all losses.

Low-Impact Sites (95% availability, ≤ six hours downtime):

- **First Breach:** Verbal warning, corrective action within six hours, and recovery of losses. The main supplier must ensure the service partner rectifies the issue.
- **Second Breach:** Written warning, additional training, and recovery of losses. The main supplier must review the service partner's performance.
- **Third Breach:** Financial penalty (5% of annual contract value), performance review, and recovery of losses. The main supplier must replace the non-performing service partner.

5.3.5 Customer Satisfaction

High-Impact Sites (≥ 95% Satisfaction):

- **First Breach:** Formal written warning, improvement plan, and recovery of losses. The main supplier must ensure the service partner implements the plan.
- **Second Breach:** Financial penalty (5% of annual contract value), independent review, and recovery of losses. The main supplier must replace the non-performing service partner.
- **Third Breach:** Termination of contract and recovery of all losses.

Low-Impact Sites (≥ 85% Satisfaction):

- **First Breach:** Verbal warning, improvement plan, and recovery of losses. The main supplier must ensure the service partner implements the plan.
- **Second Breach:** Written warning, additional training, and recovery of losses. The main supplier must review the service partner's performance.
- **Third Breach:** Financial penalty (5% of annual contract value), performance review, and recovery of losses. The main supplier must replace the non-performing service partner.

Any financial penalty deductions applied must first be authorized by Procurement, ensuring alignment with Eskom and National Treasury guidelines.

6. Detailed Specifications for Security Components

6.1 Alarm Systems Specification:

Must comply with **Specification for Integrated Security Alarm System for Protection of Eskom Installations and Its Subsidiaries (240-86738968)**.

- Integration with motion detection systems for early threat detection.
- Must include tamper-proof mechanisms and backup power supply (e.g., UPS or solar).
- Real-time alerts to a centralised monitoring system.

Performance Metrics:

- False alarm rate: ≤ 5%.
- Uptime: 98% over 36 months.

6.2 Motion Sensors Specification:

Must comply with the **Standard for Intrusion Pre-Detection Systems used at Eskom Sites (240-170000691)**.

- Strategically placed to cover all critical areas, including perimeters, entry points, and high-value assets.

- Must include advanced features such as thermal imaging and pet immunity to reduce false alarms.
- Integration with alarm systems and CCTV for real-time intrusion detection.

Performance Metrics:

- Detection accuracy: ≥ 95%.
- Response time: ≤ 5 seconds from detection to alert.

6.3 CCTV Cameras Specification:

Must comply with **Specification for CCTV Surveillance with Intruder Detection (240-91190304)**.

- High-resolution cameras (minimum 4mp) with night vision and wide dynamic range (WDR) for low-light conditions.
- AI-based analytics for real-time threat detection (e.g., loitering, perimeter breaches).
- Active monitoring 24/7 with footage stored for a minimum of 90 days.
- Integration with alarm systems and motion sensors.

Performance Metrics:

- Coverage of critical areas: 100%.
- Uptime: 98% over 36 months.

6.4 License Plate Recognition (LPR) Cameras Specification:

Must comply with **Physical Security Integration Standard (240-170000096)**.

- High-resolution cameras capable of capturing license plates in various lighting and weather conditions.
- Integration with access control systems to automate vehicle entry/exit.
- Real-time alerts for unauthorised or flagged vehicles.

Performance Metrics:

- Recognition accuracy: ≥ 95%.
- Response time: ≤ 10 seconds from detection to alert.

6.5 Access Control Systems Specification:

Must comply with **Specification for Integrated Access Control System (IACS) for Eskom Sites (240-102220945)**.

- Biometric scanners (fingerprint or facial recognition) for personnel access.
- Integration with LPR cameras for vehicle access.
- Real-time monitoring and logging of all access events.

Performance Metrics:

- System uptime: 98% over 36 months.
- False acceptance rate: ≤ 0.1%.

6.6 Public Address Systems Specification:

Must comply with Security Public Address Systems for Substations and Telecoms High **Sites (240-170000098)**.

- Clear and audible announcements for emergency notifications.
- Integration with alarm systems for automated alerts.

Performance Metrics:

- Coverage of critical areas: 100%.
- Uptime: 98% over 36 months.

6.7 Intrusion Detection Systems Specification:

Must comply with **Standard for Intrusion Pre-Detection Systems Used at Eskom Sites (240-170000691)**.

- Combination of motion sensors, thermal imaging, and perimeter detection systems.
- Real-time alerts to a centralised monitoring system.

Performance Metrics:

- Detection accuracy: ≥ 95%.
- Response time: ≤ five seconds from detection to alert.

7. Baseline Security Measures

The minimum baseline for all security contracts includes:

- **Alarm Systems:** Integrated with motion detection systems for early threat detection.
- **Motion Sensors:** Strategically placed for real-time intrusion detection.
- **CCTV Cameras:** Covering critical areas, with 24/7 active monitoring.

- **License Plate Recognition (LPR) Cameras:** Installed at specified facilities for vehicle monitoring.
- **Access Control Systems:** Biometric and automated systems for personnel and vehicle access.
- **Public Address Systems:** For emergency notifications and alerts.
- **Intrusion Detection Systems:** Advanced systems for perimeter and internal security.
- **Vibration Sensors:** Recommended for line patrol.
- **Security Fogging Unit System:** Recommended for RDC and telecommunications substation.

7.1 Mandatory Technology

- Electronic registers, access control devices, and body cameras (bodycams) must have availability of more than 95%, and failures must be rectified within two hours.
- Licence plate recognition (for specific high-volume sites) – Recommended for CNC and RDC, must have availability of more than 95%, and failures must be rectified within two hours.

