REPUBLIC OF MOZAMBIQUE

MINISTRY OF PUBLIC WORKS, HOUSING AND WATER RESOURCES, NATIONAL ROADS ADMINISTRATION, PUBLIC INSTITUTE

CLIMATE RESILIENT ROADS FOR THE NORTH (P500488)

In the Provinces of Cabo Delgado, Nampula & Niassa – Mozambique

SECURITY MANAGEMENT PLAN

(SMP)

MAY 2025

PREPARED FOR

Administração Nacional de Estradas (ANE)
Gabinete do Director Geral
Attention: Mr. Elias Anlaué Paulo - Director General
Av. de Moçambique, Nº 1225, C.P. 403
Maputo Mozambique
Telephone: +258 21 476 163 / 7,
Email: anenorte.42@ane.gov.mz

PREPARED BY

info@jbn.co.ug / www.jbn.co.ug
Kampala, Uganda
in Joint Venture with
info@ea.intelligentperspectives.com
Maputo, Mozambique

	SECURITY MANAGEMENT PLAN (SMP) - 2024	**PLAN.21.01.24 REV. 003**
	SMP – CLIMATE RESILIENT ROADS FOR THE NORTH	Page i of 40
Periodicity of review	Annual	
Level of coverage	North Region – Cabo Delgado, Nampula and Niassa	
Responsible for the plan	ANE	
Direct implementers	PSC, PIU, Security Risk Management Company and PIs	
Type of Information	CONFIDENTIAL	

DOCUMENT CLEARANCE FORM

Name of Unit	Environmental Services
Document Title	Consultancy Services to Develop the Environmental and Social Instruments for Climate Resilient Roads for the North of Mozambique.
Project Name	Climate Resilient Roads for the North (P500488)
RFP Nº	**47A003041/CP/157/2023**
Client Address	Administração Nacional de Estradas (ANE) Gabinete do Director Geral Attention: Mr. Elias Anlaué Paulo - Director General Av. de Moçambique, Nº 1225, C.P. 403 Maputo Mozambique Telephone: +258 21 476 163 / 7, Email : anenorte.42@ane.gov.mz

Quality Assurance	Reviewer/Approver	Title/Role	Version
Consultant (JBN Team)			
Author	JBN in Joint-Venture with EA Consultoria	Consultants	v.003
Reviewer(s)	Alfredo Ricardo Zunguze	Project Manager	v.003
Approver	Nelson Omagor	Team Leader	v.003
External Parties - Client Reviewers			
Current Version		Draft Report ☐	Final Version ☑

Acronyms

ANE, IP	National Roads Administration, Public Institute
CRRNP	Climate Resilient Roads for the North Project
CSOs	Civil Society Organizations
COP	Community of Practice
EHS	Environmental Health and Safety
EHSS	Environmental, Health, Safety and Security
ESG	Environmental and Social Governance
GBV	Gender-Based Violence
GRC	Grievance Redress Committee
GRM	Grievance Redress Mechanism
GDP	Gross Domestic Product
M&E	Monitoring and Evaluation
GoM	Government of Mozambique
GRS	Grievance Redress Service
KRI	Key Risk Indicator
IGP	International Good Practices
ILO	International Labor Organization
ICOCA	International Code of Conduct Association
IPs	Implementing Partners
ISO	International Organization of Standardization
INATRO	National Institute of Road Transport
M&E	Monitoring and Evaluation
OHS	Occupational Health and Safety
PIU	Project Implementation Unit
PSC	Project Steering Committee
PPE	Personal Protective Equipment
RF, PF	Road Fund, Public Fund
SRA	Security Risk Assessment
SRAp	Security Risk Appetite
SRT	Security Risk Treatment
SEP	Stakeholder Engagement Plan

SCP	Stakeholder Consultation Plan
SMP	Security Management Plan
SRMC	Security Risk Management Company
SOP	Standard Operating Procedures
ToRs	Terms of Reference
UN	United Nations
WGRC	Workers Grievance Redress Committee
WB	World Bank

APPENDIX		
Ref	**Topic**	**Pag**
1	Terms of Reference for Security Risk Management Specialist – Security Officer – Security Representative (IP's)	40
2	Crisis Management Plan	49
3	Security Checklist and Minimum-Security Standards	55
4	Activity Security Plan	59
5	Weekly Security CoP (Community of Practice)	62
6	PIU Travel Policy	65

Executive Summary

With the purpose of addressing potential risks in the project to be implemented, the Security Management Plan was designed to handle risks with consequences on people, assets, infrastructure, and operations.

The present Security Management Plan was developed based on the Security Risk Assessment for the project and describes how and by whom security will be managed and implemented.

Considering the security situation in the country in general and particularly in the northern region, where we have been witnessing the phenomenon of insurgents attacks and their consequences since 2017, there arose the need to conduct a Security Risk Assessment for the area to be covered by the project, namely the provinces of Cabo Delgado, Niassa, and Nampula.

In this context and aiming to determine the necessary security level for the project, the Security Risk Assessment was carried out, considering the districts covered by the project, which served as the foundation for this Security Management Plan. For the identified risks, the plan defined the treatment that is deemed most appropriate based on ISO 31000:2018 (Risk Management) through the principles, framework, and process (as attested below), Mozambican legislation, International Humanitarian Law, World Bank Environmental and Social Standards (ESS), the Voluntary Principles on Security and Human Rights (VPSHR), and the International Code of Conduct for private security companies.

To ensure the effectiveness and acceptance of the security plan, engagement with stakeholders, guideline was defined for Stakeholder Engagement Plan (SEP).

With the objectives of establish a mechanism to receive and process complaints in a timely manner, with special attention to vulnerable groups, were defined Project Grievance Redress Mechanism (PGRM), that will be implemented through the installation of green lines.

In terms of the security governance, were defined:

- ✓ Responsible at the Strategic and Implementation level;
- ✓ Security Structure;
- ✓ Security Priorities, Roles and Responsibilities (PSC, PIU, SRMC and PIs).

Considering that, incident reports and security incident analysis are extremely critical for, management decisions, were defined Security Incident Report (SIR) document structure to report incident that impact people and loss incident.

This SMP, also defined some Operation Security Procedures (OSP) such as:

- ✓ Project Perimeter Security Control;
- ✓ Storage and Control of Materials;
- ✓ Information and Communication – Categorization, Treatment, and Control of Sensitive Information;
- ✓ Protection of people; and
- ✓ Emergency response exercises and report structure document.

Throughout the project lifecycle, the SMP were defined five security gateways. Each security gateway, the PIU Project Manager, in consultation with the PIU Security Risk Management Specialist, must provide authorization for the Project to progress.

In accordance with the International Good Practices (IGP), the SMP were defined Partners Security Requirements, Security Partners in CRRNP Project and Weekly Security CoP, PIU Travel Policy, and Crisis Management Plan.

Table of Contents

1. Background of the Project

Mozambique's economy grew steadily until 2015, averaging 7.3 percent. From 2016 to 2020, economic activity decelerated sharply, and in 2020, gross domestic product (GDP) declined by 1.2 percent, marking the first economic contraction in three decades.

Agriculture employs about 80 percent of the total workforce and generates about 30 percent of gross domestic product (GDP). This sector is the mainstay of Mozambique's economy and is critical for overall poverty reduction. However, agricultural productivity remains low and constrained by many factors, including limited access to transport infrastructure and services in rural areas.

In addition to the poor accessibility to rural areas, Mozambique is highly exposed to extreme weather events, principally flooding that may become even more frequent because of Mozambique's geography and long coastline.

The recovery of the economy has a low impact on the reduction of poverty for the rural people as is driven by capital-intensive and import-dependent sectors, while low-skilled jobs in the agriculture sector continue to dominate employment. As a result, the poorest people, living mainly in rural areas of Mozambique's northern region, have benefited less from economic growth than the overall population.

In Cabo Delgado province, the cyclones, heavy rains and floods destroyed various infrastructures, including roads and bridges, hitting an already vulnerable population, which was in many areas affected by terrorism, violence and poverty.

According to CRRN Project Concept Note (2023), the delays in rebuilding road infrastructures caused by insufficient financial resources had increased the degradation of the road network and bridges, especially steel bridges, causing partial isolation of the Mueda, Quissanga, Muidumbe, Macomia, Mecufi and Metuge districts, affecting around 378,762 people.

In line with the above, the Government of Mozambique (GoM) through the National Roads Administration, Public Institute (ANE, IP) and Road Fund, Public Fund (RF, PF) is therefore preparing the implementation of the **Climate Resilient Roads for the North Project (CRRNP)** to enhance climate-resilient, safe and sustainable road connectivity in the Northern Provinces of Mozambique.

The involvement of project-affected parties (PAPs) and other interested parties is one of the activities that must be carried out throughout the project life cycle, starting during the process

of preparation, selection, implementation and operation of the project and within a time frame that allows relevant consultations with PAPs on project design.

In this context, the need to prepare the Stakeholder Consultation Plan (SCP) inclusively is established, providing relevant data on the security situation for people, infrastructure, assets, and operations in the areas covered by the project, serving as the basis for the Security Management Plan.

2. PROJECT DESCRIPTION

2.1. Project Development Objectives and Description

The project objective is to enhance climate-resilient, safe and sustainable road connectivity in the Northern provinces of Mozambique, namely Cabo Delgado, Niassa and Nampula. It will target the upgrading, rehabilitation, and maintenance of selected secondary and tertiary roads, as well as the construction and rehabilitation of bridges in the secondary road network and installation of bailey bridges in the tertiary road network.

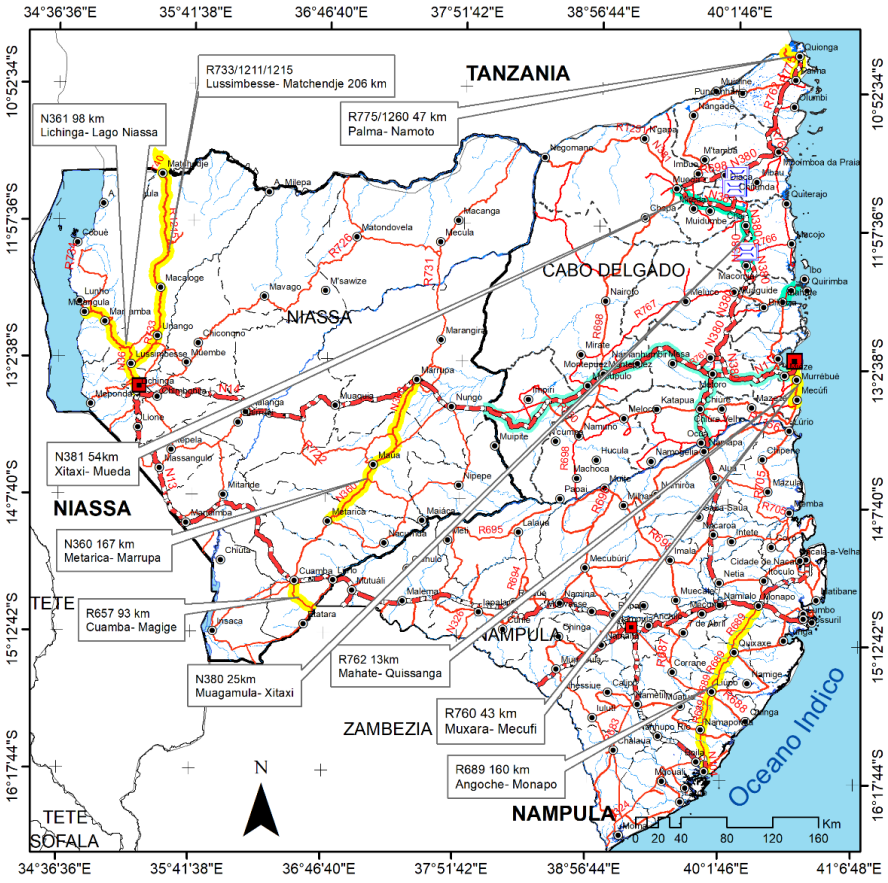


Figure 1 – Project target área

2.2 Project Components

The project consists of three (3) components, as described in the table below:

