



ELECTRICIDADE
DE MOÇAMBIQUE, E.P.

TERMS OF REFERENCE

FOR

AN INDIVIDUAL CONSULTANT

On

**Preparation of Technical Specifications, Procurement and
Supervision on the Implementation of Information Security
(InfoSec) Project**

under

**POWER EFFICIENCY AND RELIABILITY IMPROVEMENT
PROJECT (PERIP)**

June 2020

TORs on Preparation of Technical Specifications, Procurement and Supervision on the Implementation of Information Security (InfoSec) Project

1. PURPOSE

The purpose of this Terms of Reference (ToRs) is to outline the requirements for an individual consultant to supervise the Tendering process for the Implementation of Information Security (InfoSec) Project, which include preparation of Technical Specifications, Execution of the end-to-end Procurement Process and Supervision of Project Implementation.

2. BACKGROUND

2.1. EDM'S Information and Communication Technology Infrastructure Improvement and redesign

EDM is a company with approximately 4,000 workers and more than 150 agencies (shops) to provide service to the 2.1 million consumers. The management of this business increasingly requires good metrics and tools, to allow for analysis-based decision making and proper planning for sustainable growth. In other words, EDM is evolving to adopt the modern practices associated with concepts such as smart grid, big data and the internet of things, while preserving the effectiveness and quality of operations of the power infrastructures.

EDM's Information and Communication Technology (ICT) Infrastructure improvement and Redesign Project, which is managed by ICT Directorate of EDM is structured in multiple pillars and phases at various stages of implementation.

The majority of EDM ICT applications are hosted on-premises in two geographical dispersed datacenters facilities within Maputo, the two Datacenters are interconnected by fiber, and some limited numbers of applications are hosted in the Microsoft Azure cloud.

2.2. EDM ongoing IT activities under PERIP

ICT plays a strategic role in the transformation process of EDM. To this end, EDM is pursuing various IT activities under PERIP to fast-track the implementation of its digital transformation strategy, those activities revolve around EDM IT aspects below including but not limited to

1. IT Infrastructure Upgrade
2. IT Applications Development
3. IT Strategy & InfoSec

2.2.1 IT infrastructure upgrade

EDM is currently running two major IT infrastructure upgrade projects under PERIP; these projects are:

- Network upgrade project scheduled into two phases i.e., Network Upgrade Phase 1 and Network Upgrade Phase 2
- Data Center upgrade project which includes Datacenter facility build and Datacenter IT (compute, storage) upgrade

Network upgrade project Phase 1 and Phase 2: This phased project aims to modernize EDM corporate data communication system by replacing the current end of life network systems and introducing a digital network system built with automation features to increase network performance and availability.

Data Center upgrade project: This project aims to provide EDM with redundant fit-for-purpose Data Center facilities furnished with Data Center IT systems to meet EDM compute, storage, and network to enable on-premises hosting of EDM IT services and applications.

2.2.2 IT Applications Development

EDM is currently preparing the specifications for two IT application developments to be acquired under PERIP; these applications are:

- Corporate Information and Services Portal
- Enterprise Application Integration (EAI) - Enterprise Service Bus

Corporate Information and Services Portal: The corporate portal will function as a gateway to widespread corporate IT applications such as access to e-learning services, leave application system, fleet management, etc. and a tool to promote corporate information dissemination and provisioning of more incisive IT-based services.

Enterprise Application Integration (EAI) - Enterprise Service Bus: The objective of Enterprise Application integration is to facilitate the integration of multiple IT application components through a custom-fit integration architecture Enterprise Service Bus (ESB), in order to eliminate silos and enables different EDM application software programs such as CMS, MDM, BPMS, 3E, GIAF, OMS to communicate with each other - these applications must be able to integrate with each other in ESB structure, to avoid quality inefficiencies, duplications, data silos.

2.2.3 IT Strategy & InfoSec

EDM is currently preparing the specifications for Enterprise Architecture, and Infosec Baseline Security to be initiated under PERIP

- Enterprise Architecture (EA)
- InfoSec Baseline Assessment

Enterprise Architecture (EA): The objective of EA in the context of the ongoing program is to produce an as-is business capability map which would depict existing EDM business processes mapped to their IT applications/Technologies counterpart and to develop a framework for EA practice at EDM to govern technologies adoption and integration in order to deliver value to Business and value to IT.

InfoSec Baseline Assessment: The InfoSec Baseline Assessment aims at identifying vulnerabilities in EDM information technology (IT) infrastructure; supporting EDM in the development of a cybersecurity plan and strategy; assisting EDM in the framing of Cybersecurity policies and establishing a structured cybersecurity improvements implementation roadmap.