8. Payment Structure

8.1 Pricing Structure

- Service providers must provide a monthly rate that includes physical guarding and technology-driven solutions.
- The pricing structure should be broken down as follows:

8.1.1 Bill of Quantities (BOQ) for Security Outcomes-based Model (RFP Level) Site information

Site ID	Site Name Not for public knowledge and only shared after contract award.	Location	Number of Access Points	Risk Level (High/Medium/Low)

8.1.2 Cost Breakdown Per Site (RFP Level)

Example

Site ID	Service Category	Description	Quantity	Unit Cost	Total Cost for contract period (three years)	PM cost
001	**Physical Guarding**	**Cost for providing trained security personnel (24/7 coverage, 2 guards per shift)**	**4 guards**	**R25000 X 4**	**R3 600 000.00**	**R100k**
001	Technology Integration	Upgrade CCTV cameras to 4K resolution (10 cameras)	10 cameras			
001	Technology Integration	Replace PA system with new Bosch LBC-350	1 system			
001	Monthly Maintenance	Technology on site	1			
001	Monitoring					
001	Armed Response					
Total for Site 001						
002	Physical Guarding	Cost for providing trained security personnel (24/7 coverage, 2 guards per shift)	2 guards			

002	Technology Integration	Upgrade alarm system to DSC Power Series Neo	1 system			
002	Innovation and Continuous Improvement	Monthly cost for proposing and scaling innovative solutions	1			
Total for Site 002						
...	...	...	...			

Total Monthly Rate

Site ID	Site Name	Total Monthly Rate

9. Technology and Data Ownership

- **Ownership of Installed Technology:** All technology (e.g., surveillance cameras, access control systems, alarms, GPS tracking devices, etc.) installed by the contractor during the contract period will remain the property of Eskom upon contract expiry or early termination.
- **Data Ownership and Access:** All data collected (e.g., surveillance footage, access logs, incident reports) during the contract period will be the sole property of Eskom. The contractor must provide Eskom with unrestricted access to this data.
- **Data Storage and Security:** The contractor must store all data securely in compliance with the Protection of Personal Information Act (POPIA) and other relevant legislation. Data must be encrypted and stored on servers located within South Africa unless otherwise approved by Eskom.
- **Data Handover:** Upon contract expiry or termination, the contractor must provide Eskom with all data in a usable format (e.g., digital files, cloud access) and ensure no data is retained or deleted without Eskom's written consent.
- **Monitoring Access:** Eskom must be provided with a secure link to monitor all surveillance and access control systems in real time. The contractor must ensure the link is operational 24/7 and accessible to authorised Eskom personnel.

- **Third-Party Control Centre access:** Eskom must have the right to visit the contractor's or third-party control centre at any time, without prior notice, to inspect operations, verify compliance, and ensure data integrity.
- **Licence Fees:** The contractor shall ensure that all license fees for installed systems, equipment, and technologies are paid and maintained throughout the contract period, with ownership and responsibility transferring to Eskom upon contract expiry or termination.

10. Key Considerations

- **Maintenance Costs:** These are recurring and should be budgeted annually.
- **Replacement Costs:** These depend on the lifespan of existing equipment and should be planned for as systems age or fail.
- **New Technology Costs:** These are one-time or periodic costs for upgrading or adding new systems.
- Payment will be aligned with the achievement of the above outcomes.
- Service providers will receive full payment only if all performance metrics are met

11. Continuous Improvement

- Service providers must submit a **technology roadmap** outlining how they will introduce and scale innovative solutions over the contract period.
- Regular performance reviews will be conducted to assess progress and identify areas for improvement.

12. Incident Reporting and Management

- **Real-Time Incident Reporting:** The contractor must provide real-time incident reports to Eskom, including details such as:
  - Date, time, and location of the incident.
  - Nature of the incident.
  - Actions taken by guards.
  - Outcome and resolution.
- **Comprehensive Investigation Reports:** The contractor must submit detailed investigation reports within 24 hours of an incident, with a full report within seven days.
- **Root Cause Analysis:** The contractor must conduct root cause analysis for all incidents and provide Eskom with recommendations to prevent recurrence.

13. Contract Management and Accountability

- Regular performance reviews will be conducted to assess the achievement of outcomes.
- Failure to meet agreed-upon outcomes will result in penalties, performance improvement plans, or contract termination.
- Service providers must continuously propose and implement innovative solutions to improve security outcomes.

14. Conclusion

This outcome-based model aims to transform Eskom's physical guarding contracts by integrating technology and innovation to enhance security while reducing costs. Service providers are encouraged to propose creative and cost-effective solutions that align with Eskom's strategic objectives.

15. Acceptance

This document has been seen and accepted by:

Full Name and Surname	Designation
Tembela Kulu	General Manager: Group Investigations and Security
Botse Sikhwitshi	Senior Manager: Security Business Intelligence
Remone Govender	Senior Manager: Security Solutions Physical
Peter Malitsha	Senior Manager: Investigations
Nomsa Spaumer	Senior Manager: Business Enablement
Melvin Murugen	Middle Manager: National Transmission Company South Africa
Motlhatlhani Khunou	Middle Manager: ERI
Monette Roets	Middle Manager: Generation
Adolph Lekganyane	Middle Manager: Distribution
Samaria Mabona	Middle Manager: ERE
Nnosi Motlana	Middle Manager: Procurement

16. Revisions

Date	Rev.	Compiler	Remarks
April 2025	1	Kgotso Moloi	Business requirement

17. Development Team

- Remone Govender, Senior Manager: Security Solutions
- Kgotso Moloi, Senior Advisor: Security Solutions
- Matsobane Phosa, Senior Advisor: Security Solutions
- Mokgadi Mthimunye, Middle Manager: National Security Control Centre

18. Acknowledgements (if applicable)

Not applicable.

