NKANGALA DISTRICT MUNICIPALITY

PROJECT NO: 185571

ESTABLISHMENT OF AN ENTERPRISE-WIDE SECURITY OPERATIONS CENTRE (SOC) AS A MANAGED SERVICE FOR NKANGALA DISTRICT MUNICIPALITY FOR A PERIOD OF THREE (03) YEARS

SCOPE OF WORK

Terms of Reference (TOR): Technical Specification: Physical Security Information Management (PSIM) / Physical Security Operations Centre (PSOC) as a Managed Security Services (MSS) offering.

1. Purpose and Background

1.1. Purpose

The purpose of this RFB is to invite Suppliers (hereinafter referred to as "SITA_ACCREDITED bidders on contract RFA1183") to submit bids for the provisioning of a Managed Security Services Provider (MSSP) – ICT Cybersecurity for both network and physical infrastructure. This initiative is driven by the organization's holistic view and commitment to fortify its security posture in response to emerging network cyber threats, compliance, and physical security (i.e., Applications stack, Networking, Data Centre, End User Computing Devices, CCTV etc.) as well as incident management.

1.2. Background

Over the years, NDM has invested extensively in building standard processes and infrastructure designed to support and secure the efficient operation of its ICT Security including the Local Municipalities. This growing reliance on digital technology, alongside the expansion of service offerings, business processes, transactions, and regulatory demands, has heightened the potential risks related to service disruptions. Unforeseen incidents, ranging from natural disasters and hardware failures to cybersecurity breaches, can significantly impact business continuity, potentially preventing the organization from maintaining its standard service operations.

In response to these risks, NDM has established a Business Continuity Management (BCM) framework aligned with globally recognized standards, including ISO 22301, Business Continuity Institute Good Practice Guidelines, ISO 31000, and King IV. The BCM framework incorporates a comprehensive approach, covering emergency response, crisis management, business recovery, and disaster recovery.

A critical pillar of this framework is IT Disaster Recovery (DR), which focuses on safeguarding ICT Security within the ICT Infrastructure. In line with the BCM framework, ICT is tasked with developing and implementing robust recovery strategies to ensure that IT services, systems, infrastructure, hardware, and software are recoverable within the organization's specified Recovery Time Objective (RTO) and Recovery Point Objective (RPO). This involves implementing Security Operational Centre (SOC) for the Primary ICT Infrastructure and the Disaster Recovery site inclusive of the Local Municipalities within the region.

2. Objectives

The objectives of this RFB are outlined as follows:

- To appoint SITA contract 1183 accredited service provider for the provisioning of Managed ICT Security Services (MSS) for a period of three years.

- The MSSP (Managed Security Service Provider) must be accredited and qualified on SITA 1183 to provide ICN Codes as described and listed in this requirement. Failure for the service provider to comply to the ICN codes as prescribed by SITA will lead to automatic disqualification.
- The required services shall include support and maintenance of the MSS (Managed Security Services)/ PSIM (Physical Security Infrastructure Management)/ PSOC (Physical Security Operational Centre) infrastructure hosted in South Africa for the duration of the contract period.
- The MSSP must at least be accredited on SITA1183 contract with a footprint in Mpumalanga.
- Appoint a resourced MSS with proven expertise to deliver comprehensive managed security services aligned with industry standards and regulatory frameworks.
- The MSS must have intensive application, networking and physical security knowledge, skills and expertise.
- Appoint MSS with an existing, well-established Security and capacitated Operation Centre (PSOC / PSIM) within border of South Africa.
- Enhance the organization's security posture through robust security monitoring, proactive threat detection, incident response, and vulnerability management.
- Ensure compliance with relevant regulatory standards and industry best practices, including ISO27001, PCI DSS, POPI, and other applicable regulations.