Component	Subcomponents and Description
Component 1: Climate Resilient, Safe and Sustainable Improvement of Roads (US$ 119.6 million)	Sub-component 1.1: Improvement and maintenance of road network (US$81.5 million). This sub-component will focus potentially on the following: (i) Upgrade of 52km of the secondary road N381 Mueda – Xitaxi; and 15km of the tertiary road R762 Muepane – Quissanga; and rehabilitation of 25km of sealed secondary road N380 Muagamula – Xitaxi in Cabo Delgado province, including the rehabilitation or reconstruction of culverts and other drainage infrastructure; (ii) Consultancy services for the preparation of concept design and bid documents for upgrading/rehabilitation of roads, including for follow-on operations, and the monitoring of road works; and (iii) Land acquisition and resettlement of project affected persons. Road safety audits/inspections will be conducted at different stages of the project, speed management and improved Vulnerable Road User (VRU) facilities will be ensured across project roads and bridges. Pedestrian sidewalks, and cycle lanes in urban and community centres, including wider shoulders along road segments will be introduced for non-motorized traffic to increase road safety of VRUs. Through this Subcomponent, Community infrastructure (markets, schools, health centers, agriculture produce storage facilities) will be provided to rural population along segments of roads targeted by the project and incorporated into the works contracts.
	Sub-component 1.2: Improvement of bridges and drainage structures (US$38.1 million). This sub-component will focus on: (i) Construction and rehabilitation of five concrete bridges along the secondary road N380 in Cabo Delgado (Mirohote (45m), Muaguamula (40m), Muera 1 (55m), Muera 2 (30m) and Nango (35m); (ii) Consultancy services for the preparation of concept design and bid documents, and the monitoring of the bridge works in Cabo Delgado province; (iii) acquisition and installation of 1,500m of bailey/metallic bridges in

	tertiary roads in all three northern provinces, including the construction of substructure of the bridges; and (iv) Consultancy services for design and preparation of bid documents for construction of the substructure for installation of the bailey/metallic bridges in all three northern provinces.
Component 2: Improvement of Road Safety and Transport Mobility (US$ 2.5 million).	The Safe System approach for road safety will be an integral part of the road design and implementation. This component will finance: • The enhancement of the capacity of the National Institute of Road Transport (INATRO) on road safety regulation, inspection and supervision, and ANE on road safety engineering. • A pilot program on safe road infrastructure, inclusive road safety programs targeting youth, awareness-raising and dissuasive measures, and improving gender disaggregated crash data collection. • First responder training for youth across project roads. • A “safer route to school” pilot to improve access to schools. • Capacity building and accreditation on road safety audit; and • A study on improving transport services in rural areas, including addressing the recommendations of the report.
Component 3: Institutional Strengthening and Project Management (US$ 2.9 million).	Component 3 will include incremental operating costs and institutional strengthening activities. It will cover: • An institutional assessment of the road sub-sector. • Road asset management. • Enhancement of climate resilience in planning and management of road infrastructure. • Road and traffic data collection. • Preparation of a road maintenance strategy. • Study on facilitation of public private partnerships in road rehabilitation and maintenance; (vii) development of community resilience committees led by women to support emergency preparedness and response; and

	• Promotion of women's employment in the road sub-sector. Effort will be made to incorporate a skills development and livelihoods sub-component to provide opportunities for conflict-impacted local labour in the road works. This component will also provide technical assistance for the implementation of the project including procurement, FM and audits, environmental and social oversight, and M&E.

Table 1: Summary of project componentes

3. APPROACH

Mixed methods were adopted to develop the SMP effectively. This involved reviewing relevant literature and collecting primary information through stakeholder interviews. The following section details the approach followed in developing the SMP

3.1 International Standards and Best Practices

This SMP was developed in accordance with ISO 31000:2018 (Risk Management) through the principles, framework, and process (as attested below), Mozambican legislation, International Humanitarian Law, World Bank Environmental and Social Standards (ESS), the Voluntary Principles on Security and Human Rights (VPSHR), and the International Code of Conduct for private security companies.

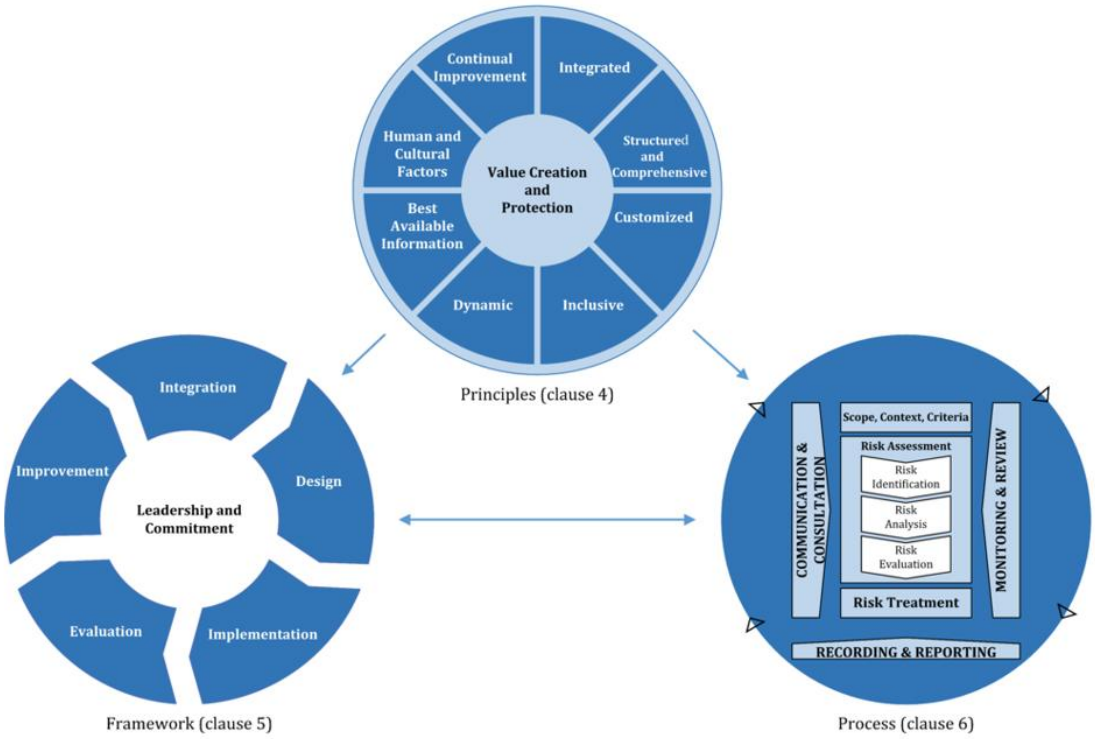


Figure 2 – Risk Management Integrate

According to ISO 31000:2018, there are three fundamental elements:

Principles - guiding that risk management should:

- Be an integral part of all organisational activities;
- Have a structured and comprehensive approach to risk management, contributing to consistent results;
- Have the risk management framework and processes tailored and proportional to the internal and external contexts of the organization related to its objectives;
- Include all stakeholders (those who can affect or be affected by a decision or activity);
- Due to the current dynamics, risks may emerge, change, or disappear as the external and internal contexts of an organization change;
- Have inputs based on historical data, current information, and future expectations (anticipation). Risk management should work with timely, clear, and available information for all relevant stakeholders;
- Consider that human and cultural behavior influences risk management aspects at each level and stage;
- Be continuously improved through learning and experiences (PDCA cycle).

Structure - which integrates risk management into the management system at the strategic level; and

The Process - that integrates risk management at the operational level.

3.2 Stakeholders Consultation Plan

The Stakeholder Consultation Plan (SCP) is integral to the Stakeholder Engagement Plan (SEP). A methodology has been defined for its implementation, aiming to create a robust engagement plan with effective collaboration from stakeholders while respecting critical aspects of an area characterized by some attacks by armed insurgents. In this context, the following steps were followed in the methodology:

3.2.1 Identification and Mapping of Stakeholders

Preliminary identification and mapping of key stakeholders to be consulted for the Security Risk Assessment and Security Management Plan in the provinces of Cabo Delgado, Nampula, and Niassa.

- Governmental and non-governmental institutions directly or indirectly involved in managing security risks impacting people, infrastructure, assets, and project operations;
- Institutions handling data related to security issues concerning people, infrastructure, assets, and project operations;
- Institutions with relevant information regarding security risks for people, infrastructure, assets, and project operations;
- Local communities and citizens with relevant information (guards, drivers, traders, etc.).

3.2.2. Definition of Objectives

- Gain a deep understanding of the local context and identify security risk factors for people (ANE and project staff, PIU, IPs, and communities), infrastructure, assets, and project operations in the project-covered areas;
- Bring different parties together to negotiate their interests;
- Enable the public to discuss and analyze project-related security issues;
- Achieve sustainable development of the project;
- Incorporate the wishes and opinions of interested and affected parties on security matters.

3.2.3. Principles of Stakeholder Consultation

- Public consultations will be organised throughout the project's life cycle, conducted openly, free from external manipulation, interference, coercion, or intimidation;
- Information will be provided and widely distributed among all stakeholders in an appropriate format, providing opportunities for stakeholder feedback, analysis, and addressing comments and concerns;
- Stakeholder identification is carried out to support better communications and build effective relationships. The participation process is inclusive, encouraging all stakeholders to participate in the consultation process.

Special Attention to Critical Groups

Special attention should be given to critical groups such as individuals - project workers (ANE, PIU, and IPs), drivers, who frequently travel to high-security risk zones, those involved in high-security risk project operations, and affected communities.

Commitment, Integrity, and Respect

Commitment to understanding, engagement, and stakeholder identification recognized and practiced from the outset. Integrity occurs when engagement is conducted in a way that promotes mutual respect and trust.

Transparency and Trust

Transparency is demonstrated when community concerns are responded to in a timely, open, effective manner and with the knowledge of all stakeholders. Trust is achieved through open and meaningful dialogue that respects and defends differences expressed in the community's beliefs, values, and opinions.

Ethical Considerations

The consulting team will rigorously adhere to the recommendations o maintain the utmost confidentiality and privacy of all participants during the consultation and data collection processes. Informed consent will be diligently obtained from each participant involved.

Continuous Evaluation

Conduct ongoing engagement assessments, adjusting the approach based on feedback and the evolving situation.

This plan aims to ensure an ethical, inclusive, and transparent consultation process that considers the diversity and specific needs of stakeholders and affected communities.

Tools for information collection

This process used information collection tools, including interviews (formal and informal), brainstorming, and checklists based on ISO 31010:2019.

4. MOZAMBIQUE SECURITY CONTEXT

A detailed analysis of the country's political, social, economic, and cultural situation was conducted by cross-referencing security data (crime statistics, reports on the Mozambican population, and various other available data) collected from different sources. The aim was to highlight security trends and specific threats in different regions of the country, particularly in the project-covered areas.

4.1 Socio-Political Context

Mozambique's estimated population is about 32 million, and approximately two-thirds of this population live and work in rural areas (World Bank, 2022).

Since 2017, Mozambique has registered Insurgents' attacks in the province of Cabo Delgado, and currently, incidents (albeit sporadically) in the province of Nampula and threats in the province of Niassa. The province of Cabo Delgado, in northern Mozambique, has been suffering Insurgents' attacks, with greater incidence in the districts of Mocímboa da Praia (the district which registered the first attacks), expanding later to other districts such as Macomia, Quissanga, Ibo, Muidumbe, Nangade, Palma and Meluco.