Appendix A – Scope of Work (Example)

Note: Please compile a Scope of Work according to your operational requirements

Request for Information (RFI)

Outcome-based physical security services for Eskom facilities

Eskom Holdings Limited invites qualified and experienced service providers to submit proposals for the provision of Outcome-Based Physical Security Services at Eskom facilities in the (Sector name). The tender aims to deliver a value proposition centred on an outcomes-based security model, leveraging advanced technology, innovation, and measurable performance metrics to enhance safety and protection. By focusing on achieving specific, predefined security outcomes such as risk reduction, incident prevention, and operational resilience the model ensures a proactive and adaptive approach tailored to safeguarding Eskom's assets, personnel, and operations. This results-driven framework emphasizes continuous improvement, accountability, and the integration of cutting-edge solutions to provide a comprehensive, future-ready security strategy that aligns with Eskom priorities and delivers tangible, long-term value. As part of the service delivery requirements, the service provider must include the construction of a new control centre or the refurbishment of the existing control centre in their proposal. The control centre will be responsible for monitoring all technology and operations, ensuring efficient service delivery and rapid response to any issues.

Next steps

The information gathered through this RFI will be used to shortlist suppliers who demonstrate capability and a value proposition aligned with Eskom's requirements.

Shortlisted suppliers will be invited to participate in the subsequent Request for Proposal (RFP) process, where detailed technical and commercial proposals will be required.

Scope of Work (example)

The successful bidder(s) will be required to provide the following services across **(number) sectors** within the (name of area). The sites have been divided into **Sector A, Sector B, and Sector C** to ensure equitable distribution of work.
To ensure operational continuity, flexibility, and risk mitigation, it is recommended to divide service areas within each province and engage multiple suppliers. This approach ensures that the termination of a contract with one supplier does not disrupt operations, as the remaining suppliers can seamlessly overlap and cover the affected area, maintaining uninterrupted service delivery. Suppliers will be contracted for specific provinces but must be prepared to operate anywhere within the province as needed. This flexibility allows for dynamic resource allocation based on demand

fluctuations or unforeseen circumstances, ensuring that services can be scaled up or adjusted efficiently.
Engaging multiple suppliers reduces dependency on a single provider, minimising risks associated with underperformance, contractual disputes, or other operational challenges. To facilitate smooth transitions and overlap between suppliers, clear communication and coordination mechanisms must be established. These mechanisms will ensure that all parties are aligned and can respond effectively to changes or emergencies, maintaining service quality and reliability.

As part of the service delivery requirements, the service provider must include the construction of a new control centre or the refurbishment of the existing control centre in their proposal. The control centre will monitor all technology and operations, ensuring efficient service delivery and rapid response to any issues. The costs of building or refurbishing the control centre must be included in the supplier's submission during the Request for Proposal (RFP) process. Further details regarding the control centre requirements, including technical specifications and operational expectations, will be provided to suppliers during the RFP process.

This approach not only enhances operational resilience but also ensures that services can be delivered consistently and efficiently across all areas. By incorporating a control centre, oversight and coordination will be strengthened, enabling better technology and operations management. Additionally, the flexibility to deploy resources dynamically within the province ensures that suppliers can adapt to changing demands, emergencies, or other unexpected requirements, further safeguarding the continuity and quality of service delivery.

Sector Division

Sector	Sites
Sector A	
Sector B	
Sector C	

Key Requirements for RFI Submission:

1. **Company Profile and Experience:**

   Provide an overview of your organisation, including its history, size, and core competencies.

   - Demonstrate relevant experience in delivering similar services, particularly in high-security or critical infrastructure environments.
   - Include examples of past projects, highlighting success stories and measurable outcomes.

2. **Technical Capability:**

   - Describe your technical approach to delivering the required services, including any innovative methodologies or technologies you propose to use.

- Provide details on your ability to meet Eskom's specific requirements, such as incident management, regulatory compliance, and technology availability.

3. **Compliance and Certifications:**
   - List all relevant certifications, licenses, and accreditations (e.g., PSIRA, FCA, NKP, etc.).
   - Confirm your ability to comply with all regulatory and legislative requirements outlined in the RFI.
4. **Value Proposition:**
   - Clearly articulate the unique value your organisation brings to Eskom, including innovation and reliability.
   - Highlight any competitive advantages, such as advanced technology, skilled personnel, or a proven track record in similar projects.
5. **Proposed Team and Resources:**
   - Provide details of the team that will be assigned to the project, including their qualifications, experience, and roles.
   - Describe the resources (e.g., technology, equipment, and infrastructure) you will deploy to ensure successful service delivery.
6. **Risk Management and Contingency Planning:**
   - Outline your approach to identifying, mitigating, and managing risks associated with the project.
   - Provide examples of contingency plans you have implemented in previous projects to ensure continuity of service.
7. **References:**
   - Include at least three references from clients for whom you have delivered similar services, with contact details for verification.

Compliance with Eskom Standards

- **Adherence to Eskom Specifications:** All services, technologies, and systems proposed must comply with Eskom's technical standards and specifications, including but not limited to:
- **CCTV Surveillance:** Compliance with Specification for CCTV Surveillance with Intruder Detection (240-91190304).
- **Access Control Systems:** Compliance with Specification for Integrated Access Control System (IACS) for Eskom Sites (240-102220945).
- **Alarm Systems:** Compliance with Specification for Integrated Security Alarm System for Protection of Eskom Installations and Its Subsidiaries (240-86738968).
- **Intrusion Detection Systems:** Compliance with Standard for Intrusion Pre-Detection Systems Used at Eskom Sites (240-170000691).
- **Fogging Unit:** Compliance with the Standard for Fogging Unit (270-171000363)
- **Bodycam Standard:** Compliance with Standard for Body-worn Cameras (559-620181114)

- **Documentation:** Bidders must provide evidence of compliance with Eskom standards, including technical specifications, certifications, and test reports.

