

TECHNICAL ASSISTANCE PROJECT

Mapping of Critical Information Infrastructures and the Assessment of National-Level Cybersecurity Risks

Mozambique

I. INTRODUCTION

Mundi Consulting is leading the preparation of a Proposal to develop the Project “*Mapping of Critical Information Infrastructures and the Assessment of National-Level Cybersecurity Risks*”, in **Mozambique**, to **INTIC** – Instituto Nacional de Tecnologia de Informação e Comunicação, integrated in the **Ministry of Communications and Digital Transformation**.

For the implementation of the Project, there is the need to set up a Consultancy Team to integrate the Proposal. The present document intends to present a general overview of Project activities, as well as to describe the **PROFILE of the Experts** that **Mundi Consulting** would like to identify potential candidates to integrate the Consortium TEAM.

II. OBJECTIVES

General Objective

To hire a firm to identify and classify the assets and stakeholders of **Critical Information Infrastructures (CII)**, followed by the development of a **National Cybersecurity Risk Management Framework** adapted to the context of Mozambique.

Specific Objectives

- Develop and present the methodology and criteria for the selection of **Critical Information Infrastructures (CII)**.
- Identify, classify, and develop a database of all **Critical Information Infrastructures (CII)** at the national level.
- Situational analysis and gap assessment of the cybersecurity risk management practices of **Critical Information Infrastructures (CII)**, conducted as a summary (light-touch) assessment, aimed at supporting the development of the **National Cybersecurity Risk Management Framework for CIIs**;
- Develop the **National Cybersecurity Risk Management Framework for CIIs**.

III. SCOPE OF WORK

The project comprises the following phases and activities.

Phase 1: Inception and Methodology Development

Develop and validate the work plan and methodology, including:

- Stakeholder Engagement Plan
- Risk Assessment Approach
- Alignment with international frameworks and/or national legal and regulatory requirements

Phase 2: Identification and Classification of CIIs

- Review national development priorities, sectoral strategies, and interdependencies to identify critical sectors and assets at the national level.
- Propose criteria for the classification and designation of Critical Information Infrastructures (CII).
- Conduct a survey of Critical Information Infrastructures (CII) at the national level.
- Conduct a business impact analysis and create a national registry of Critical Information Infrastructures (CII), including their location, operational dependencies, and interconnections.
- Recommend institutional mechanisms for the designation, review, and oversight

Phase 3: Situational Analysis and Gap Assessment of Cybersecurity Risk Management Practices of CIIs

- Conduct the situational analysis, and identify and assess gaps in the cybersecurity risk management practices of Critical Information Infrastructures (CII).
- Identify the legal and regulatory requirements related to cybersecurity risk management and CII compliance.
- Prepare a report with recommendations to improve the governance and monitoring of Critical Information Infrastructures (CII) at the national level.
- Engage with relevant stakeholders through in-person and virtual bilateral meetings, and conduct three (3) workshops—one in the northern region, one in the central region, and one in the southern region—to gather insights, validate the results obtained, and obtain feedback for the mapping process and the development of the action plan.

Phase 4: Development of the National Cybersecurity Risk Management Framework for CIIs

- Based on the results of the identification, mapping, and risk assessment, develop the National Cybersecurity Risk Management Framework for CIIs, which should enable governance and accountability, risk assessment, treatment, monitoring, and response in a standardized manner across the country, while respecting the particularities of each sector.
- Propose a standardized national methodology for the identification, assessment, mitigation, and reporting of risks (e.g., risk matrices, asset assessment, threat taxonomy).
- Establish guiding principles for risk prioritization and treatment.
- Implement a reliable mechanism for sharing information on risks and mitigation measures among CII operators and other stakeholders.
- Develop specific recommendations for cybersecurity resilience and security measures for each sector of the identified critical infrastructures, in close collaboration with sectoral regulators.
- Conduct a final in-person validation workshop to present the CII mapping and review the first version of the National Cybersecurity Risk Management Framework, gather input from stakeholders, and finalize the document before submission.

IV. DURATION & PLACE OF EXECUTION

The consultancy is expected to be completed within **7 months** from the start date. The process should include data collection, meetings, consultations with relevant entities, and workshops with stakeholders.

V. EXPERTISE REQUIRED

Team Composition & key expert profiles

1. Project Manager

- Hold a Master's degree in Information Technology or related fields, or in Public Administration and Public Policy, Project Management, Engineering, Public Safety, or related areas, and have at least 10 years of experience in risk management and critical infrastructure security projects in the cybersecurity field.
- Knowledge of international security standards (ISO 22301, ISO 27001, NIST, ISO 31000, NIST 800-30, IRAM2) is considered an advantage
- Demonstrated ability in inter-institutional coordination (government, private sector, security).

2. Cybersecurity Specialist

- Hold a Master's degree in Information Technology, Information Security, Computer Engineering, or related fields.

- At least five (5) years of experience in network protection, industrial systems security, and cybersecurity incident response.
- The following certifications are considered an advantage: ISO 22301, CISSP, CEH, CISM, ISO 27001.

3. Cyber Risk and Resilience Management Specialist

- Hold a Master's degree in Information Technology, Information Security, Security Engineering, or related field
- At least five (5) years of experience in threat analysis, business continuity and disaster recovery planning, and information security risk management.
- Knowledge of risk mitigation strategies and vulnerability assessment.
- The following certifications are considered an advantage: CISSP, CEH, CISM, ISO 27001.

4. Physical Security and Strategic Protection Specialist

- At least five (5) years of experience in physical security planning, access control, and crisis management
- Hold recognized professional certifications such as CISSP, CISM, ISO/IEC 27001 Lead Implementer, or equivalent certifications in physical security and critical infrastructure protection.
- Knowledge of security related to against terrorism, sabotage, and transnational crimes.

Mundi Consulting
Lisbon, August 2026