3. Scope of Work

- The Scope of work for this RFB entails the appointment of SITA RFA1183 accredited services provider and the provision of Managed Security Services (MSS) - ICT Cybersecurity for both network and physical infrastructure for the period of three years. In order for the service provider to implement and manage a resilient PSOC /PSIM infrastructure or environment as an MSS, it is important that a Service Provider has an intensive understanding of the end to end ICT technologies, applications stack , networking and physical security environment. Below is the diagram illustrating the organization requirements and scope of work.
- The MSSP must be accredited and qualified on SITA 1183 to provide ICN Codes as described and listed herein:

List of Required ICN Codes:

ICT Management Services

- Technical Management Services: ICN no. 81112011-0001
- Programme Management Services: ICN no. 81112011-0004
- ICT Management - Project Administration Support: ICN no. 81112011-0006
- ICT Governance and Compliance Services: ICN no. 81112011-0007
- Quality Management Services: ICN no. 81112011-0009

Business Planning and Development

- ICT Strategic Consulting: ICN no. 81112011-0010
- Business Analysis Services: ICN no. 81112011-0011
- Business Process Architecture Services: ICN no. 81112011-0012
- Information Systems Architecture Services: ICN no. 81112011-0013
- Information Architecture Services: ICN no. 81112011-0014
- Information Technology Architecture Services: ICN no. 81112011-0015
- Business Modelling Services: ICN no. 81112011-0016
- Enterprise Architecture Services: ICN no. 81112011-0017

Business Solutions Delivery Services

- Systems Analysis and Design Services: ICN no. 81112011-0018
- Business Solution Development: ICN no. 81112011-0019
- Business Solution Certification/Accreditation: ICN no. 81112011-0020
- Business Solution Maintenance: ICN no. 81112011-0021
- Specialised Business Intelligence Services: ICN no. 81112011-0022
- Specialised Geographic Information Management Services: ICN no. 81112011-0023

Information Security Services

- Security Architecture Services: ICN no. 81112011-0029
- Business Continuity Consultancy Services: ICN no. 81112011-0030
- Policy Development and Implementation Services: ICN no. 81112011-0031
- Specialised Access Control Services: ICN no. 81112011-0032
- Specialised Identity Management: ICN no. 81112011-0033
- Specialised Physical and Environmental Security: ICN no. 81112011-0034
- Specialised Communication and Operations Security: ICN no. 81112011-0035
- Specialised Application Security Services: ICN no. 81112011-0036
- Business Solution Compliancy Services: ICN no. 81112011-0037

Business Solution Implementation services

- Application/ICT/COTS Training: ICN no. 81112011-0038
- Organisational Change Management Services: ICN no. 81112011-0040
- Functional Application Support/COTS/ICT Services: ICN no. 81112011-0042