Nampula, with a record of at least one case of proven attack, whose target was a Christian institution (with one death recorded) and other facilities (Economic infrastructure) destroyed. Furthermore, Memba district, despite being a recruitment center for the Insurgents' is highly vulnerable to the risk

The consequences of this phenomenon are multidimensional, starting with the destruction of private homes, buildings and public and private entities, the paralysis of essential health and education services, the looting of commercial establishments, economic stagnation due to the lack of regular movement of people and goods, death and the existence of displaced people

throughout the country (Macalane, at all 2022). Generally, the insecurity in the region makes it less attractive for investment and economic activity, thus negatively affecting an already vulnerable population.

According to the latest annual report of the President of the Republic for 2023, the phenomenon of terrorism has led to the displacement of 627,846 people, of whom 50% are children, and 29.4% are women.

Mozambique will have presidential elections in 2024, this political event considered critical during the entire electoral period (propaganda/campaign period, elections, dissemination of results and post -elections period), will create great pressure on civil society organisations and, consequently, the need for observance of specific security procedures since wrong elements could seize the opportunity to harm the unsuspecting population.

In this context, a security risk assessment was carried out, considering the probability and consequence matrix, using the ISO 31000:2018 guidelines, in conjunction with IEC/ISO 31010: 2019, with the following criteria:

Probability		**Consequence (considered: people, tangible and intangible assets, and infrastructure)**	
Improbable	1	**Human harm (staff and community)**: No impact on the physical integrity of individuals; **Reputational**: Minor internal complaints; **In operations**: Operations halt for a maximum of 2 hours	1
Possible	2	**Human harm (staff and community)**: temporary disability and/or hospitalization; **Reputational**: local media backlash; **Operations**: 50% operations constraint	2
Probable	3	**Human harm (staff and community)**: disability (30%), temporary disability and/or hospitalization; **Reputational**: negative national backlash; **Operations:** 75% operations constraint	3
Almost certain	4	**Human harm (staff and community)**: disability (+30%) or death; **Reputational**: negative international backlash; **Operations**: Conditions the entire operation	4

Table 2 – Probability and Consequence criteria

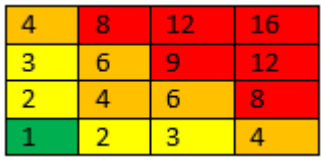
Inherent/residual risk level (IRL/RRL) Matrix	Ref.	Action
	1	Low risk: Maintain practices and procedures
	2,3	Moderate risk: Define management responsibilities
	4,6	High risk: high-level management action
	8,9,12,16	Extreme risk: Immediate action

Table3 – Inherent/Residual risk matrix level

4.2 Crime and Security

According to data made available by the National Statistics Institute (statistical yearbook - INE, 2022), the crimes registered and cleared by the Police of the Republic of Mozambique in the period 2020 to 2021 went from 16,624 to 14,985 registered crimes and from 14,321 to 14,230 cleared crimes, which corresponds to a reduction of 9.9% and 0.6%, respectively.

The category of crimes **against property** (robberies, armed robberies, thefts in their most different forms, arson, among other crimes related to loss of possession of property) and crimes **against persons** (voluntary and frustrated homicide, bodily harm in its most diverse forms, rapes, rape and others), are the categories that registered the highest number of cases for the year 2021, not being different in other previous years. Since no deliberate effort has been put in place to mitigate this, the trend is projected to continue.

4.3 Insecurity

The attacks that have a greater incidence in the northern area, specifically in Cabo Delgado Province, perpetrated by Armed insurgents, considering the ***Modus Operandi*** (attacks against the local population, creating fear and panic, burning residences, stealing food and people's goods, etc), in addition to grief and pain, have contributed to the destruction of socio-economic infrastructures, reduction of productive capacity, increase in unemployment and setback in the levels of social welfare.

This scenario in Mozambique has a direct and indirect impact on the presence of NGOs in the northern region, who, fearing that they could potentially be secondary or collateral victims, may simply withdraw and avoid their direct presence despite the communities' enormous needs, including humanitarian needs.

To respond fully to the insurgency in the north and considering that terrorism is an event that does not stop at the border, the Mozambican government, under cooperation agreements, is currently counting on the presence of Rwandan and SADC forces.

4.4 Kidnapping

This crime, which significantly impacts the human, social and economic aspects, tends to occur in large urban centres, especially in Maputo Province, Maputo City, Sofala and Manica and has created a feeling of insecurity for citizens, especially the victims.

The most common ***motive*** is financial (ransom demand), but we also have situations of account adjustments between groups and scenarios motivated by cultural issues (for superstition purposes), etc.

5. ASSESSING RISKS

Considering that there is a real threat in almost all districts covered by the project, this scenario requires that a security risk assessment guide all project activities to ensure that all people, assets, and infrastructure are safe and protected. Recognizing the fundamental importance of preserving life, all risk assessments aim to establish an understanding of the threats posed by malicious actors to the personnel affected by the project within the local environment.

The assessment methodology used follows a "Risk-Based" approach grounded in ISO 31000:2018 combined with ISO 31010:2019, where risk is assessed based on the probability of a threat, the severity of the consequences, and the vulnerability of the project in terms of the effectiveness of existing and proposed risk mitigation measures. In this context, the risk assessment process should follow the steps below:

- **Risk Identification**: Find, recognize, and describe risks that may hinder the project from achieving its objectives;
- **Risk Analysis:** Aims to understand the nature of the risk and its characteristics, including the level of risk where applicable. Considers factors such as probability, consequence, effectiveness of existing controls, matrices, etc;
- **Risk Assessment:** Aims to support decision-making. Uses the analysis (previous step) to determine where additional action is needed.

5.1 Security Gateways

Throughout the project lifecycle, there are five security gateways. At each security gateway, the PIU Project Manager, in consultation with the PIU Security Risk Management Specialist, must provide authorization for the Project to progress. The five gateways are:

- Initial Risk Assessment and Work Plan Review;
- Project Feasibility Assessment;
- Tender Process;
- IP Onboarding Process;
- Security Audit during Project Implementation

6. SECURITY RISK TREATMENT

6.1 Districts Cover by project major risks exposed

Considering the activities developed by the ANE, below is a compilation of the greatest risks exposed:

Ref.	Description
R1	Insurgent attacks
R2	Kidnapping related to Insurgents' attacks
R3	Theft/Assault related to Insurgents' attacks
R4	GBV
R5	Demonstrations/tumults/vandalism related to Insurgents' attacks
R6	Residential Fire related to Insurgents' attacks
R7	Traffic Accidents
R8	Natural disaster and Health Risk
R9	*Logistics*: Inability to transport materials to the project due to insecurity
R10	Social: Conflicts with the community related to land access and unemployment
R11	Infiltration of insurgents among the project workers

Table 4 – Project risks exposed

ANE must ensure the presence of an internal staff member or consultant who will be responsible for managing security issues, ensuring the existence and implementation of a policy, plan, and procedures, and defining the security Level of security risk tolerance.

This individual should ensure that the treatment for the inherent risk is observed and that the residual risk falls within ANE's security risk appetite.

Risk	Average risk level –all districts	Risk treatment	
		Change probability	**Change consequence**
Insurgents' attacks	Lower category of the Extreme Risk	X Strengthen physical security barriers; Establish a robust access control system; Implement Conflict Early Warning Systems through intelligence collection and analysis; Maintain constant collaboration with local forces and share relevant information; Use Artificial Intelligence or specific software for data analysis; Install Monitoring and Alert Systems – intrusion and explosive detection systems; Use drones for patrol and monitoring (within legal limits).	Design of a security procedure; Design of a travel policy for critical areas; Design of an emergency response procedure; Design of minimum-security standards for vehicles, individuals in high-risk areas, infrastructure, and assets; All project employees traveling to the districts must have a portable first aid kit and a first aid bag in the vehicle. They should also have a survival kit; Design of key risk indicator.
Kidnapping	The last category of the High Risk	Training and simulation exercises on procedures to follow in a kidnapping situation Training to avoid kidnappings, including but not limited to the following topics: Operational security – sensitive information and route management;	Design of an emergency response procedure; Assigning panic buttons and gps equipment to individuals with specific profiles.

		How to maintain a low profile; Techniques for escaping a captivity situation; Use of codes and secure communication systems; How to handle and avoid violence from the kidnapper.	
Theft/Assault	Last category of the High Risk	The internal security manager or consultant must close liaison with local authorities (police and military); Training on procedures to follow in a theft/assault situation. Training to avoid robbery/assault situations, including but not limited to the following topics: Identification of suspicious situations/people; Personal safety and the use of personal safety apps; Security at home, work, and of personal belongings; Protocols for managing valuable items;	Ensure that private security deployment is subject to a Code of Conduct and binding agreement on the use of force; Private security actor should be a member of ICOCA (International Code of Conduct Association).
GBV	Second category of the Extreme Risk	Design awareness programs on topics of GBV for the community	Design of a GBV policy and procedures which should cover all people (stakeholders in the

		and project contractors; Coordinate with the local integrated mechanism for support in matters of prevention and reporting of GBV cases.	project) - ANE, PIU, IPs, and the local community
Demonstrations/tumults/ vandalism	Last category of the High Risk	The internal security manager or consultant must close liaison with local authorities (police and military); Implementation of Grievance Redress Mechanism (GRM); Training on procedures to follow in a tumult's situation	To reduce the consequence of this risk, the following measures should be observed: Adherence to emergency response procedures for applicable scenarios; Efficient communication process for all involved parties; Training people on what to do and not to do in these situations; Conducting simulation exercises; Placing first aid kits in strategic locations; Definition of safe havens.
Fire	Lower category of the extreme Risk	Training on procedures to follow in a fire situation; simulation exercises on procedures to follow in a fire situation; Train staff in firefighting, first aid, and emergency management.	Ensure the existence of fire prevention and combat equipment in contractor camps; Ensure the presence of visible emergency contacts;
Traffic Accidents	Last category of the High Risk	Ensure that all vehicles have undergone preventive maintenance;	Ensure compliance with travel and communication plans;

		Travel by day where possible and with a 4x4 enabled vehicle; Test and ensure the operability of communication equipment; All drivers must undergo defensive driving training; All vehicles must have an emergency kit; Ensure daily checklist vehicles.	
Natural disaster and Health Risk	Last category of the High Risk	Simulation an evacuation exercises on procedures to follow in a natural disaster situation;	Design of an evacuation plan; Design of key risk indicator.
Logistics: Inability to transport materials to the project due to insecurity	Last category of the High Risk	Plan alternative routes that offer greater security, even if they are longer or less efficient – Plan B for logistics; Implement real-time monitoring systems to track transport vehicles; Establish clear communication protocols between drivers, the project command center, and security forces;	Train drivers and transport team in security procedures, emergency response, and attack evasion; Conduct simulation exercises for risk situations.

		Maintain confidentiality regarding transport route details to minimize the risk of information leaks and limit this information to essential personnel only.	
Social: Conflicts with the community related to land access and unemployment	Last category of the High Risk	Create engagement with the community and include community members in the decision-making process. Empower communities and prioritize hiring local workers. Implement Conflict Resolution Mechanisms.	
Infiltration of insurgents among the project workers	Lower category of the extreme Risk	Implement background check procedures for all workers, contractors, and subcontractors. Strengthen security in camps with controlled access and constant surveillance. Implement intelligence and monitoring systems to identify suspicious activities and potential infiltrators.	Regular training on recognizing signs of infiltration and personal security procedures.