Value Proposition

- **Innovative Solutions:** Bidders must propose innovative and cost-effective solutions that enhance security outcomes while reducing reliance on physical guarding.
- **Measurable Outcomes:** Bidders must outline measurable outcomes, such as:
  - Reduction in physical guarding personnel.
  - Improved incident detection and response rates.
  - Cost savings through technology integration.
- **Continuous improvement:** Bidders must demonstrate a commitment to continuous improvement by proposing a **technology roadmap** that outlines how they will introduce and scale innovative solutions over the contract period.

Request for Proposal (RFP Phase).

Bidders must submit a **detailed proposal** that includes the following:

Approach to Service Delivery

Methodology for Physical Guarding Services:

- Describe the approach to deploying physical guards, including recruitment, training, and deployment strategies.
- Explain how guards will be equipped and managed to ensure optimal performance.

Integration of advanced technologies:

- Outline how technologies such as surveillance systems, access control, drones, AI-based analytics, and IoT devices will be integrated with physical guarding.
- The service provider must outline their plan for constructing or refurbishing the control room, including details on how the technology will report and transmit data to the control room, and the construction and integration of a video wall. They must provide a comprehensive approach demonstrating how these elements will be implemented to ensure effective monitoring and operational management.

- Provide a clear plan for ensuring seamless collaboration between human guards and technology.

Technology Roadmap

Implementation Plan:

- Provide a phased timeline for deploying technologies, including pilot testing, full-scale implementation, and scaling across sites.

Scalability:

- Explain how the proposed solutions can be scaled to meet Eskom's growing or changing needs

Innovation Strategy:

- Detail how the bidder will avoid emerging security threats by adopting modern and advanced technologies.

Cost breakdown

Capital Outlay:

- Explain how the initial capital investment will be sourced (e.g., internal funding, partnerships, or financing).

Performance Metrics

Metric	Target	Measurement Method	Tolerance Level
• Incidents relating to loss or damage of property during deployment to the Eskom facility	• High-impact sites (e.g., Eskom network-critical facilities): 0 incidents (zero tolerance). • Low-impact sites (e.g., non-critical facilities): ≤ 2 minor incidents per month (with corrective actions implemented).	• Daily incident reports reviewed by the site manager. • Monthly audit of incident logs. • Verification through client feedback and Eskom facility reports.	• High-impact sites: Zero tolerance for any incidents. • Low-impact sites: Minor incidents (e.g., non-critical property damage) allowed, provided corrective actions are taken within 24 hours.
• All security incidents are detected, recorded, and a correct response is rendered	• High-impact sites: 100% detection, recording, and correct response (zero tolerance for failures). • Low-Impact Sites: ≥ 95% detection, recording, and correct response (minor delays allowed, provided they are resolved within one hour).	• Review of incident logs and response reports. • Eskom feedback on incident handling.	• High-impact sites: Zero tolerance for missed incidents or incorrect responses. • Low-impact sites: Minor delays (e.g., < one hour) allowed, provided they are documented and resolved promptly.

• Compliance with regulatory and legislative requirements (PSIRA, FCA, NKP, 2.2.1, CIPA, etc.)	• High-impact/Low-impact sites: 100% compliance (zero tolerance for non-compliance).	• Monthly audits of compliance documentation. • Review of training records and certifications (e.g., PSIRA licenses). • External regulatory body inspections and reports.	• High/Low Impact sites: Zero tolerance for non-compliance.
• Mandatory technology availability and equipment compliance.	• High-impact sites: 99% availability; failures rectified within two hours. • Low-impact sites: 95% availability; failures rectified within six hours.	• Daily system uptime reports. • Maintenance logs and response time records.	• High-impact sites: zero tolerance for extended downtime (> two hours). • Low-impact sites: Minor downtime (< six hours) allowed, provided it does not recur frequently.
• Achieve overall customer satisfaction of security services of at least 90% per month	• High-impactites: ≥ 95% satisfaction per month. • Low-impact sites: ≥ 85% satisfaction per month.	• Monthly customer satisfaction surveys. • Site Manager/Supervisor to compile and submit a customer service report to the Security Manager.	• High-impact sites: zero tolerance for satisfaction below 95%. • Low-impact sites: Satisfaction levels between 85-95% are acceptable, provided improvement plans are implemented.

Monitoring and Reporting:

- Describe how performance will be monitored, reported, and reviewed regularly.

Maintenance Plan

Technology Availability:

- Explain how 100% technology availability will be ensured, including redundancy plans and backup systems.

Monitoring and Response:

- Detail the monitoring mechanisms (e.g., 24/7 control rooms, real-time alerts) and response protocols.

Response Times:

- Guarantee specific response times for different types of incidents (e.g., minor faults, major breaches).

Fault Resolution:

- Provide a clear turnaround time for resolving faults, including escalation procedures.

Installation Timeline

Installation Duration:

- Provide a realistic timeline for installing and commissioning the systems, including any site preparation required.

Phased Rollout:

- If applicable, outline a phased approach to installation to minimise disruption.

Mitigation Strategies

System Failures:

- Describe the contingency plans in place if the system fails, especially during critical times (e.g., middle of the night).

Redundancy Measures:

- Explain how backup systems or manual overrides will be implemented to ensure continuous security.

Failing Strategies:

- Outline how the bidder will identify, assess, and address strategies that are not delivering the expected outcomes.

Reduction of Guards

Transition to Full Automation:

- Provide a clear plan for reducing the number of physical guards as technology takes over, including timelines and criteria for reduction.

Retraining and Redeployment:

- Explain how affected guards will be retrained or redeployed, if applicable.

Investment in Technology

Commitment to Modern Technology:

- Confirm the bidder's willingness to invest in modern and advanced technologies.

Future Investments:

- Provide assurances that the bidder is prepared to make further investments if the current technology fails or becomes obsolete.

Additional Considerations

Stakeholder Engagement:

- Describe how the bidder will engage with Eskom and other stakeholders throughout the project lifecycle.