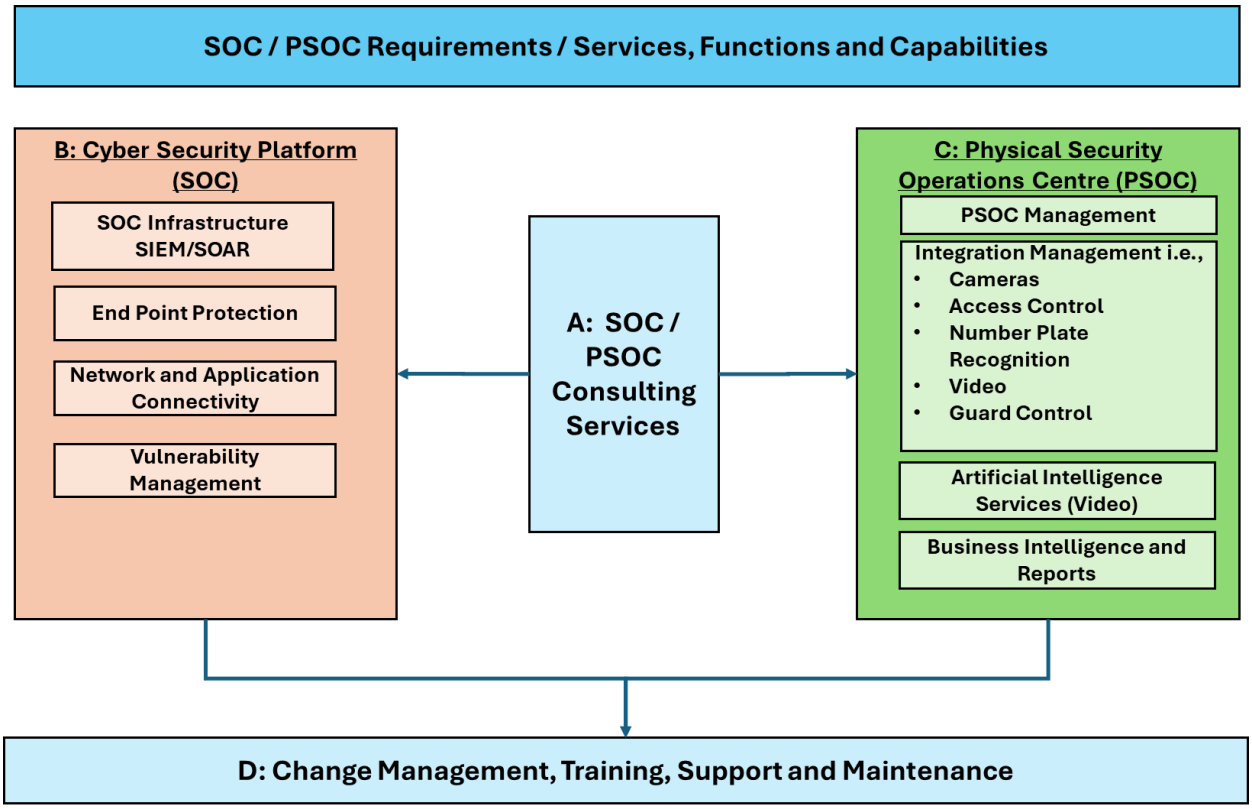
ICT Service Support Management

- Service Management Centre Services (Service Desk): ICN no. 81112011-0047

Planning and Organisation

- Architecture and Governance Services: ICN no. 81112011-0069
- Functional Application Support Services: ICN no. 81112011-0070

3.1. High Level Scope of Work (SOW)



3.2. Scope of Work Deliverables

3.2.1. Phase A: PSOC / PSIM Consulting Services

1) List of deliverables and documents
   a) Project Charter / Project Initiation Document (PID)
   b) Implementation Plan
   c) Requirements Verification and Confirmation
   d) High level To-Be Business scenario
   e) GAP Analysis
   f) Business Architecture
   g) Data and Systems Architecture
   h) Technology Architecture
   i) Solution Architecture
   j) Integration Architecture and GAP Analysis: Integration costing from systems into the PSOC / PSIM are excluded and will be priced separately as a variation order to the contract.
   k) Migration and Implementation Plans
   l) Architecture Change Management

3.2.2. Phase B: Cyber Security Platform (PSOC / PSIM)

1) List of deliverables and documents
   a) As-Is Audit and Assessment of Cyber Security environment
   b) Perform Cyber Security Penetration testing if required
   c) Establish an internal and External Vulnerability Management Capability
   d) Create and establish a POC environment
   e) Create and establish a testing environment
   f) Training of staff

g) Manage Vulnerabilities to GREEN
h) Create and establish a production environment
i) Setup and configuration of production environment
j) Compile and agree om migration plan
k) Migration = Go Live Phase
l) As-Build document and Handover

3.2.3. Phase C: Physical Security Operations Centre (PSOC / PSIM)

2) List of deliverables and documents

a) As-Is Audit and Assessment of Physical and Cyber Security environment
b) Perform Cyber Security Penetration testing if required
c) Create and establish a POC environment
d) Create and establish a testing environment
e) Training of staff
f) Create and establish a production environment
g) Setup and configuration of production environment
h) Compile and agree om migration plan
i) Migration = Go Live Phase
j) As-Build document and Handover

3.2.4. Phase D: Change Management, Training, Support and Maintenance

3) List of deliverables and documents

a) Training of staff as per Phase B and C above
b) Compile a Change Management Plan with roles and responsibilities
c) Provide Support and Maintenance as per Phase B and C above.