Table 5 – Risk treats measures

6.2 Security Risk Treatment According to Key Risk Indicator

Risk	Security Procedures	
Insurgents' **attacks**	Travel policy for critical areas: Observance the recommendations from the security area according to Key Risk Indicator (KRI); Travel conducted with the escort of local forces Observance of minimum security standards for vehicles (bulletproof vehicles) for critical groups, individuals in high-risk areas (bulletproof vests), infrastructure, and assets design by Internal Security Risk Manager or Security Risk Consultant; Formalization of the relationship with local authorities. The formalization of the relationship with local authorities should be observed through an MoU that includes, among other aspects: Non-violation of human rights and negative impact on communities; Clear definition of roles, responsibilities, and compliance requirements with international standards and local regulations; Training and capacity building on human rights, and protocols to address risks and ensure the security of all project stakeholders; Compliance with defined ethical and legal standards. All project employees traveling to the districts must have a portable first aid kit and a first aid bag in the vehicle. They should also have a survival kit; Medical evacuation plan; The emergency contact list and the communication tree should be available and tested frequently; Observance Hostile Environment Awareness Training (HEAT) Observance emergency response procedure: Comply with the local force guidance at the attack site. In case of absence, follow the recommendations below: • Run; • Hide; and • Survive	
	Quissanga District	Due to the criticality of this district concerning the risk under analysis, the following procedures should be added: Definition of the

		frequency of contact during the travel route; Provision of a satellite phone; Checking the security checklist before departure, monitoring staff/vehicle movements.
	Macomia District	Due to the criticality of this district concerning the risk under analysis, the following procedures should be added: Definition of the frequency of contact during the travel route; Provision of a satellite phone; Checking the security checklist before departure, monitoring staff/vehicle movements.
	Mecufi District	Follow the recommended procedures
	Ancuabe District	Follow the recommended procedures
	Palma District	Due to the criticality of this district concerning the risk under analysis, the following procedures should be added: Definition of the frequency of contact during the travel route; Provision of a satellite phone; Checking the security checklist before departure, monitoring staff/vehicle movements.
	Mueda District	Follow the recommended procedures
	Muidumbe	Due to the criticality of this district concerning the risk under analysis, the following procedures should be added: Definition of the frequency of contact during the travel route; Provision of a satellite phone; Checking the security checklist before departure, monitoring staff/vehicle movements.
	Districts from Nampula	In districts with no history of attacks, the use of armored vehicles and bulletproof vests will

		depend on the recommendation of the Project Security Risk Manager or Security Consultant
	Districts from Niassa	In districts with no history of attacks, the use of armored vehicles and bulletproof vests will depend on the recommendation of the Project Security Risk Manager or Security Consultant

Table 6 – Security Risk treatment insurgent's attack

Risk	Security Procedures	
Kidnapping	Training and simulation exercises on procedures to follow in a kidnapping situation; Training to avoid kidnappings, including but not limited to the following topics: Operational security – sensitive information and route management; How to maintain a low profile; Techniques for escaping a captivity situation; Use of codes and secure communication systems; How to handle and avoid violence from the kidnapper. Assigning panic buttons and gps equipment to individuals with specific profiles.	
	Quissanga District	Follow the recommended procedures
	Macomia District	Follow the recommended procedures
	Mecufi District	Follow the recommended procedures
	Ancuabe District	Follow the recommended procedures
	Palma District	Follow the recommended procedures
	Mueda District	Follow the recommended procedures
	Muidumbe	Follow the recommended procedures
	Districts from Nampula	Follow the recommended procedures
	Districts from Niassa	Follow the recommended procedures

Table 7 – Security Risk treatment Kidnapping

Risk	**Security Procedures**
	The internal security manager or consultant must close liaison with local authorities (police and military); Training on procedures to follow in a theft/assault situation; Training to avoid robbery/assault situations, including but not limited to the following topics: Identification of suspicious situations/people;

Theft/Assault	Personal security and the use of personal security apps; Security at home, work, and of personal belongings; Protocols for managing valuable items; Project Perimeter Security Control; Storage and Control of Materials; Access control procedure Physical security (private company security guards).	
	Quissanga District	Follow the recommended procedures
	Macomia District	Follow the recommended procedures
	Mecufi District	Follow the recommended procedures
	Ancuabe District	Follow the recommended procedures
	Palma District	Follow the recommended procedures
	Mueda District	Follow the recommended procedures
	Muidumbe	Follow the recommended procedures
	Districts from Nampula	Follow the recommended procedures
	Districts from Niassa	Follow the recommended procedures

Table 8 – Security Risk Treatment Theft/Assault

Risk	Security Procedures	
GBV	Design awareness programs on topics of GBV for the ANE, PIU, IPs, community and project contractors; Coordinate with the local integrated mechanism for support in matters of prevention and reporting of GBV cases.	
	Quissanga District	Follow the recommended procedures
	Macomia District	Follow the recommended procedures
	Mecufi District	Follow the recommended procedures
	Ancuabe District	Follow the recommended procedures
	Palma District	Follow the recommended procedures
	Mueda District	Follow the recommended procedures
	Muidumbe	Follow the recommended procedures
	Districts from Nampula	Follow the recommended procedures
	Districts from Niassa	Follow the recommended procedures

Table 9 – Security Risk treatment GBV

Risk	**Security Procedures**
	The internal security manager or consultant must close liaison with local authorities (police and military);

<table>
<tr>
<td>Demonstrations/tumults/vandalism</td>
<td>To reduce the consequence of this risk, the following measures should be observed:
Adherence to emergency response procedures for applicable scenarios;
Efficient communication process for all involved parties;
Training people on what to do and not to do in these situations;
Conducting simulation exercises;
Placing first aid kits in strategic locations;
Definition of safe havens.
Training on procedures to follow in a tumults situation.
Those plans must be in place:
• Crisis management plan;
• Business continuity plan;
• Business recovery plan
<table>
<tr><td>Quissanga District</td><td>Follow the recommended procedures</td></tr>
<tr><td>Macomia District</td><td>Follow the recommended procedures</td></tr>
<tr><td>Mecufi District</td><td>Follow the recommended procedures</td></tr>
<tr><td>Ancuabe District</td><td>Follow the recommended procedures</td></tr>
<tr><td>Palma District</td><td>Follow the recommended procedures</td></tr>
<tr><td>Mueda District</td><td>Follow the recommended procedures</td></tr>
<tr><td>Muidumbe</td><td>Follow the recommended procedures</td></tr>
<tr><td>Districts from Nampula</td><td>Follow the recommended procedures</td></tr>
<tr><td>Districts from Niassa</td><td>Follow the recommended procedures</td></tr>
</table>
</td>
</tr>
</table>

Table 10 – Security Risk treatment Demonstrations/tumults/vandalism

Risk	Security Procedures
	Training on procedures to follow in a fire situation;

Fire	Simulation exercises on procedures to follow in a fire situation; Train staff in firefighting, first aid, and emergency management; Ensure the existence of fire prevention and combat equipment in contractor camps; Ensure the presence of visible emergency contacts; Medical Evacuation Plan, must be in place	
	Quissanga District	Follow the recommended procedures
	Macomia District	Follow the recommended procedures
	Mecufi District	Follow the recommended procedures
	Ancuabe District	Follow the recommended procedures
	Palma District	Follow the recommended procedures
	Mueda District	Follow the recommended procedures
	Muidumbe	Follow the recommended procedures
	Districts from Nampula	Follow the recommended procedures
	Districts from Niassa	Follow the recommended procedures

Table 11 – Security Risk treatment Fire

Risk	Security Procedures	
Road Traffic Accidents	Ensure that all vehicles have undergone preventive maintenance; Travel by day where possible and with a 4x4-enabled vehicle; Test and ensure the operability of communication equipment; All drivers must undergo defensive driving training; All vehicles must have an emergency kit; Ensure daily checklist of vehicles (see below) ; Ensure that all Project vehicles circulates during daylight only (until 6h00 PM)	
	Quissanga District	Follow the recommended procedures
	Macomia District	Follow the recommended procedures
	Mecufi District	Follow the recommended procedures
	Ancuabe District	Follow the recommended procedures
	Palma District	Follow the recommended procedures
	Mueda District	Follow the recommended procedures
	Muidumbe	Follow the recommended procedures
	Districts from Nampula	Follow the recommended procedures

	Districts from Niassa	Follow the recommended procedures

Table 12 – Security Risk treatment Road Traffic Accident

6.3 Vehicles Daily checklist

Items	Description	S	N	N/A	Remarks/Measures
1	Seat belt perfect and working?				
2	Tyres in good condition? Describe situation!				
3	Wheels and tyres in good condition?				
4	Break working perfectly?				
5	Steering in good condition?				
6	Windshield wiper working well?				
7	Dashboard Instruments?				
8	Rear view mirror in perfect condition?				
9	Horn working?				
10	Headlight working well?				
11	Arrows working?				
12	Alert working?				
13	Rear View Light and Rear-View Alarm working?				
14	Brake light working?				
15	Extinguisher in good condition and on time				
16	Battery, ok?				
22	Oil, Water and/or Fuel leakage?				
23	Fuel cap, is it there and is it ok?				
24	Noise level?				
25	Seats in good condition?				
26	Jack and wheel wrench				

Observations: All legal documents (Driving licence, a title deed, car registration, etc) will eventually be required and if they do not exist then the vehicle will be banned immediately.

Table 13 – Vehicles Daily checklist

7. STAKEHOLDER ENGAGEMENT

In order to ensure the effectiveness and acceptance of the security plan, engagement with stakeholders proves to be a critical action, which will underpin the existence of a Stakeholder Engagement Plan for the project. The strategy to be observed for the implementation of the plan throughout the project's lifecycle will follow specific crucial procedures:

- Stakeholder mapping (identification of all stakeholders, including communities);
- Definition of channels and forms of communication;
- Selection of relevant topics in the areas of security, environment, and social aspects and understanding the expectations and needs of stakeholders;
- Creation of security content and measures beneficial to stakeholders;
- Feedback and continuous improvement.

ANE must ensure the hiring of a collaborator or consultant to manage stakeholders.

8. PROJECT GRIEVANCE REDRESS MECHANISM

To ensure additional dialogue and consultations with the beneficiaries and individuals affected by the project, a Project Grievance Redress Mechanism (PGRM) will be implemented through the installation of green lines.

The objectives of the PGRM are:

- Establish a mechanism to receive and process complaints in a timely manner, with special attention to vulnerable groups;
- Support the need for clarification and information;
- Create an effective, transparent, timely, fair, and non-discriminatory system that allows affected individuals to file complaints and avoid litigation;
- Promote social and amicable resolution of complaints and avoid resorting to justice;
- Minimize negative publicity, avoid/minimize delays in the execution of infrastructure works, and;
- Ensure the sustainability of project interventions.

8.1 Principles and values guiding the PGRM

- Accessibility and inclusiveness. The mechanism must be accessible to diverse community stakeholders, including vulnerable groups;
- Community involvement in the design. Stakeholder representatives should be involved in the design of community involvement in the mechanism and have the opportunity to suggest improvements at any time;
- Confidentiality. The anonymity and privacy of complainants (and the recording of complaints) should be preserved when circumstances require it;
- Culturally appropriate and gender-sensitive. The design and operation of the mechanism should take into account the cultural specificities and preferences of communities in the negotiation and resolution of complaints;
- Use of a complaints register to monitor and improve the mechanism. The register can be used to identify trends in complaints and conflicts related to project operations to anticipate problems and propose organizational or operational changes related to the project;
- Identification of a central coordination point. The mechanism and those in charge should be well identified and disclosed to stakeholders;
- Transparent and non-retaliatory. Complaints should be handled in an understandable and transparent process without cost or retaliation;
- Proactive information. Communities should be informed about the judicial and administrative remedies available in the country for conflict resolution at all times;

8.2 Types of complaints to be submitted through the PGRM

- Negative impacts on communities or individuals, which may include financial losses, physical damage, and inconvenience caused by construction or operational activities;
- Security, Health and safety risks resulting from project implementation;
- Negative impacts on the environment, and
- Unacceptable worker behavior, including gender-based violence and sexual abuse and exploitation.