Risk Management:

- Provide a comprehensive risk management plan, including mitigation strategies for potential challenges.

Compliance and Standards:

- Ensure all proposed solutions comply with relevant industry standards and regulations.

Consequence Management:

- Eskom will implement strict consequence management for underperformance or breaches of contract.

The following Measures will apply:

Consequence Management Framework

Incidents Relating to Loss or Damage to Property

High-Impact Sites (Zero Tolerance):

- **First Breach:** Formal written warning, mandatory retraining, and recovery of losses by Eskom. The main supplier must ensure that corrective actions are taken by the service partner.
- **Second Breach:** Financial penalty (5% of annual contract value), independent audit, and recovery of losses. The main supplier must replace the non-performing service partner.
- **Third Breach:** Termination of contract and recovery of all losses.

Low-Impact Sites (≤ 2 minor Incidents/month):

- **First Breach:** Verbal warning, corrective action within 24 hours, and recovery of losses. The main supplier must ensure the service partner implements corrective actions.
- **Second Breach:** Written warning, additional training, and recovery of losses. The main supplier must review the service partner's performance.
- **Third Breach:** Financial penalty (5% of annual contract value), performance review, and recovery of losses. The main supplier must replace the non-performing service partner.

All Security Incidents are Detected, Recorded, and a Correct Response is Rendered.

High-Impact Sites (Zero Tolerance):

- **First Breach:** Formal written warning, mandatory retraining, and recovery of losses. The main supplier must ensure that corrective actions are taken by the service partner.
- **Second Breach:** Financial penalty (5% of annual contract value), independent review, and recovery of losses. The main supplier must replace the non-performing service partner.
- **Third Breach:** Termination of contract and recovery of all losses.

Low-impact sites (≥ 95% detection and response):

- **First Breach:** Verbal warning, corrective action within one hour, and recovery of losses. The main supplier must ensure the service partner implements corrective actions.
- **Second Breach:** Written warning, additional training, and recovery of losses. The main supplier must review the service partner's performance.
- **Third Breach:** Financial penalty (5% of annual contract value), performance review, and recovery of losses. The main supplier must replace the non-performing service partner.

Compliance with Regulatory and Legislative Requirements

- **First Breach:** Formal written warning, immediate corrective action, and recovery of losses. The main supplier must ensure the service partner complies.
- **Second Breach:** Financial penalty (5% annual of contract value), independent audit, and recovery of losses. The main supplier must replace the non-compliant service partner.
- **Third Breach:** Termination of contract and recovery of all losses.

Mandatory Technology Availability and equipment compliance

High-impact sites (99% availability, ≤ 2 hours downtime):

- **First Breach:** Formal written warning, immediate rectification, and recovery of losses. The main supplier must ensure the service partner rectifies the issue.

- **Second Breach:** Financial penalty (5% of annual contract value), independent review, and recovery of losses. The main supplier must replace the non-performing service partner.
- **Third Breach:** Termination of contract and recovery of all losses.

Low-impact sites (95% availability, ≤ six hours downtime):

- **First Breach:** Verbal warning, corrective action within six hours, and recovery of losses. The main supplier must ensure the service partner rectifies the issue.
- **Second Breach:** Written warning, additional training, and recovery of losses. The main supplier must review the service partner's performance.
- **Third Breach:** Financial penalty (5% of annual contract value), performance review, and recovery of losses. The main supplier must replace the non-performing service partner.

Customer Satisfaction

High-impact sites (≥ 95% satisfaction):

- **First Breach:** Formal written warning, improvement plan, and recovery of losses. The main supplier must ensure the service partner implements the plan.
- **Second Breach:** Financial penalty (5% of annual contract value), independent review, and recovery of losses. The main supplier must replace the non-performing service partner.
- **Third Breach:** Termination of contract and recovery of all losses.

Low-impact sites (≥ 85% satisfaction):

- **First Breach:** Verbal warning, improvement plan, and recovery of losses. The main supplier must ensure the service partner implements the plan.
- **Second Breach:** Written warning, additional training, and recovery of losses. The main supplier must review the service partner's performance.
- **Third Breach:** Financial penalty (5% of annual contract value), performance review, and recovery of losses. The main supplier must replace the non-performing service partner.

Performance Improvement Plans (PIPs):

- Persistent underperformance will require the service provider to submit a PIP within 14 days of notification.
- Failure to improve performance after the PIP may result in contract termination.

Recovery of Losses:

- Eskom reserves the right to recover **all direct and indirect losses** incurred due to the service provider's failure to meet contractual obligations.

This includes but is not limited to:

- Loss or damage to Eskom property.
- Costs associated with security breaches or incidents.
- Costs incurred due to system downtime or failures.

Mandatory Requirements

Bidders must comply with the following mandatory requirements. Failure to meet any of these requirements will result in disqualification.

Company Requirements

- **PSIRA Registration:** Valid PSIRA certificate in the name of the company or close corporation.
- **Letter of Good Standing:** Recent PSIRA letter of good standing (not older than six months).
- **COIDA Compliance:** Valid letter of good standing from the Compensation Fund (COIDA).
- **UIF Compliance:** Valid UIF registration certificate or proof of payment for the last six months.
- **Tax Compliance:** Valid tax clearance certificate.
- **Public Liability Insurance:** Proof of public liability insurance coverage of at least **R10 million**.

Personnel Requirements

- **PSIRA Registration:** All security personnel must be registered with PSIRA (minimum Grade C).
- **Training Certificates:** Proof of competency training for security personnel from accredited institutions.
- **Firearm Licenses:** Valid firearm licenses and competency certificates for armed guards.

Technical Requirements

- **Technology Integration:** Demonstrated capability to implement and maintain advanced security technologies (e.g., CCTV, access control systems, drones).
- **Control Room:** Established 24/7 control room with reinforced doors and walls, cameras, and electronic access control.