2.3. InfoSec Baseline Assessment

The Implementation of Information Security (InfoSec) Project is a top priority for EDM and seeks to ensure the safety of critical ICT infrastructure. Accordingly, EDM is taking steps to enhance its critical ICT infrastructure cybersecurity posture. This initiative aims at significantly improving the security and resiliency of EDM Critical ICT Infrastructure by closely engaging with a range of key stakeholders within EDM and its ecosystem as categorized below:

- Data Owners: Senior management or the heads of departments that have IT Systems;
- Policies and Procedures: Strategy and Programs Division
- Systems Owners: The systems administrators
- Internal Users of the Systems

- External partners interfacing with EDM systems or managing systems

The following are some of the critical ICT infrastructure:

1. Credelec - EDM's power Prepayment System
2. MDM (Meter Data Management) - Automatic Meter Reading system at large customers
3. Enterprise Resource Planning (ERP) system - Covering the operational procedures for all corporate activities including accounting and finance, Human Resources, staff health & welfare, general administration, purchases and contracting (procurement), logistics (management warehouses), asset management, corporate planning, and regulatory affairs (economic and service quality regulation).
4. Commercial Management System (CMS): Covering the review and restructuring of a new commercial management process flow and systems management. This central area is critical to EDM operations because it is the main interface with customers and clients and it is responsible for billing, collection and accurate recording of EDM electricity sales.
5. Outage Management System (OMS): to enable EDM to better respond to client contingencies by automating the detection of distribution faults and ensuring the quality of power supply.
6. Corporate Email System.
7. Network infrastructure
8. Unified Communications Infrastructure

The cybersecurity Baseline Assessment has been identified as a first step to establish the current state of EDM cybersecurity posture of EDM's ICT infrastructure. The outcome of this assessment will serve as a basis to develop a plan and prioritize a set of activities, policies and procedures to mitigate the exposures identified.

To this end, EDM has decided to recruit an individual consultant to fulfill the advisory role of the Consultant to design the Technical Specifications to address the InfoSec needs of the company, to co-ordinate the Tender Process together with the EDM team, including selection of Consultancy firm to execute the Implementation of the program, as well as supervise the Implementation and stabilization of the Information Security Solution together with a designated EDM Team.

3. SCOPE AND OBJECTIVES

The purpose of engaging an individual consultant is to advise ICT Director to manage complex, multi-disciplinary ICT infrastructure programs and umbrella projects. Plan requirements with internal EDM teams, external consultants and contractors to guide projects through the entire project lifecycle.

The consultant will directly report to the ICT director and work with EDM ICT teams and other consultants to keep all the players coordinated on the project's progress and deadlines to ensure projects across all ICT infrastructure verticals are delivered on time and within budget.

4. TASKS

The specific tasks of the consultancy services are the following:

4.1. General Expectation

The tasks to be undertaken by the consultant to be hired have been outlined in three stages, namely:

- Pre-implementation stage;
- Implementation stage; and
- post-implementation stage.

The consultant will act as an adviser to the ICT director and will be responsible for overall architecture design of EDM ICT Information Security Technical Specifications, Supervision of the Tender Process together with the EDM team, to select the Consultancy firm, that will execute Implementation of Information Security program, as well as supervise the Implementation and stabilization of the Information Security Solution together with a designated EDM Team. The ICT Director is responsible for validating designs, integration and implementation strategy and planning and managing project delivery schedules related to:

Pre-implementation stage

- Development of Technical Specifications, including:
 - Penetration test and security assessment processes and tools
 - EDM Perimeter and public facing infrastructure Penetration tests
 - EDM Corporate wired network Penetration tests
 - EDM Corporate Wireless network Penetration tests
 - EDM Videoconferencing System Penetration tests
 - EDM Penetration test and security assessment tools

- Cyber Crisis Management Plan
- ICT Security Policies and Procedures based on ISO/IEC 27001 and ISO/IEC 27002
- Cyber Security Operation guideline and Incident Response Procedure
- Cyber Security Monitoring
- End user security: anti-virus, email security, and application security
- Cyber Security Training
- End-to-end Procurement of ICT Security Service provisioning:
 - Preparation of Tender Documents
 - Bid Clarifications
 - Bid Evaluations (Presential)
 - Contract Negotiations
 - Contract Award

Implementation stage

- Supervision of Program Implementation:
 - Implementation Planning
 - Implementation of Information Security Solution
 - Contract Performance Review
 - Ensure knowledge transfer

Post-implementation stage

Along with the strategy team, the consultant will support EDM in devising an implementation plan in line with the recommendations which will derive from the infosec baseline assessment report to design and implement a business-focused Cyber risk program

The InfoSec consultant will help EDM to review all handover documentations and to prepare the Project Completion Report.