9. SECURITY MANAGEMENT PLAN – GOVERNANCE

9.1 Responsible at the Strategic and Implementation level

Strategic Direction: Project Steering Committee (PSC) – Security Management Decision-Making: ANE - Security Risk Management Strategic Direction of the PSC: Project Implementation Unit (PIU) – Defines specific risk treatment strategies and approves project

activities of implementing partners (PIs). The PIU Security Risk Specialist will have direct support from a security risk management company, which will implement security measures by the PIs and ensure compliance with security protocols by all entities.

Note: The IPs can seek in the market, provided they meet the requirements defined by the PIU Security Risk Specialist. However, the Specialist can provide references, avoiding conflict of interests and considering offer on the market of companies that meet the requirements leaving the IPs to decide.

Daily direction of project security risks: The PIU Security Risk Specialist or Security Risk Consultant – Supports the implementation of security issues at the project level and is responsible for implementing the Security Plan in coordination with the PIU, Implementing Partners (PIs), and contractors. However, all implementers, PIU, PIs, and contractors have the right to decide on the temporary closure of project activities. Permanent withdrawal and closure of project activities can be implemented after discussions between PIU, ANE, and the World Bank. Any early withdrawal of activities must be accompanied by careful stakeholder consultations and management, if possible, given the circumstances.

Decisions will be based on local security risk assessments provided by the Security Risk Management Company. The local security risk assessment will describe the local security environment in the specific area of the site. Then, the threat scenario is adjusted to the specific project activity and location and analyzed in relation to the potential impact on project workers and beneficiaries. This impact scoring will inform decisions made about the temporary or complete suspension of activities.

The PIU will conduct a weekly Security Community of Practice that brings together all security stakeholders, including ANE and all PIs.

9.2 Security Structure

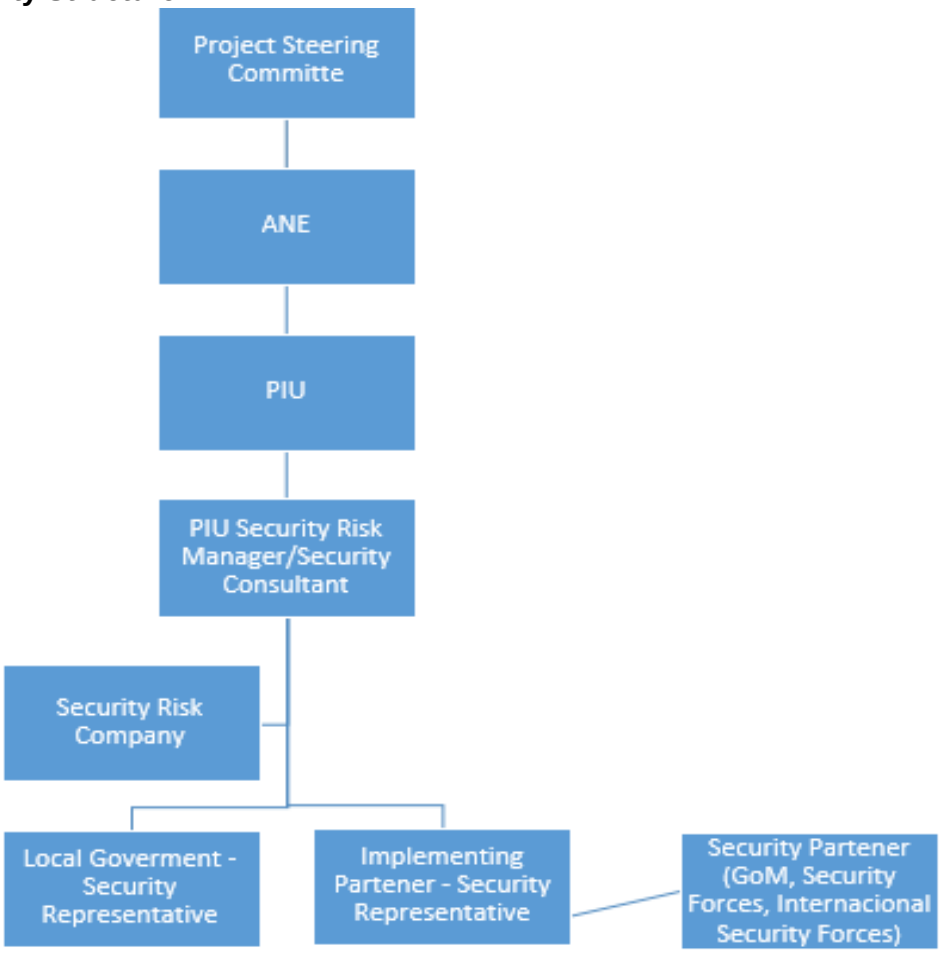


Figure 2 – Security Structure

9.3 Priorities, Roles and Responsibilities

PSC	• Responsible for the strategic security management through the SMP (Security Management Plan); • Conducts an annual review of the SMP. Instructs the PIU on security strategy.
PIU	• Ensures the implementation of the SMP at the local level; • Supervises the activities of the Security Risk Management Company; • Supervises, inspects, and monitors the local implementation of the SMP by IPs; • Ensures the adequacy of local security requirements and budget.
Security Risk Management Company	• Responsible for developing SRA and SMP at the local level; • Produces periodic reports on the results of the Security Risk Assessment (SRA) and SMP implementation; • Provides data for risk-based decision-making on security issues.
IPs	• Develops an action plan based on shared security risk information;

	• Implements security risk treatment and control measures at the operational level; • Submits a budget for security risk treatment; • Authorized to suspend operations based on the severity of threats.

Table 14 – Priorities, Role and Responsibilities

9.4. Security Incident Report Management

A security incident is any significant event, circumstance or change of context that affects the safety and security of personnel, assets, information, infrastructure or projects. A security incident is not only limited to direct events affecting the ANE project, but incidents involving other NGOs (including the UN and security forces, where appropriate) should also be reported. A security incident also includes "near misses" involving project staff, assets and communities.

Security incidents must be reported within 24 hours and directed to the project Security manager/security consultant.

All incidents are recorded and reported. Best practice is to report any incident as soon as possible.

It is important to provide as much information as possible to enable rapid assistance in an event or incident.

Incident reports and security incident analysis are extremely critical for management decisions. In fact, this mechanism allows the project security manager/security consultant, to:

- ✓ Informing employees and others of actual and potential threats in an area of operation;
- ✓ Form the basis for incident mapping and trend analysis in specific contexts;
- ✓ Increase the institutional memory that can be passed on to new employees by informing them of relevant threats;
- ✓ Monitor security and identify practices that require change.

Structure of the preliminary document, must comply with the answers below:

Incident that impacts people

	Required Details
Who, Name(s):	Names of persons involved and country of origin
What, happened	Brief description of what happened, detailed report will follow later.

Where, location:	Where the incident occurred, building, hotel, street, etc.
When:	Time and date of the incident
Injuries:	Mention any injuries sustained or medical assistance required, already called, etc.
What has been done	Police or emergency services contacted, first aid provided, etc.
Call-back contact numbers	Any mobile phone, hotel, friends, helping people, etc.
Security Focal Point/Manager Contact	
Police (National)	Up-to-date contacts
Clinics (Districts)	
Medical/Ambulance Insurance	

Table 15 – Structure security Incident Report

Loss incidents

	Required Details
Current status of the incident:	
Who:	Name of person, e-mail, contact person making the communication
What, happened	Brief description of what happened
Where, location:	Where the incident occurred, business unit
When:	Time and date of the incident
Impact level:	Extreme, high, moderate or low
Actual loss	
Estimated potential loss	
Description of the root cause	
Areas involved/affected	
Resolution of the incident	Up-to-date contacts
Corrective action plan and deadline	
Responsible for the action plan	

Table 16 – Structure security Incident Report: Loss Incident

9.5. Operational Security Procedures

9.5.1Project Perimeter Security Control

- Identify and map the project perimeter (identify boundaries and access/exit areas for people and equipment);
- Develop a project access control plan with a clear definition of the access control process for people and equipment/materials;
- Define the type of verification and screening for people and vehicles;
- Define the patrolling to be observed, including frequency and route;
- Conduct regular training with security personnel to ensure proper access control and treatment of the community wishing to access the project.

9.5.1.1 ***Minimum requirement for perimeter security***:

- Safe perimeter fence, physical barrier, punches;
- Implementation of access control (electronic or manual access control systems, security doors for high security locations, CCTV system and drones within legal limits);
- Adequate lighting;
- Intrusion, alarm and fire detection system;
- Regular/daily assessment of the security situation; and
- Perimeter patrol.

9.5.2 Storage and Control of Materials

- Establish an appropriate storage system for road and bridge construction materials and equipment;
- Ensure material storage according to environmental, health, and safety guidelines;
- Conduct regular inspections to ensure proper storage;
- Provide training on proper storage and material control guidelines and practices.

9.5.3 Information and Communication – Categorization, Treatment, and Control of Sensitive Information

- Define the type of information that should be categorized, treated, and controlled;
- Define the categorization procedure;
- Develop policies and guidelines for information handling and security measures;

- Make continuous adjustments and improvements based on audit results.

9.5.4 Protection of People

Considering people as the organisation's most precious "asset", the project will be premised on safeguarding them first and foremost.

In this context, the following controls will be safeguarded:

- Access control policy;
- Implementation of minimum security standards (security project);
- First aid kit (portable) for all employees with frequent travel and who work in the critical districts, as well as for all drivers;
- Survival kit for all employees who work in areas at high risk of Insurgents' attack;
- Training of employees, as champions, in matters of handling fire extinguishers, first aid and emergency managers, at all districts. Updated every 2 years

9.5.5 Emergency Response Exercises

Emergency response exercises (including, but not limited to, fire, rescue and spill drills) should be conducted to test the effectiveness of emergency procedures and equipment as well as the knowledge and proficiency of all response personnel.

The results of the simulation should be reported to the Security Project Implementer. The aspects to be observed during the simulation can be found below:

Order	Item	Yes	No	N/A	Comment
1	Was the communication clear and audible in your area?				
2	Did employees respond immediately to the notification?				
3	Has energised equipment been switched off by employees?				
4	Did employees go directly to the emergency rendezvous point?				
5	Has the area been completely vacated?				
6	Was the reporting of the emergency done in a timely and orderly manner?				
7	Have employees been accounted for?				

9	Were employees informed of the reason for the evacuation and given the route?				
10	Is the Emergency Response Team contactable?				
General Comments					

Table 17 – Simulation Report Structure

10. IMPLEMENTING PARTNERS SECURITY REQUIREMENTS

The security requirements for implementing partners (IPs) in the project involve several key aspects:

10.1 Procurement

- IPs must respond to the Terms of Reference (TOR) will define their roles and responsibilities, including security responsibilities;
- IPs need to implement specific risk mitigation measures during project activity, and associated costs must be considered in their operational solutions;
- IPs should be prepared for potential changes in the security environment, requiring adjustments to risk mitigation measures, with associated costs being the responsibility of the IP.

10.2 Security Checklist

- A mandatory Security Checklist is part of every IP tender process;
- Discrepancies found during audits may lead to the suspension of project activity or removal of the IP from the contract.

10.3 Activity Security Plan (ASP)

- IPs, after being awarded a contract, must complete an ASP before engaging in project activity;
- The ASP will be evaluated, and IPs failing to meet standards will work with the PIU to implement required risk mitigation measures before project commencement.

10.4 Security Audit Process

- The PIU can demand audits of IP security policies and procedures throughout the contract;

- Audits will follow the Security Checklist format, and IPs failing to possess required documentation may face project activity restrictions or cancellations.