4. Mandatory Requirements: Non-Technical

Table 1: Non-Technical Mandatory Requirements

No	Requirement description	Evidence / Comments
1	The bidder must have an existing or establish a Physical Cyber Security Platform (PSOC / PSIM) SAAS and IAAS) after the appointment with staffing capacity, Support and Call logging process – Help Desk	Evidence **NOT APPLICABLE** for now, however the Client reserve the rights to physically audit the premises of the Bidder after appointment.

5. Technical and Functional Requirements

5.1. SOC: Platform Technology and Functionality

Table 2: Platform Technology and Functionality: The MSS shall provide the following technology and functionalities.

No	REQUIREMENTS & DESCRIPTION

1.	The bidder must deploy and manage a robust Security Information and Event Management (SIEM) system as Software as a Service (SAAS) and Infrastructure as a Service (IAAS)
2.	SIEM shall offer User and Entity Behavior Analytics (UEBA)
3.	Implementation of Security Orchestration, Automation, and Response (SOAR) capabilities for efficient incident handling and enrichment
4.	SOAR should be SIEM vendor agnostic
5.	Comprehensive vulnerability management software and services, including vulnerability identification and have the capability to remediate directly out of Platform
6.	SIEM and Security Orchestration, Automation, and Response (SOAR) must provide integration with all the clients technical controls and critical assets.
7.	SIEM should correlate data from multiple sources.
8.	SIEM and SOAR should offer AI (Artificial Intelligence (AI or MI) capabilities and should be able to detect 0-day attacks.
9.	Licensing cost for all technologies offered must be included i.e., large storage/EPS size on disk.
10.	Minimum of 3 Month Warm Storage to be included in the solution
11.	The platform must integrate into a Ticketing system
12	The Platform must be ingest from Internet of Things (IOT) devices
13	Open source and commercial threat intelligence feeds and threat intelligence sharing.
14	MSS SOC must offer an Extended Detection and Response (XDR) solution which will collect network telemetry and end point data
15	MSS must provide a vulnerability management (VM) service. The VM service should preferably be part of the SIEM capabilities

5.2. Security Operations Centre (SOC) Services

Table 3: General SOC services requirements

No	REQUIREMENTS & DESCRIPTION
1.	Continuous monitoring and management of security events. Services must be 24x7x365.
2.	Proactive detection of threats and rapid incident response. First Expert Verdict of 15 minutes, Remediation and containment plan delivery within two hours
3.	In-depth analysis and investigation of security incidents and automated correlation and enrichment
4.	Escalation and resolution of security incidents as per predefined protocols.
5.	Timely reporting and documentation of security incidents.
6.	The incumbent must offer continues threat hunting capability, both IOC and hypothesis-based threat hunts.
7.	Prioritisation and categorisation must align with the client's prioritisation and categorisation scheme.
8.	Incident response processes should integrate with the client's incident response process.
9.	Incident response should be offered on-prem and virtual for priority 1 and priority 2 incidents.
10.	MSS SOC must be local with no information leaving South Africa's borders.