The consultant will ensure that knowledge transfer has been conducted for EDM staff and consultants to continue to operate and improve the cybersecurity infrastructure. The handover documentation includes but are not limited to:

- Detailed Technical Report on the finding together with recommendations
- Detailed Document Cybersecurity implementation roadmap
- ICT Security Policies and Procedures
- Document on best suitable proposed Cybersecurity Architecture
- Detailed Infosec strategy document
- Infosec Crisis Management Plan

- Detailed Cyber Security Policy and Procedures document

The Consultant will plan requirements with designated EDM internal ICT teams and external consultants. He will monitor the whole project lifecycle, this includes managing development of Technical Specifications, Supervision of Procurement lifecycle, development and management of the project schedules, identifying risks and clearly communicating them to project stakeholders, explaining analyses and recommendation to EDM executives and discuss the technical trade-offs in design and implementation plan adoption with hired Consultant Company.

The InfoSec consultant will provide advisory and technical expertise to help EDM designing and deploying state-of-the-art cybersecurity infrastructure, practices and operating models. The consultant will provide subject matter expertise and utilize his savvy to work collaboratively with EDM internal ICT teams and contractors to advise, design, build, and implement pragmatic cybersecurity solutions.

The InfoSec consultant will also function as a technical resource for EDM during the procurement process, providing technical advice as requested. To this end, the consultant will be expected to:

- Working with EDM to elaborate cyber security technical requirements.
- Working in a multi-disciplined team of Strategy, Network infrastructure, Data Centre, and business applications to bring the best mix of Cybersecurity defense in line of business requirements
- Designing a pragmatic but effective cybersecurity defense roadmap for EDM.

4.2. Specific Tasks

4.2.1 Pre-implementation stage:

Task 1: Support to the EDM tender process for the Information Security project

The Consultant will provide technical support to the EDM Team for the ongoing procurement process related to the Information Security Implementation project. This include support to EDM in development of Tender documentation, contract negotiation with the selected Vendors and Service Providers, Contract Award and Contract monitoring and controlling; it includes but is not limited to the following activities:

- (i) Define information security requirements to be included in the bid document, including both information security components for the ICT

- systems and information security assessments to be conducted by the selected vendor
- (ii) Assist and review in preparing technical clarifications during the bidding processes including during the pre-bid conference, if proposed for the package
 - (iii) Assist EDM teams on preparing and issuing technical addendum to the bid document, if required
 - (iv) Assist EDM in Tender evaluation and Reporting
 - (v) Assist EDM in Contract Award and Implementation

4.2.2 Implementation stage:

Task 2: Supervision on the Implementation of Information Security (InfoSec) and related activities and Project

- Participate, vet, and validate the Implementation delivery plans, outlining the approach, dependencies, and activities needed to achieve on time and within budget a successful delivery of the project.
- The consultant will ensure that internal stakeholders well understand the approach and tasks needed to achieve successful network and other penetration tests, and the activities are carried out on time and within budget.
- Facilitate, coordinate, vet, and validate the network and other penetration test activities that the selected vendor will perform under the Infosec assessment project. The scope of each penetration test must be clearly defined to make sure the vendor has fully covered the define scope.
- Monitor and manage the delivery and execution of EDM Information Security Project
- Monitor Project Implementation planning and execution up to completion by the vendor
- Define Contract Performance Indicators and Execute Performance Reviews

Task 3: Management of Infosec Baseline Assessment

- Participate, vet, and validate the delivery of cybersecurity baseline assessment project, outlining the success criteria, approach, dependencies, and activities needed to achieve on time and within budget a successful delivery of the project.