10.5 Monitoring and Evaluation (M&E)

- The PIU will conduct M&E of IP's risk mitigation measures on the ground, documenting results with evidence;
- IPs not implementing measures as described in their ASPs may face project activity restrictions or cancellations.

10.6 Security Exercises

- IPs may be required to conduct tabletop or physical security exercises with security partners to ensure preparedness for extreme events;
- Exercises will be planned collaboratively and run by the Security Risk Management Company on behalf of the PIU.

10.7 Training

- The PIU will provide security training to IPs with identified capability shortfalls;
- Training will cover risk management, including policy and procedure writing, risk assessments, security management plans, and effective risk mitigation measures;
- These requirements aim to ensure that IPs operate in a safe and secure manner, addressing potential security threats during the project lifecycle.

11. SECURITY PARTNERS IN CRRNP PROJECT

11.1 Government of Mozambique (GoM)

- GoM (Local force and Police) engagement and support are crucial for project success in areas with an unstable security environment;
- Support includes intelligence, armored escorts, area security, and rapid response to extreme events;
- PIU facilitates communication between PIU and GoM security organizations, with contact details in Local SMPs;
- IPs should form relationships with local GoM security commanders, reporting engagement as part of the framework;
- Deployment of public security forces must adhere to ES2 on Labor and Working Conditions and ESS4 on Community Health and Safety.

11.2 International Security Forces

- Potentially effective partners, the PIU engages international security forces for support;
- Protocols for assistance requests established at government and local levels.

11.3 Local Militia

- IPs may receive support from local communities, necessitating deconfliction to avoid clashes with official security partners;
- IPs report on local support, and the PIU evaluates situations case by case to ensure proper security levels.

11.4 Private IPs can procure pre-qualified private security companies if needed;

- Private security activities may include guarding, close protection, movement support, tracking, and advisory services;
- PIU conducts prequalification exercises through defined audit processes;
- PIU may provide training and consultancy to upskill private security companies critical to project activity if they don't initially meet required standards.

12. WEEKLY SECURITY COP, PIU TRAVEL POLICY, AND CRISIS MANAGEMENT PLAN

12.1 Weekly Security CoP (Community of Practice)

- Hosted by the PIU Security Risk Management Specialist, attended by Security Risk Management Company, IP Security Reps, and ANE Security Reps;
- Provides a forum for sharing intelligence, discussing security incidents, giving security direction, making requests to GoM security partners, sharing security best practices, addressing IP concerns, and providing feedback to shape internal policy;
- IPs must attend with their nominated security representative. (The full TOR will be shared).

12.2 PIU Travel Policy

- Applies to PIU personnel or those working directly on behalf of the PIU traveling to project sites or visiting GoM Government personnel;
- Informed by Local SRAs, it outlines risk mitigation measures to be adopted during travel on PIU business;
- Risk Management Specialist and Security Risk Management Company. (The policy will be shared).

12.3 Crisis Management Plan

- Acknowledges the potential for crises despite risk mitigation measures in SMP and Travel Policy;
- Defines a crisis as any incident with severe consequences threatening the life or safety of PIU affected personnel. (The CRRNP Crisis Management Plan details crisis response measures will be shared).

References

1. Cabo Ligado Monthly Report: https://www.caboligado.com/monthly-reports
2. Conflito Armado no Norte de Mocambique, 2022, Macalane at all: https://www.iese.ac.mz/wp-content/uploads/2022/01/BB51.pdf
3. Good Practice Note related to Security topics: https://www.worldbank.org
4. International Organization for Standardization. (2019). ISO 31010:2019 Risk management — Risk assessment techniques. Geneva, Switzerland
5. International Organization for Standardization. (2018). ISO 31000:2018 Risk management — Guidelines. Geneva, Switzerland:
6. Mozambique Situation Report: https://reports.unocha.org/en/country/mozambique/
7. Provincial Statistical Yearbook: https://www.ine.gov.mz/estat%C3%ADsticas/-/document_library/pfpz/view/44568
8. UN Basic Principles on the Use of Force and Firearmas by Law Enforcement Officials: Basic Principles on the Use of Force and Firearms by Law Enforcement Officials | OHCHR
9. UN Code of Conduct for Law Enforcement Officials: Code of Conduct for Law Enforcement Officials | OHCHR World Bank Open Data: https://data.worldbank.org/country/MZ

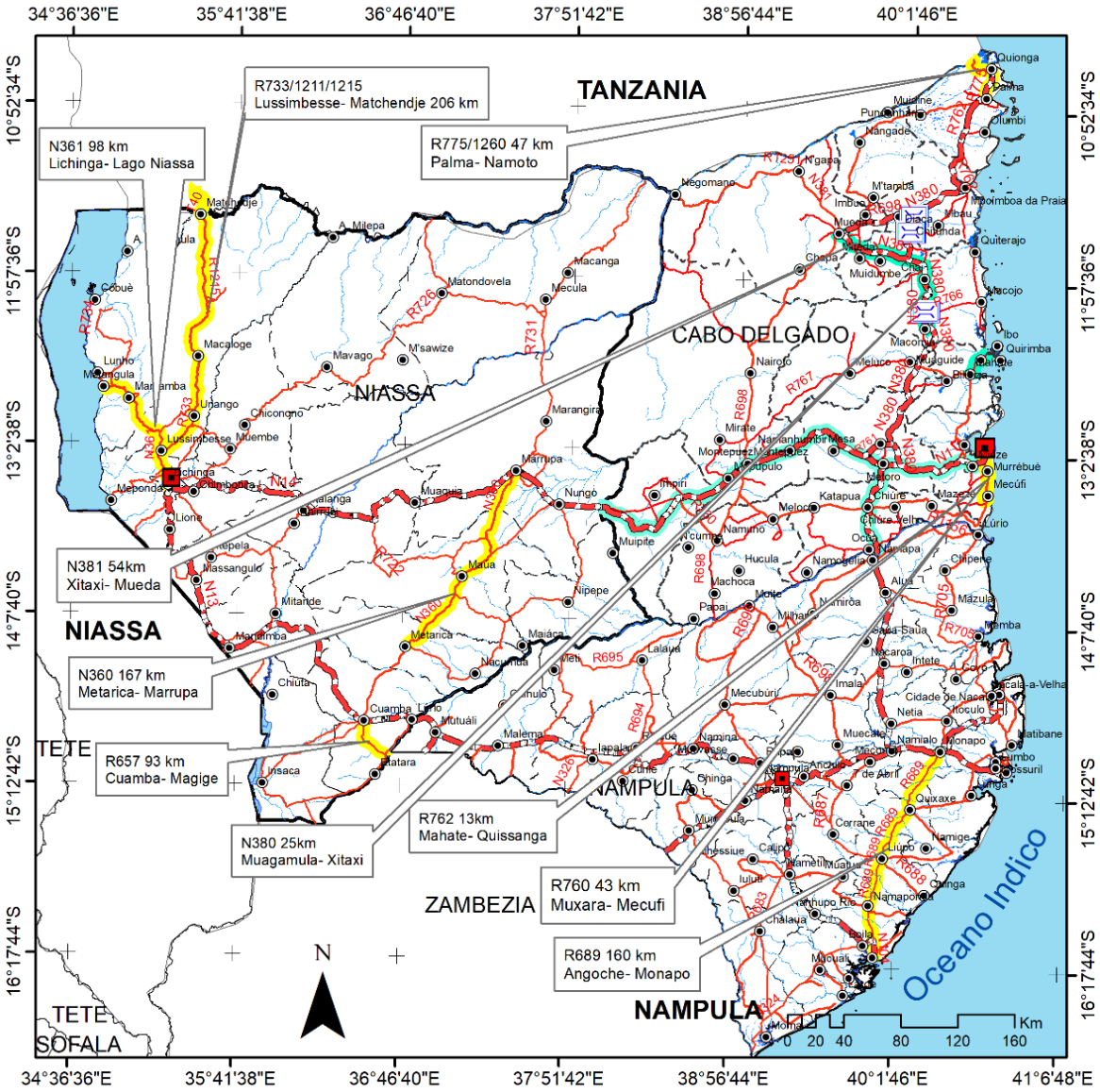
APPENDIX

APPENDIX 1

TERMS OF REFERENCE FOR SECURITY RISK MANAGEMENT SPECIALIST – SECURITY OFFICER – SECURITY REPRESENTATIVE (IP's)

1. Project Description

The project objective is to enhance climate-resilient, safe and sustainable road connectivity in the Northern provinces of Mozambique, namely Cabo Delgado, Niassa and Nampula. It will target the upgrading, rehabilitation, and maintenance of selected secondary and tertiary roads, as well as the construction and rehabilitation of bridges in the secondary road network and installation of bailey bridges in the tertiary road network.



2. Area covered by the project

Province	Road to be intervened	Road section	District	Number of communities
Cabo Delgado	R762	Mahate - Quissanga	Quissanga	2
Cabo Delgado	R762	Mahate - Quissanga	Macomia	1
Cabo Delgado	R760	Muchara - Mecufi	Mecufi	5
Cabo Delgado	R760	Muchara - Mecufi	Ancuabe	5
Cabo Delgado	R775/1260	Palma - Namoto	Palma	4

Cabo Delgado	N380	Muagamula - Mueda	Mueda	2
Cabo Delgado	N380	Muagamula - Mueda	Muidumbe	8
Nampula	R689	Angoche - Monapo	Angoche	6
Nampula	R689	Angoche - Monapo	Mogincual	10
Nampula	R689	Angoche - Monapo	Monapo	3
Niassa	R657	Magige - Cuamba	Cuamba	17
Niassa	N360	Metarica - Marupa	Metarica	4
Niassa	N360	Metarica - Marupa	Maua	6
Niassa	N360	Metarica - Marupa	Marupa	3
Niassa	N361	Lichinga - Lago Niassa	Lichinga	3
Niassa	N361	Lichinga - Lago Niassa	Sanga	8
Niassa	N361	Lichinga - Lago Niassa	Lago	5
Niassa	R733	Lussimbesse - Matchedje	Sanga	17
		Total	**18**	**109**

3. Positions details

Function	**Representation**	**Location**
Security Specialist	PIU	Cabo Delgado, Nampula and Niassa. Based in Pemba
Security Officer	PIU	Nampula
Security Officer	PIU	Niassa
Security Representative	IP	Cabo Delgado

Security Representative	IP	Nampula
Security Representative	IP	Niassa

A) Scope of Services - Security Specialist

Overall Scope of Work

To hire a Security Specialist to implement and manage the Security Management Plan (SMP) of the ANE in the provinces of Cabo Delgado, Nampula, and Niassa, ensuring the safety of people, assets, and infrastructure. The overall scope of this consultancy is to hire a Security Specialist to provide technical support and assistance to the ANE in the implementation of:

- Plans, processes, and security procedures with an emphasis on the Security Management Plan for the ANE project in Cabo Delgado, Nampula, and Niassa;
- Ensuring the safety of people, assets, and infrastructure;
- Assisting and advising the ANE on all security matters related to or impacting the project.

Responsibilities:

The Security Specialist will be responsible for creating and maintaining a safe environment for everyone involved in the Climate Resilient Roads for the North Project (CRRNP) of the ANE, through the implementation of effective security measures, risk management, and coordination with various stakeholders.

Implementation and Monitoring:

- Ensure strict compliance with the implementation of security policies, plans, procedures, and processes;
- Respond quickly to emergencies and provide flexible and adaptive responses to crisis situations;
- Implement and monitor the Security Management Plan (SMP) at all project sites;
- Ensure compliance with procedures and safety standards;
- Oversee the activities of contracted security companies and implementation partners;
- Respond effectively to security incidents.

Risk Management:

- Conduct the risk assessment process (identify, analyze, and evaluate) periodically;
- Develop and implement risk mitigation strategies;
- Analyze trends and identify emerging threats;
- Develop contingency and disaster recovery plans.