- **Vehicle Fleet:** Proof of ownership or leasing of at least three **(3) operational vehicles** less than two years old and with less than 50,000 km.

Experience Requirements

- **Company Experience:** Minimum of **five (5) years' experience** in providing physical guarding services and security systems installation and maintenance.
- **References:** Three (3) contactable references for similar services provided in the last 36 months.

Submission requirements

Bidders must submit the following as part of their proposals:

- **Executive Summary:** Overview of the proposal and key value propositions.
- **Detailed Approach:** Address all the points outlined above.
- **Appendices:** Include supporting documents, such as technical specifications, case studies, and references.

Gatekeepers

The following gatekeepers will be used to evaluate compliance with mandatory requirements:

Gatekeeper

Description: Compliance (Yes/No)

Compliance	Yes	No
Valid PSIRA certificate		
Valid PSIRA certificate for the directors (Min B grade)		
Recent PSIRA letter of good standing		
Valid COIDA letter of good standing		
Valid UIF registration or proof of payment		
Valid tax clearance certificate		
Public liability insurance (R10 million)		

PSIRA registration for all personnel (Grade C)		
Valid firearm licenses and competency certificates		
Proof of technology integration capability		
Proof of operational vehicle fleet (4 vehicles)		
Minimum 5 years' experience		
Three contactable references		

Appendix B: Technical Evaluation (RFI)

Technical Evaluation: To be used during the RFI (Request for Information) process

TECHNICAL EVALUATION CRITERIA FOR CLUSTER (Name) (REQUEST FOR INFORMATION).

Introduction

Eskom Holdings Limited invites qualified and experienced service providers to submit proposals for the provision of outcome-based physical guarding services at Eskom facilities in the (sector name). The tender aims to deliver a value proposition centred on an outcomes-based security model, leveraging advanced technology, innovation, and measurable performance metrics to enhance safety and protection. By focusing on achieving specific, predefined security outcomes such as risk reduction, incident prevention, and operational resilience, the model ensures a proactive and adaptive approach tailored to safeguarding Eskom's assets, personnel, and operations. This results-driven framework emphasises continuous improvement, accountability, and the integration of cutting-edge solutions to provide a comprehensive, future-ready security strategy that aligns with Eskom priorities and delivers tangible, long-term value. As part of the service delivery requirements, the service provider must include the construction of a new control centre or the refurbishment of the existing control centre in their proposal. The control centre will be responsible for monitoring all technology and operations, ensuring efficient service delivery and rapid response to any issues.

Technical Criteria

These are the technical evaluation criteria to be used for evaluating the tender submissions for the Request for Information process only. The detailed evaluation criteria will be included in the Request for Proposal process.

Description	Weighting (%)
Turnkey Solutions: **1. Physical Guarding:** • The bidder to propose physical guarding solution e.g., guard deployments, shift management, incident handling and escalations, emergency readiness and to propose backup plans. Deploy qualified guards with certificates of compliance from regulatory bodies. The guards should have bulletproof vests with body-worn cameras. **2. Technology Solutions:** • The bidder to propose turnkey solutions to implement security technology and systems solutions. The solution must be in line with the Eskom standards: • CCTV Surveillance: Compliance with Specification for CCTV Surveillance with Intruder Detection (240-91190304). • Access Control Systems: Compliance with Specification for Integrated Access Control System (IACS) for Eskom Sites (240-102220945). • Alarm Systems: Compliance with Specification for Integrated Security Alarm System for Protection of Eskom Installations and Its Subsidiaries (240-86738968). • Intrusion Detection Systems: Compliance with Standard for Intrusion Pre-Detection Systems used at Eskom Sites (240-170000691). • Fogging Units: • Body-worn cameras: **Note**: The above standards are not limitations to the proposals. The bidders can propose more solutions.	45
Monitoring and Response Time: • The bidder to clearly indicates how they respond to emergencies for defective systems and incidents on site. The proposal should indicate incidents response times. There should be a 24/7 monitoring site (Control Room) to monitor all sites.	15

Maintenance and Support: • The bidder to propose and demonstrate plans for preventative and corrective maintenance and support. The plan can include service and testing schedules, and process for fixing systems failures.	20
Cost Effectiveness: • The bidder to demonstrate return on investment to Eskom.	10
Capital Funding: • The bidder to demonstrate financial capabilities to roll out the proposed turnkey solutions. Proposal to outline funding sources, e.g., internal funding, partnerships, private investments, etc.	10
TOTAL CLAIMABLE POINTS	**100**

Appendix C: Technical Evaluation (RFI) Process

Technical Evaluation: To be used during RFI (Request for Information)

Technical Requirements

Bidders must demonstrate compliance with the following technical requirements:

Alarm Systems

- Compliance with Eskom's Specification for Integrated Security Alarm System (240-86738968).
- Integration with motion detection systems and backup power supply.

CCTV Cameras

- Compliance with Eskom's Specification for CCTV Surveillance with Intruder Detection (240-91190304).
- High-resolution cameras (minimum 4MP) with night vision and AI-based analytics.

Access Control Systems

- Compliance with Eskom's Specification for Integrated Access Control System (240-102220945).
- Biometric scanners and integration with license plate recognition (LPR) cameras.

Intrusion Detection Systems

- Compliance with Eskom's Standard for Intrusion Pre-Detection Systems (240-170000691).
- Motion sensors, thermal imaging, and perimeter detection systems.

Public Address Systems

- Compliance with Eskom's Security Public Address Systems for Substations (240-170000098).
- Clear and audible announcements for emergency notifications.

Physical Security Integrated

- Compliance with Eskom's Physical Security Integrated standard (240-170000096).