- Monitor and manage the delivery and execution of EDM Infosec security baseline assessment.
- Review and validate the cybersecurity baseline assessment report

Task 4: Infosec Plan, and Strategy

- Participate in the preparation and review of Infosec and Cyber Defense Strategy defining a medium to long-term vision, objectives, priority action areas, roles, and tasks to serve as the basis for activity planning and resource allocation for EDM Cybersecurity improvements effort.
- Participate in the preparation of Cybersecurity Policies & Procedures, including the list of specific procedures to be defined. Monitor the development of Cybersecurity Policies & Procedures, Cyber Crisis Management Plan as part of the above Policies and Procedures, including quality control of the deliverables.
- Participate and oversee the Preparation of Information / Cyber Security Incident management system

Task 5: Infosec implementation roadmap

Along with EDM network infrastructure team, Data Centre infrastructure team, Strategy team and Application team, the individual consultant will work with the selected bidder to devise a synopsis and strategic cybersecurity implementation roadmap to equip EDM with a cybersecurity ecosystem that should include but not limited to,

- Identity and Access Management System
- Network Segmentation and Zoning design
- Security Information and Event Management (SIEM), Correlation and Visibility system
- Threat Detection system
- Data Loss Prevention system
- Vulnerability management program
- Security incident response and Mitigation system
- People and Process around cybersecurity
- Design a Plan for Incident Management and Disaster Recovery
- Risks assessment and acceptance framework
- Threat and vulnerability intelligence and Accessibility
- Cybersecurity awareness program
- Strategy and security controls in adoption cloud computing services

4.2.3 Post - Implementation stage:

Along with the strategy team, the consultant will support EDM in devising an implementation plan in line with the recommendations which will derive from the infosec baseline assessment report to design and implement a business-focused Cyber risk program

The InfoSec consultant will help EDM to review all handover documentations and to prepare the Project Completion Report.

The consultant will ensure that knowledge transfer has been conducted for EDM staff and consultants to continue to operate and improve the cybersecurity infrastructure. The handover documentation includes but are not limited to:

- Detailed Technical Report on the finding together with recommendations
- Detailed Document Cybersecurity implementation roadmap
- ICT Security Policies and Procedures Overview
- Document on best suitable proposed Cybersecurity Architecture
- Detailed Infosec strategy document
- Infosec Crisis Management Plan
- Detailed Cyber Security Policy and Procedures documents

5. DELIVERABLES

The InfoSec consultant will lead and manage end-to-end Cybersecurity related projects which deliver spans from Tender specifications preparation and support, project inception stage through network penetration, Infosec assessment validation, and implementation roadmap while ensuring on-time and quality delivery.

The following contribution and deliverables are expected from the consultant.

- Technical Specifications for ICT Information Security Solution
- ICT Information Security Solution Procurement Plan
- Information Security Implementation plan
- Validate post-implementation documents for

- Detailed Technical Report on the finding together with recommendations
- Detailed Document Cybersecurity implementation roadmap
- ICT Security Policies and Procedures Overview
- Document on best suitable proposed Cybersecurity Architecture
- Detailed Infosec strategy document
- Infosec Crisis Management Plan
- Detailed Cyber Security Policy and Procedures documents
- Validate post-implementation Report

Apart from the various documents described across this ToR such as the Technical Specifications, Tender Documents, draft Bid Evaluation Report for the prospective vendors, the consultant shall deliver Monthly Progress Reports across the whole project implementation period and at the end of implementation by Vendor he/she will prepare the Project Completion Report, which will be subject to review and approval by EDM.

6. CONSULTANT'S EFFORT AND DURATION OF THE ASSIGNMENT

The estimated duration of this assignment is 13 months with possibility of renewal based satisfactory completion of deliverables. The commencement of the assignment will be with effect from the first half of 2020.

The assignment activities will be rolled out over three stages below and estimated duration below:

#	Stage	Task	Timeline
1	Pre-implementation	a) EDM Information Security Tech Specs Development	Month 1 - 2
		b) Support to the tender process for the Infrastructure projects	Month 3 - 5
3	Implementation	Support Project Implementation	Month 6 - 12
3	Post Implementation	Handover and project completion	Month 13

7. SUPERVISION OF WORKS

The Consultant will directly report to the ICT Director.

EDM ICT will be the main focal point for the consultant.

In order to ensure that the key essential questions/issues are addressed in the individual and group consultations, the specialist Consultant agreed on a guideline template of process issues/questions as outlined below:

TASK	KEY ACTIVITIES	TIMELINE
Preparation of Technical Specifications and Tender Documents Preparation		
EDM Information Security Tech Specs Development	<ul style="list-style-type: none">• Preparation of Technical Specifications• Preparation of Tender Documents	Month 1 – Month 2
Support to the EDM tender process for the Information Security project		
Support to the EDM tender process for the Infrastructure projects	<ul style="list-style-type: none">• Assist and review in preparing technical clarifications for the pre-bid conference, if proposed for the package, including issuance of technical addendums to the bid document, if required• Assist and Evaluate Bids submitted• Assist in Contract Negotiations with selected Bidder, including Contract Award procedure and mobilization works	Month 3 – Month 5