Planning and Analysis: Develop security plans, analyze trends, and forecast future risks.

Coordination and Communication:

- Coordinate actions with government agencies, security forces, and other stakeholders;
- Advise the project team and all stakeholders on security issues and keep everyone informed about the situation;
- Develop reports and presentations on the security situation.

Training and Awareness:

- Develop and implement security training programs for all stakeholders;
- Promote security awareness among all project stakeholders;
- Conduct security simulation exercises for all project workers and stakeholders.

Technical Support:

- Provide technical support for the implementation of security measures;
- Analyze data and relevant information for decision-making.

Collaboration: Work together with various stakeholders, such as government, local communities, armed forces (national and international), and contractors.

Reporting: Prepare incident reports, weekly and monthly reports, give presentations, and participate in weekly security meetings.

Qualifications and Experience: The Consultant should have the following qualifications and experience:

- Degree in security management, risk or disaster management, emergency preparedness, criminal justice, law, or a related security field, or formal multi-year

education in Security Management, such as military, police or national security, command. Formal training in security risk management would be an advantage;

- Solid knowledge of ISO 31000 (Risk Management);
- At least 8 years of experience;
- Knowledge of security standards and legislation;
- Leadership, communication, and problem-solving skills.

B) Scope of Services - Security Officers

Description of the Functions of Security Officers for Nampula and Niassa

Security Officers in Nampula and Niassa will be the eyes and ears of the Security Specialist in their respective provinces, ensuring the day-to-day execution of security strategies and adapting them to local realities.

Considering that the Security Specialist will be based in Cabo Delgado and will have an overall view of the project, Security Officers in the provinces of Nampula and Niassa should have a more operational role, reporting directly to the Specialist and implementing security guidelines within the scope of their respective provinces.

Note: Security Officers should have the autonomy to make decisions within the scope of their responsibilities, but always in accordance with the guidelines established by the Security Specialist.

Responsibilities of Security Officers:

Local Implementation: Ensure the effective implementation of security plans and procedures defined by the Security Specialist, adapting them to the specificities of each province.

Monitoring: Continuously monitor security conditions in the operational areas, identifying and reporting any incidents or potential threats.

Local Coordination: Coordinate activities with local government, local security teams, including contracted security companies.

Training: Conduct security training for local staff and partners, aiming to increase awareness of risks and procedures.

Reporting: Prepare periodic reports on the security situation in their province, including incidents, measures taken, and recommendations.

Communication: Maintain constant communication with the Security Specialist, informing about any relevant developments and requesting guidance when necessary.

Stakeholder Relations: Establish and maintain relationships with local authorities, communities, and other stakeholders, aiming to ensure collaboration and support for the implementation of security measures.

Incident Management: Respond to security incidents quickly and effectively, following established protocols.

Verification and Audit: Conduct periodic verifications of implemented security measures, ensuring compliance with established standards.

Skills and Qualifications:

The Consultant should have the following qualifications and experience:

- Degree in security management, risk or disaster management, emergency preparedness, criminal justice, law, or a related security field, or formal multi-year education in Security Management, such as military, police or national security, command;
- Solid knowledge of ISO 31000 (Risk Management);
- At least 5 years of experience in security management;
- Knowledge of security management and standard operating procedures (SOPs);
- Experience in field work in challenging environments;
- Communication and interpersonal skills;
- Knowledge of local legislation and security contexts in the provinces of Nampula and Niassa;
- Fluency in Portuguese and, preferably, other local languages.

C) Scope of Services - Safety Representatives (Safety Officers of Contracted Companies)

Responsibilities of Safety Representatives

Safety representatives of contracted companies working on the ANE project in the provinces of Cabo Delgado, Nampula, and Niassa play a crucial role in ensuring the safety of operations. Their responsibilities are directly linked to the implementation of security measures established by the Security Specialist and Security Officers, but with a more specific focus on the activities of the contracted company.

Primary Responsibilities:

Compliance with Safety Standards: Ensure that all activities of the contracted company are carried out in accordance with safety standards established by the ANE, the Security Specialist, and applicable national and international standards.

Personnel Training: Ensure that all employees of the contracted company receive adequate safety training, including emergency procedures, use of personal protective equipment (PPE), and awareness of the project's specific risks.

Risk Management: Identify, assess, and control the specific risks of the contracted company's activities, implementing appropriate mitigation measures.

Incident Investigation: Investigate all security incidents that occur during the contracted company's operations, preparing detailed reports and implementing corrective actions.

Reporting: Prepare periodic reports on the safety status of the contracted company's operations, including performance indicators and accident statistics.

Coordination with the ANE Security Team: Maintain constant communication with the Security Specialist and Security Officers, reporting any incidents or unsafe conditions and requesting guidance when necessary.

Cooperation with Other Contracted Companies: Collaborate with safety representatives of other contracted companies to ensure the safety of all operations on the project.

Ensuring the Safety of Equipment and Materials: Ensure the safety of all equipment and materials used by the contracted company, including protection against theft and damage.

Specific Responsibilities According to the Nature of the Contracted Company:

Construction Companies: Ensure safety at construction sites, including the correct use of equipment, signage of risk areas, and worker protection.

Transportation Companies: Ensure safety in the transportation of personnel and materials, including checking vehicle conditions and the use of personal protective equipment.

Supply Companies: Ensure safety during the delivery and storage of materials, including access control to storage areas.

APPENDIX 2

CRISES MANAGEMENT PLAN

Crises Management Plan

As previously outlined in point 12.3 of the SMP, but presented here with greater specificity.

CMP - Defines a crisis as any incident with severe consequences that threatens the life or safety of UIP-affected personnel and acknowledges the potential for crises, even with risk mitigation measures established in the SMP and Travel Policy.

Objectives

1. ***Ensure Safety and Security***: Protect the lives and safety of all involved in the project;
2. ***Minimize the Impact of Crises***: Reduce the negative impact of any crisis on the project's operations;
3. ***Coordinate Effective Responses***: Ensure a coordinated and effective response to any crisis incident.

Crisis Management Structure

Considering that the security risks (previously mapped and with treatment measures presented in the SMP) are threats that may occur in the present project, thus transforming into a crisis scenario (materialization of the risk with negative effects for the project), the crisis management structure follows below.

Crisis Management Committee (CMC):

Composed of representatives from the PIU, contractors, IPs, Project Liaison Committee (PLC) and community leaders.

Crisis Coordinator:

Designated to lead the implementation of the CMP and coordinate response actions.

Crises Response Team (CRT):

It will be composed of professionals specialized in areas such as security, first aid, negotiation, and communication. The team will be responsible for implementing the actions defined by the crisis committee.

The specific functions of a crisis management team may vary depending on the nature of the crisis and the specific circumstances. However, it is always essential to ensure compliance with certain critical requirements: diversity of skills, effective communication, clarity of roles, training/simulations, and continuous planning.

Key roles within a crisis management team include:

Team Leader/Coordinator: Defines the strategy, makes decisions, and coordinates the team's actions.

Communications Officer: Serves as the primary point of contact with senior management, other teams, and external parties.

Security Specialist/Coordinator:

- Assesses physical and security risks, and implements measures to protect people (employees, contractors, and the surrounding community), facilities, and assets;
- coordinates with local authorities (police, fire department) and other security specialists;
- oversees compliance with security protocols such as evacuations, lockdowns, and the use of security systems;
- ensures that facilities are secure and free from threats, minimizing risks during a crisis.

Risk Management Specialist: Identifies, analyses, and assesses potential risks, and develops plans to address/mitigate the impacts of risks.

Operations Specialist: Coordinates the operational actions necessary to resolve the crisis and ensures logistics management.

Human Resources Specialist: Keeps employees informed about the crisis and measures taken, and provides emotional and psychological support to employees affected by the crisis.

Information Technology Specialist: Ensures the security of the project's systems and data.

Crisis Management Phases:

Preparation:

- Establish a clear communication plan and define the communication channels to be used during a crisis;
- Train employees in safety procedures and emergency response;
- Maintain constant contact with local authorities and other stakeholders;
- Monitor the security situation in the area of operations and conduct crisis simulations.

Containment:

- Upon identifying a crisis incident, immediately activate the response plan and notify the crisis committee;
- Prioritize the safety of all involved and take measures to isolate the incident area;
- Establish contact with local authorities and request assistance, if necessary;
- Initiate an investigation into the incident to determine the cause and extent of damage.

Recovery:

- Implement measures to restore project operations, ensuring the safety of employees and local communities;
- Provide psychological and emotional support to employees affected by the incident;
- Communicate transparently with stakeholders about the incident and recovery measures:
- Conduct a thorough analysis of the incident to identify lessons learned and improve the crisis management plan.

Types of Crises and Response Plans

Types of Crises	**Crisis Response Plans**
Insurgent Attacks: Response to armed attacks against workers, facilities, or local residents	***Early Detection and Warning:*** Early warning systems and monitoring to identify imminent threats;

	Facility Protection: Strengthening facilities and using barricades and safe shelters; ***Immediate Response:*** Mobilization of armed escorts and safe evacuation to predetermined locations.
Kidnappings: Procedures for responding to kidnappings of workers or local residents	***Prevention:*** Situational awareness training and operational security training; ***Negotiation and Rescue:*** Procedures for communicating with kidnappers and coordinating with security forces for rescue operations; ***Post-Incident Support:*** Medical and psychological assistance for victims.
Theft/Robbery: Responses to incidents of theft or robbery in the operational areas	***Risk Minimization:*** Theft prevention training and strategies to minimize risk exposure; ***Incident Response:*** Immediate communication procedures and security mobilization; ***Incident Reporting:*** Detailed documentation and investigation of incidents.
Demonstrations/Riots: Management of protests, demonstrations, or riots that may affect project operations	***Conflict Monitoring:*** Use of alert systems to identify potential conflict points; ***Community Engagement:*** Open communication with community leaders and PLC to mitigate tensions;

	Evacuation Procedures: Safe routes and shelters for evacuating workers and residents in case of riots.
Logistics Disruptions: Inability to transport materials to the project due to insecurity	***Contingency Planning:*** Development of alternative supply routes and storage facilities; ***Security Escorts:*** Providing armed escorts for convoys transporting materials.
Social Conflicts: Conflicts with the community related to land access, SEA/SH and unemployment	***Community Engagement:*** Ongoing dialogue with community leaders and PLC to address grievances and build trust; ***Conflict Resolution:*** Training in mediation and negotiation skills.
Insurgent Infiltration: Infiltration of insurgents among project workers	***Background Checks:*** Conducting thorough background checks on all personnel; ***Access Control:*** Implementing strict access control measures to project sites;

Communication during Crises:

Emergency Communication Network: Establishment of a robust and redundant communication network to ensure continuous contact during crises.

Communication Protocol: Clear procedures for incident notification, internal and external communication, and coordination with local authorities.

Training and Simulations:

- ***Regular Training:*** Periodic training for all project personnel on crisis response protocols and personal security. ;

- ***Crisis Simulations:*** Conducting crisis simulations to test the effectiveness of the CMP and improve response capabilities.

The organization and coordination of the trainings will be the responsibility of the PIU Security Specialist or Security Specialist Consultant.

Proposed schedule:

Annual training on crisis management should be conducted for all stakeholders, focusing on updating knowledge and procedures.

Given the security risks in the northern zone, **semi-annual** simulations involving specific teams, such as emergency response teams, should be conducted to test responses to different scenarios.

Ongoing awareness campaigns, internal communications, and small, targeted training sessions should be implemented to keep stakeholders updated on procedures

Monitoring and Evaluation:

Continuous Monitoring: Continuous monitoring of security conditions and the effectiveness of crisis response measures;

Post-Crisis Evaluation: Review and evaluation of crisis responses to identify lessons learned and improve future responses.