Mandatory Criteria Evaluation

Item	Criteria	Comply	Comments
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, Annex A (related to technical specification 240-91190304) (Written in English)		
1.3	IACS System: Submission of Technical Schedules A/B from this standard, 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 Detection System: Submission of Technical Schedules A/B from the Technical specification 240-240-170000691 (Written in English)		
1.6	System Integration: Submission of Technical Schedules A/B from the Technical specification 240-170000096 (Written in English)		
1.7	Compliance with the Eskom bodycam standard		
1.8	Submission of reference letters from previous clients and a CV indicating Engineer/Technician experience related to security (minimum experience of five years)		
1.9	Proof of certificate indicating the supplier is OEM accredited		
1.10	Project plan (Bidder must provide a comprehensive implementation plan, on how the work, implementation and commissioning will be carried out)		
1.10	Submission of the PSIRA registration certificate		
1.12	CIPC Registration Documents		
1.13	Valid Tax Clearance Certificate/Tax Pin		
1.13	Valid CSD report (Not older than three (3) months)		
1.15	CIDB Rating: 1GB, 2EB or 1EP		
1.16	ECB/SAIEE/ECSA Registration: Proof of valid Registration Electrical/Electronic Engineer/Technologist/Technician		
1.17	Valid Letter of Good Standing issued by the Department of Labour or RMA.		
	Threshold	**Compliance with all of the above**	

Desktop Evaluation Criteria

	Technical Criteria Description	Criteria Weighting (%)	Criteria Sub-Weighting (%)
1.	Alarm System	**15**	
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	**20**	
2.1	Compliance with Technical Schedules A/B from this standard, Annex A (related to technical specification 240-91190304). (Full compliance = 402 x 3 = 1206 points (i.e., 100%)).		100
3	IACS	**15**	
3.1	Compliance with Technical Schedules A/B from this standard, Annex B (related to technical specification 240-102220945). (Full compliance = 335 x 3 = 1005 points (i.e., 100%)).		100
4.	PA System	**10**	
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	System Integration	**20**	
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	Supplier Services and organisation experience (minimum of five years)	**5**	
6.1	Submission of reference letters from previous clients and a CV indicating engineer/technician experience		100
7	System Design Report The tenderer is required to produce and submit a System Design Report covering at a minimum the following:	**15**	
7.1	Overview of the overall design and detailing of each of the different components (sub-systems)		15
7.2	System architecture (logical and physical designs), including the integration of the different components (sub-systems).		35
7.3	A cause-and-Effect matrix of the overall system is to be provided.		10
7.4	Schematics displaying the location of each component's (subsystems) sensor (e.g., CCTV, alarm contacts, etc.)		20
7.5	Equipment list of all the different components (sub-systems)		10
7.6	Equipment data sheets		10
	TOTAL:	**100**	

Overall Qualitative Evaluation Criteria

Item	Criteria	Weight (%)	Score obtained (%)	Comment
1.	Mandatory evaluation	20		
2.	Desktop evaluation	80		
	Total	**100**		
	Threshold	**70**		

Evaluation Process

The evaluation process will consist of two parts:

Desktop Evaluation

Mandatory Requirements: Compliance with gatekeepers.

Technical Proposal: Evaluation of the bidder's approach, methodology, and technology integration.

Cost Proposal: Assessment of the cost breakdown and pricing structure.

Appendix D – NEC 3 Terms of Contract

NEC 3 Terms of Contract

Service Information

The **Service Information** section should include the detailed scope of work, performance metrics, and other requirements. This section will form the basis of the contractor's obligations.

Service Information Content:

- **Scope of Work:** Include the entire **Scope of Work** provided (physical guarding, technology integration, innovation, performance metrics, etc.).
- **Service Delivery Points:** Specify the locations (Eskom facilities) where services will be delivered.
- **Service Levels:** Define the expected service levels, including response times, uptime, and other performance metrics.
- **Technology and Data Ownership:** Clearly state that all installed technology and data will belong to Eskom upon contract expiry or termination.
- **Payment Structure:** Include the pricing structure, cost breakdown, and payment terms aligned with the outcomes-based model.
- **Incident Reporting and Management:** Detail the requirements for real-time incident reporting, investigation reports, and root cause analysis.
- **Compliance Requirements:** List all compliance documentation required (e.g., PSIRA accreditation, tax clearance certificates).

Option C: Target Contract

Option C is a cost-reimbursable contract with a target cost. This is suitable for outcomes-based contracts where the final cost may vary based on performance.

Key Elements:

- **Target Cost:** Define the target cost based on the cost breakdown provided in the Scope of Work.
- **Pain/Gain Share Mechanism:** Specify the pain/gain share percentage (e.g., 50/50) to incentivise the contractor to meet or exceed the target cost.
- **Price List:** Include a detailed price list for physical guarding, technology integration, and other services.
- **Adjustments to Target Cost:** Define how the target cost will be adjusted for changes in scope or performance.

Core Clauses

The **Core Clauses** of the NEC3 TSC will govern the general terms and conditions of the contract.

Key Clauses:

- **Clause 10.1:** Obligation to act in a spirit of mutual trust and cooperation.
- **Clause 20.1:** Contractor's responsibility to provide the services in accordance with the Scope of Work.
- **Clause 30.1:** Requirements for the contractor to submit a program for delivering the services.
- **Clause 31.2:** Procedures for notifying and managing compensation events.
- **Clause 40.1:** Requirements for defect management and correction.

Defect W1

- The **Defect W1** option is used for contracts where the employer (Eskom) will notify the contractor of defects.

Key Elements:

- **Defect Notification:** Eskom will notify the contractor of any defects in the services provided.
- **Defect Correction:** The contractor must correct defects within a specified timeframe.
- **Defect Costs:** Costs associated with defect correction will be borne by the contractor unless otherwise agreed.

Secondary Options

Include the following secondary options to address specific requirements:

X12: Partnering

- **Objective:** Promote collaboration between Eskom and the contractor to achieve the contract objectives.