TASK	KEY ACTIVITIES	TIMELINE
Support Implementation of Information Security (InfoSec) Project		
	<ul style="list-style-type: none"> • Review the test plan and implementation plan • Review adherence to Information Security Tech Specs and design; define acceptance criteria • Participate, vet, and validate the Design and project delivery plans, outlining the approach, dependencies, and activities needed to achieve on time and within budget a successful delivery of the project. • Monitor and manage the post Implementation activity scheduling • Activity Infosec Baseline Assessment and depending activities • Infosec Plan, and Strategy and depending activities • Infosec implementation roadmap and depending activities • Completion Project report 	Month 7 -13

8. PROFILE AND QUALIFICATIONS OF THE INDIVIDUAL CONSULTANT

The primary purpose of the position is to deliver professional cybersecurity consulting in overseeing EDM initiatives to improve its cybersecurity posture, including benchmarking/maturity assessments, developing strategies, and roadmaps for improvement.

Therefore, it is expected that the consultant is equipped with extensive knowledge in ICT infrastructure security with the strong technical expertise required in the following areas:

- Firewalls – (Cisco and FortiGate)
- Network Intrusion Detection and Prevention Systems (IDS/IPS)
- Network Access Control (Cisco ISE, etc.)
- Incident Response and Remediation
- Security Information and Event Management (SIEM)
- Packet decoding and analysis
- Web Proxy Servers
- Vulnerability management
- Load Balancing (Citrix NetScaler (ADC) or F5)
- SSL VPN Solutions
- Enterprise Wireless
- Security Monitoring and Alerting with integrated solutions
- Cloud computing

The Cybersecurity Consultant must meet the following requirements:

Basic Qualifications:

- Master Degree in Computer Engineering/Sciences, Information Technology or other applicable or related disciplines as appropriate.
- Deep Knowledge of TCP/IP network and IANA ports number
- Ability to lead and execute large, complex cybersecurity projects related to technology and ecosystem integration

Preferred Qualifications

- IT Network consulting experience with the following:
 - I. International experience (minimum 5 years) in a series of projects of similar nature and scale as this consultancy;
 - II. Extensive prior experience in developing strategic plans for Cybersecurity roadmap posture improvement
- Strong problem-solving skills and ability to provide hands-on technical support
- High-level certification in a major technology area preferred (CISSP or any of GIAC certification) and CCIE Security Lab cleared
- Encryption technologies, ethical hacking and penetration testing.

- Windows, UNIX and Linux operating systems.
- Exposure to common programming languages including, Python, C, C++, C#, Java, SQL or PHP.
- Network administration skills to test internal systems such as firewalls and IPS/IDS devices to ensure networks are safe.
- Experience with Next Generation Firewalls and IPS and Security Information and Event Management
- Engineering Project Management
- Deep understanding of Standards related to implementing a risk management framework including COBIT, ITIL, ISO 27001/2 and NIST.
- Knowledge of ITIL including Incident, Problem, and Change Management
- Experience in drafting and managing international contracts related to Data Network installation and upgrade, having proven skills in procurement for IFI funded projects.
- Experience with Procurement under World Bank Procurement Guidelines.

Moreover, the consultant should have excellent oral and written communication skills in the English language, Command of Portuguese would be also highly desirable and possess a high level of organization skills.

9. REPORTS/VARIOUS DOCUMENTATION AND SCHEDULE

TYPE OF REPORT	QUANTITY	TIME LINE	MAX. TIME FOR EDM APPROVAL
EDM Information Security Technical Specifications	Softcopy	Three weeks after contract effectiveness	10 days
InfoSec Procurement Plan	Softcopy	Five weeks after contract effectiveness	7 days
EDM InfoSec. Implementation Plan	Softcopy	Five weeks after contract effectiveness	7 days
Tender Document	Softcopy	Seven weeks after contract effectiveness	10 days
Bid Evaluation Report	Softcopy	Fourteen weeks after contract effectiveness	10 days

Contract Management Contract Review Schedule	Softcopy	Twenty weeks after contract effectiveness	5 days
Contract Documents upon negotiations with successful Bidder	Softcopy	Twenty-two weeks after contract effectiveness	10 days
Monthly Progress Report	Softcopy	Every 7 th day of following calendar month	7 days
Completion Project Report	Softcopy	Immediately after the end of the assignment, i.e., thirteen months after contract effectiveness	10 days