Emergency Contact

Name	Position	Contact

APPENDIX 3

SECURITY CHECKLIST

And

MINIMUM SECURITY STANDARDS

Security Checklist:

This security checklist is designed to ensure that all appropriate security measures are in place to protect people (all those involved in the project, including communities, assets, and infrastructure), and its compliance is mandatory.

Activity	Yes	No	Obs.
Risk Assessment			
Regularly assess the security situation in the operational area			
Identify and document potential threats and vulnerabilities			
Review and update the security plan based on risk assessments.			
Physical Protection Measures			
Implement 24-hour monitoring and surveillance systems, including cameras and patrols			
Fortify construction camps and work sites with physical barriers and safe shelters			
All construction sites with first aid kits and pre-designated safe shelters			
Coordination			
Establish communication protocols between the PIU, the contractor, the private security company, and local security forces			
Management of Public and Private Security			
Formalize the relationship with government forces through memoranda of understanding			

Ensure adheres to the Voluntary Principles on Security and Human Rights (VPSHR) and the International Code of Conduct.			
Regularly monitor and review the performance of public and private security to ensure compliance with ESS4 requirements			
Community Engagement			
Maintain regular communication with community leaders to monitor and mitigate potential tensions			
Utilize the Grievance and Resource Mechanism (GRM) for early conflict resolution			
Training and Awareness			
Ensure that all workers and local residents are aware of security protocols and evacuation routes			
Conduct regular training sessions on operational security, situational awareness, and kidnap prevention for all workers			
Train staff on crisis response and evacuation procedures			
Travel Procedures			
Implement a travel policy that includes armed escorts for all travel in high-risk areas			
Conduct security checks before all travel			
Plan alternate travel routes to avoid predictability (Plan a and B)			
Emergency Response			
Establish clear emergency response procedures, including evacuation and first aid			
Conduct regular crisis simulation exercises to test the effectiveness of emergency response plans			
Maintain an updated list of emergency contacts and evacuation routes			
Documentation, Compliance and Auditing			
Maintain detailed records of all security activities and incidents			
Regularly review and update security procedures based on incident reports and risk assessments			

Submit weekly security reports			
Conduct periodic security audits to ensure compliance with international standards and norms			
Ensure that all security policies and procedures are aligned with ESS, VPSHR, and the International Code of Conduct for Private Security Companies			

Minimum Security standards:

Minimum Security standards for the 4 main security pillars in the project (People, Infrastructure, Assets and Operations).

People	**Infrastructure**	**Assets**	**Operations**
Implementation of access control systems, visitor identification, and registration	Implementation of robust fences, physical barriers and high walls	Mapping, monitoring, and surveillance	Regular security and safety assessments, daily security reports – Security checklist
Alarm systems: Intrusion, fire, and emergency First Aid Equipment: First aid kits, basic medical equipment	Perimeter and common area lighting	Implementation of CCTV systems, drones within legal limits, 24-hour surveillance	Coordination: Collaboration with private security, integration with local security forces and other stakeholders
Personal Protective Equipment (PPE)	Designation of reinforced secure shelter areas		Communication Protocols: Establish efficient communication between PIU, contractors, private security, local forces, and other relevant stakeholders
Regular training on security procedures, evacuation, emergency			

response, and simulation exercises			

APPENDIX 4

ACTIVITY SECURITY PLAN

Activity Security Plan

This activity security plan is designed to mitigate risks and protect people (all those involved in the project, including communities, assets, and infrastructure), and its compliance is mandatory.

Objectives:

- Protect the lives and physical integrity of all those involved in the project and local residents;
- Ensure the protection of the project's facilities and equipment;
- Minimize interruptions to the project's operations throughout its lifespan due to security threats;
- Address the risks of insurgents attacks and other related threats;
- Maintain communication and coordination among all stakeholders;
- Establish clear protocols for responding to security incidents.

Exposed Risks:

Ref.	Description
R1	Insurgent attacks
R2	Kidnapping related to Insurgents' attacks
R3	Theft/Assault related to Insurgents' attacks
R4	GBV
R5	Demonstrations/tumults/vandalism related to Insurgents' attacks
R6	Residential Fire related to Insurgents' attacks
R7	Traffic Accidents
R8	Natural disaster and Health Risk
R9	*Logistics*: Inability to transport materials to the project due to insecurity

R10	Social: Conflicts with the community related to land access and unemployment
R11	Infiltration of insurgents among the project workers

Preventive Measures:

Risk Analysis: Conduct a detailed analysis of security risks in the project area;

Physical Security: Implement physical security measures at project facilities, such as fences, gates, surveillance systems, and access control;

Personal Security: Train employees in personal security procedures, including how to react in case of an attack:

Information Security: Protect the confidentiality and integrity of project information;

Communication and Coordination: Establish effective communication channels among all stakeholders;

Community Engagement: Build a trusting relationship with local residents;

Emergency Response Plan: Develop an emergency response plan that includes procedures for dealing with insurgent's attacks, kidnappings, thefts, sabotage, and violent demonstrations.

Resources:

Security Team: Hire a qualified private security team to protect the people, assets and project. Private security activities may include guarding, close protection, movement support, tracking, and advisory services.

GoM (Local force and Police) engagement and support are crucial for project success in areas with an unstable security environment.

Armored Vehicles: Whenever applicable and feasible, use armored vehicles to transport employees and materials in high-risk areas:

Security Technology: Utilize advanced security technology within legal limits, such as video surveillance systems, drones, metal detectors, and X-ray scanners.

Priorities, Roles and Responsibilities

PSC	• Responsible for the strategic security management through the SMP (Security Management Plan); • Conducts an annual review of the SMP. Instructs the PIU on security strategy.
PIU	• Ensures the implementation of the SMP at the local level; • Supervises the activities of the Security Risk Management Company; • Supervises, inspects, and monitors the local implementation of the SMP by IPs; • Ensures the adequacy of local security requirements and budget.
Security Risk Management Company	• Responsible for developing SRA and SMP at the local level; • Produces periodic reports on the results of the Security Risk Assessment (SRA) and SMP implementation; • Provides data for risk-based decision-making on security issues.
IPs	• Develops an action plan based on shared security risk information; • Implements security risk treatment and control measures at the operational level; • Submits a budget for security risk treatment; • Authorized to suspend operations based on the severity of threats.

Reporting, Monitoring, and Evaluation:

- Establish a daily security reporting system to monitor and record security incidents;

- Conduct weekly security meetings to assess the security situation and adjust measures as needed:
- The security activity plan will be monitored and evaluated periodically to ensure its effectiveness;
- The plan will be updated as necessary to reflect changes in threats and risks.

APPENDIX 5

WEEKLY SECURITY CoP (Community of Practice)

Period: [Start Date] - [End Date]

Project: [Project Name]

Localization: [Project Location]

Objective:

This weekly report provides a summary of the security activities carried out on the ANE project. The report aims to inform stakeholders about the security situation in the operational area and the measures taken to ensure the protection of all involved.

Summary of Activities:

Security Situation Monitoring: Continuous monitoring of the security situation in the operational area was carried out through (specify monitoring methods, such as security cameras, patrols, etc.);

Security Training: Security training was provided to (specify groups that received training] on [specify topics covered in training);

Security Meetings: Weekly meetings were held with the security team, contractor, and private security company to discuss the security situation and coordinate actions;

Incident Investigation: (Specify number) security incidents that occurred during the week were investigated. (Briefly describe the incidents and the measures taken);

Community Communication: (Specify communication activities) were carried out with local residents to inform them about the progress of the project and the security measures being taken;

Security Incidents:

Date	Incident Description	Action Taken

Main Risks and Challenges:

Specify the main risks and challenges identified during the week.

Preventive Actions:

Specify the preventive actions that will be taken to mitigate the identified risks and challenges.

Conclusion:

Describe the security situation, such as stable, controlled, etc.

Recommendations:

Specify recommendations to improve project security.

Attachments:

Specify the attachments that accompany the report, such as photos, maps, etc.

Signature:

APPENDIX 6

PIU TRAVEL POLICY

PIU Travel Policy

This PIU Travel Policy applies to PIU personnel or those working directly on behalf of the PIU traveling to project sites or visiting GoM Government personnel.

Considering safety as the top priority, no trip will be authorized without a proper security assessment.

Compliance:

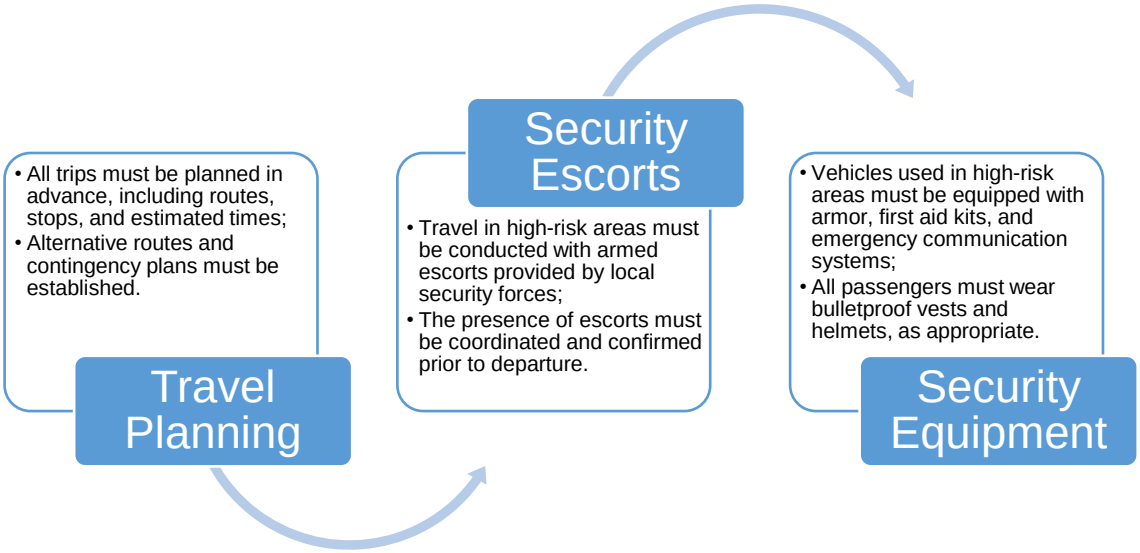
- All travel must be in compliance with established international standards and guidelines, including the International Humanitarian Law, ESS, VPSHR, and the International Code of Conduct;
- All parties involved have a responsibility to comply with this policy and to report any incident or security concern immediately.

Security Assessment and Travel Authorization:

- Prior to any travel, a detailed security assessment must be conducted to identify and mitigate potential risks;
- Assessments should include analysis of risks such as terrorist attacks, kidnappings, robberies, demonstrations, and other hazards:
- All travel must be authorized by the project security management based on the security assessment:
- Unauthorized travel is strictly prohibited

Travel procedures

Nighttime travel is prohibited, except in force majeure situations and with prior authorization.



Training and Awareness

Mandatory Training:

- All individuals must participate in mandatory training on travel safety, situational awareness, and emergency procedures;
- Specific training to prevent kidnappings and minimize exposure to risks should be conducted regularly.

Situational Awareness:

All travelers must be informed about the current security situation, potential threats, and preventive measures before the trip.

Communication:

- Constant communication with the project security team must be maintained throughout the trip;

- Any changes to the itinerary or in case of an emergency, the security team must be informed;
- To report security incidents, the communication channels established by the project must be used.

Continuous Monitoring:

- The travel should be continuously monitored through communication systems and surveillance;
- Intelligence information and security alerts should be regularly analyzed to adjust security measures.

Policy Review:

This policy should be periodically reviewed and adjusted as necessary to respond to changes in security conditions and new threats.