5.3. Physical Security Operations Centre (PSOC / PSIM)

Table 4: PSOC / PSIM - Physical Security Operations Centre requirements

No	REQUIREMENTS & DESCRIPTION
1	The solution system must be an open-architecture integrated PSOC engine with an API/SDK that allows the integration of IOT such as, CCTV, intrusion alarm, access control, fire alarm, PA, perimeter, radars, drones, IP Telephony, radio communications, building controllers, cyber systems. Includes a sophisticated rule engine and sensor management for defining workflows and automation.
2	The Physical Security Operations Centre (PSOC / PSIM) shall support Multi tendency organizational hierarchy – defining localized environments based on multi-tenancy architecture. These are local command and response centers which are partitioned on the same server and database. The local command centers have their own environment and access to their local GIS, integrations and sensors, incidents, staff, permissions, etc. The top organization can define the vertical and horizontal command structure and the top command can intervene and receive access to the information to the lower command centers beneath him.
3	The PSOC / PSIM must integrate with multiple vendor and product VMS (must be vendor and product agnostic).
4	The PSOC / PSIM must support video management for integrating VMS's and displaying cameras, including displaying the cameras straight from the GIS, through the video bar and through a dedicated video matrix. (Support Artificial Intelligence - AI)
5	The PSOC / PSIM Video streaming server must support remote cameras to be connected with the PSOC through a multi-cast video streaming engine and allows to view the live stream of these cameras on any remote user.
6	The PSOC / PSIM solution must special real time integrations i.e., radars, day/night cameras for continuous tracking, drone integration and dispatch, video analytics, face recognition and license plate recognition.
7	The PSOC / PSIM solution must be able to gather info from i.e., camera's, fire sensors, power telemetry, perimeter fences, communication devices like radio's, intrusion alarm sensors, access control readers, gates and barriers, water sensors, IT and Network devices, vehicle trackers, human sensors etc.
8	The PSOC / PSIM must have a Logical layer – data processing, automation, workflows, prioritization, and escalation: The Physical Security Operations Centre (PSOC / PSIM) solution must have an have has an advanced rule engine and automated actions module for defining business logic layer, rule configuration, workflow management and decision trees. Defining conditions and results in Boolean terms (if-and/or-then)
9	The PSOC / PSIM must have a sensor management and rule engine with automated actions – monitoring of sensors data, plotting of sensors on GIS or 2d map, controlling sensors via commands, creating simple or complex scenarios and defining automated operations via the rule engine and orchestrating the events arriving from the integration server.
10	The PSOC / PSIM must have a GIS engine – for managing dynamic layers of geo-referenced data, real time tracking and data display, management and activation of devices straight from the map, display of vector and aerial images, virtual fences, etc. 2D and 3D facility layout and floor plans - display of all building plans and blue-prints, floor plans, location of sensors and devices, etc. Including support of 3D dynamic display of external and internal building with sensors
11	The PSOC / PSIM must have an incident management system - for automatic incident reporting that allows data correlation, fusion, and analysis, with incident templates, triage tree and escalations, managing incidents.
12	The PSOC / PSIM must have a CAD (Computer Aided Dispatch) for call taking, receiving caller location and details, and dispatching the closest responder to the incident location. Allows defining hierarchy and linking responders to different territories, managing job titles, response per incident type, etc.

13	The PSOC / PSIM must have a SOP functionality build-in (Standard Operation Procedure) - event protocol, workflow, procedure management & business continuity. Allowing to automate processes and to deploy automated commands to the integrated sub-systems.
14	The PSOC / PSIM must have a mobile application work terminal for – emergency response, incident management, video camera view, PTT over IP, GIS layers, tracking, tasking, messaging, security tools, stream phone camera, etc. It must supports IOS and Android phones and tablets.
15	The PSOC / PSIM must have a Business Intelligence (BI) system - allowing it to receive dynamic data reports from all the system's accumulated data, including real time analysis, trends, predictions. Drill in from the top statistics down all the way down to the actual records.
16	The PSOC / PSIM must have an Activity Calendar to create and manage daily routines and pre-scheduled events. Integrated into the incident management module to allow seamless workflow of event data to incidents.

5.4. Reporting and Documentation

Table 5: Reporting and Documentation Requirements.

No	REQUIREMENTS & DESCRIPTION
1.	The MSS must furnish regular reports detailing security events, incidents, and vulnerabilities, along with actionable recommendations for remediation and improvement. Documentation of security incidents and responses is crucial for audit and compliance purposes.
2.	The MSS should provide a monthly report with technical and management information. The report should provide strategic and operational guidance as well as trending. The report should contain elements of machine generated reports as well as in-depth analysis and interpretation by SOC / PSOC / PSIM