Key Elements:

- Joint performance monitoring and problem-solving.
- Regular partnering workshops to review progress and address issues.
- Shared risk and reward mechanisms.

X13: Performance Bond

- **Objective:** Provide financial security for Eskom in case of contractor default.

Key Elements:

- The contractor must provide a performance bond (e.g., 10% of the contract value).
- The bond will be valid for the duration of the contract.

X17: Low Performance Damages

- **Objective:** Impose financial penalties for underperformance.

Key Elements:

- Define low performance damages for failure to meet KPIs (e.g., response time, incident detection rate).
- Specify the calculation method for damages.

X20: Key Performance Indicators (KPIs)

- **Objective:** Measure and incentivise contractor performance.

Key elements:

- Define KPIs (e.g., incident detection rate, response time, false alarm rate).
- Include a **Service Level Table** with target values and measurement methods.
- Link KPIs to payment mechanisms (e.g., bonuses for exceeding targets, penalties for underperformance).

Service Level Table

- Include a **Service Level Table** in the contract to define KPIs and performance targets.

Assets belonging to Eskom

Under **X12: Partnering** or as a separate clause, specify that all technology and data installed or collected during the contract will belong to Eskom.

Key elements:

- **Ownership of installed technology:** All technology (e.g., CCTV cameras, access control systems) will become Eskom's property upon contract expiry or termination.
- **Data ownership:** All data collected (e.g., surveillance footage, access logs) will belong to Eskom.

- **Data handover:** The contractor must provide all data in a usable format upon contract expiry or termination.

Payment mechanism

Align the payment mechanism with the outcomes-based model.

Key elements:

- **Monthly payments:** Payments will be made based on the achievement of KPIs.
- **Performance-based adjustments:** Adjust payments based on the contractor's performance (e.g., bonuses for exceeding targets, penalties for underperformance).
- **Cost reimbursement:** Reimburse the contractor for actual costs incurred, subject to the target cost and pain/gain share mechanism.

Appendix E – OBC Step-by-Step Guide

Below is a guide on step by step on how Eskom can approach the OBC

Request for Information (RFI)

The **RFI** is the first stage of the procurement process. It is used to invite service providers to submit detailed proposals on how they will deliver the required outcomes-based security services.

Key steps for issuing an RFI:

Define the Scope of Work:

Clearly outline the Scope of Work, including physical guarding, technology integration, innovation, and performance metrics (as provided in your document).

Specify the outcomes-based model and the key performance indicators (KPIs) that will be used to measure success.

Develop Evaluation Criteria:

Define the criteria for evaluating proposals (e.g., compliance with Eskom standards, innovation, cost-effectiveness, experience, and qualifications).

Assign weightings to each criterion to ensure a transparent and objective evaluation process.

Prepare the RFI document:

Include the following sections in the RFI:

- Background and objectives.
- Scope of work.
- Outcomes-based performance metrics.
- Submission requirements (e.g., detailed proposal, references, compliance documentation).
- Evaluation criteria and weightings.
- Terms and conditions (e.g., contract duration, payment structure, penalties for underperformance).

Advertise the RFI:

Receive and evaluate proposals:

- Allow sufficient time for bidders to prepare and submit their proposals.
- Evaluate proposals based on the predefined criteria and weightings.

- Shortlist the top bidders who meet the requirements and demonstrate the ability to deliver the desired outcomes.

Request for Proposal (RFP)

The **RFP** is the second stage of the procurement process. It is issued to the shortlisted bidders from the RFI stage to obtain detailed pricing and finalise the contract terms.

Key steps for issuing an RFP:

Prepare the RFP document:

Include the following sections in the RFP:

- Detailed Scope of Work (based on the RFI).
- Pricing structure and payment terms.
- Bill of Quantities (BOQ) for cost breakdown.
- Contract terms and conditions (e.g., performance bond, penalties for underperformance).
- Submission requirements (e.g., final cost breakdown, compliance documentation).

Issue the RFP to the Shortlisted Bidders:

- Send the RFP only to the bidders who were shortlisted during the RFI stage.
- Provide a clear deadline for submission and ensure all bidders have access to the necessary information

.

Evaluate Quotations:

- Evaluate the quotations based on cost-effectiveness, alignment with the outcomes-based model, and compliance with the RFP requirements.
- Conduct a cost-benefit analysis to ensure value for money.

Negotiate and Finalise the Contract:

- Negotiate with the preferred bidder to finalise the contract terms, including the target cost, pain/gain share mechanism, and performance metrics.
- Ensure all legal and compliance requirements are met before signing the contract.

Key Considerations

- **Transparency and Fairness:** Ensure the procurement process is transparent, fair, and compliant with Eskom's procurement policies and relevant legislation (e.g., Public Finance Management Act).
- **Stakeholder Engagement:** Engage key stakeholders (e.g., Eskom's security team, legal team, finance team) throughout the process to ensure alignment and buy-in.

- **Risk Management:** Identify and mitigate risks associated with the outcomes-based model, such as underperformance or cost overruns.
- **Continuous improvement:** Include provisions for continuous improvement and innovation in the contract to ensure the services evolve.

Example Timeline

Below is an example timeline for the RFI and RFP process:

Stage	Activity	Timeline
RFI Preparation	Develop an RFI document	2 weeks
RFI Advertisement	Publish RFI on procurement portals	1 week
Pre-Bid Meeting	Conduct a pre-bid meeting	1 week after RFP
RFI Submission	Receive proposals from bidders	4 weeks
RFI Evaluation	Evaluate proposals and shortlist bidders	3 weeks
RFP Preparation	Develop an RFP document	1 week
RFP Issuance	Issue RFP to shortlisted bidders	1 week
RFP Submission	Receive quotations from bidders	2 weeks
RFP Evaluation	Evaluate quotations and select a bidder	2 weeks
Contract Finalisation	Negotiate and sign a contract	2 weeks