TRADE AND DEVELOPMENT BANK GROUP
GROUPE DE LA BANQUE DE COMMERCE ET DE DÉVELOPPEMENT

Trade and Development Bank Guidance Note on Environment, Social and Governance (ESG) in Fragile and Conflict Affected Areas

October 2025

INTEGRATING & ADVANCING THE REGION
WWW.TDBGROUP.ORG

Table of Contents

1. INTRODUCTION 4
2. SCOPE AND APPLICATION OF THIS GUIDANCE NOTE 6
   2.1. Coverage of Projects and Activities 7
   2.2. Linkages with TDB's ESMS 7
   2.3. Alignment with International Good Practice 8
   2.4. Application in the FCV Context 8
   2.5. Users of the Guidance Note 8
   2.6. Binding Nature and Enforcement 9
3. GUIDANCE NOTE IN ALIGNMENT WITH EXISTING FRAMEWORKS 9
4. UNDERSTANDING THE COUNTRY/PROJECT CONTEXT – IS IT AN FCV ENVIRONMENT? 10
   4.1. Assessment and Classification 10
   4.2. Country/Area Context Appendix 11
   4.3. Methodology and Sources 12
   4.4. Approval and Updates 12
   4.5. Example Appendix 12
5. INSTITUTIONAL ARRANGEMENTS 12
   5.1. Relationship with Co-Financiers 12
   5.2. Role of TDB 13
   5.3. Oversight and Verification 14
   5.4. Implementing Partners and Suppliers 15
   5.5. Security Risk Management within Institutional Arrangements 15
   5.6. Implications for Project Operations 15
6. TDB IMPLEMENTATION UNIT 16
   6.1. Composition and Functions 16
   6.2. Accountability and Reporting 17
7. TDB ENVIRONMENTAL AND SOCIAL MANAGEMENT SYSTEM 17
   7.1. Project Categorisation and Screening 17
   7.2. Due Diligence and Appraisal 19
   7.3. Legal Documentation and Covenants 19
   7.4. Implementation and Monitoring 19
   7.5. Reporting and Completion 20
   7.6. Review and Continuous Improvement 20
8. IFC PERFORMANCE STANDARDS AND PHYSICAL SECURITY 20
   8.1. PS1 — Assessment and Management of Environmental and Social Risks and Impacts 20
   8.2. PS2 — Labor and Working Conditions 20
   8.3. PS4 — Community Health, Safety, and Security (core to security management) 21
   8.4. PS5 — Land Acquisition and Involuntary Resettlement 21
   8.5. PS7 — Indigenous Peoples 21
   8.6. PS8 — Cultural Heritage 21
   8.7. How this integrates with TDB's SRAMP/ESMS 22
9. TDB SECURITY RISK MANAGEMENT SYSTEM IN FCV ENVIRONMENTS 22
   9.1. Purpose and Requirement for Project Level Security Risk Assessment and Management Plan (SRAMP) 22
   9.2. Core Components of a SRAMP 23
      9.2.1. Introduction and Objectives 23
      9.2.2. Methodology and Approach 24
      9.2.3. Security Context and Threat Environment 25
      9.2.4. Security Risk Assessment (SRA) 26
      9.2.5. Security Risk Mitigation Framework 27
      9.2.6. Risk Levels, Escalation, and In-Extremis Events 29

9.2.7. Security Approval Gateways 30
9.2.8. Contractor Security Requirements 30
9.2.9. Security Partners, Monitoring & Evaluation, and PIU Security Procedures 31
9.3. Overlap with TDB's ESMS 32
9.4. Templates and Annexes 33
9.5. Roles and Responsibilities 34
10. USE OF SECURITY FORCES 35
10.1. Determining the Requirement 36
10.2. Categories of Security Forces 36
10.3. Governance Arrangements 36
10.4. Training and Preparedness 37
10.5. Oversight and Community Engagement 37
10.6. Prohibited Practices 37
11. CONSIDERING AND INVESTIGATING ALLEGATIONS OF UNLAWFUL ACTS BY SECURITY FORCES 38
11.1. Anticipating the Risk 38
11.2. Reporting Allegations 38
11.3. Initial Review and Escalation 39
11.4. Investigation Procedures 39
11.5. Remedial Actions 39
11.6. Disclosure and Learning 39
12. MONITORING AND COMPLIANCE 40
12.1. Integration with the ESMS 40
12.2. Contractor Self-Monitoring 40
12.3. PIU Oversight 40
12.4. TDB Supervision 41
12.5. Indicators and Key Performance Measures 41
12.6. Managing Non-Compliance 41
13. SUMMARY 42
APPENDIX A – SUDAN SECURITY CONTEXT 44
ANNEX A - TEMPLATE FOR SRAMP (SECURITY RISK ASSESSMENT AND MANAGEMENT PLAN) 72
ANNEX B – LOCAL SECURITY MANAGEMENT PLAN TEMPLATE 76
ANNEX C – SUPPLIER SECURITY QUESTIONNAIRE 78
ANNEX D – CRISIS MANAGEMENT PLAN (CMP) TEMPLATE 79

Abbreviations and Acronyms

Abbreviation	Full Form
AM	Accountability Mechanism
ASCENT	Accelerating Sustainable and Clean Energy Transformation
AWPB	Annual Work Plan and Budget
BESS	Battery Energy Storage System
BSMA	Bank - Supported Monitoring Agency
CEN	Country Engagement Note
COMESA	Common Market for Eastern and Southern Africa
DA	Designated Account
DFIL	Disbursement and Financial Information Letter
D-MRV	Digital Monitoring, Reporting, and Verification
DRE	Distributed Renewable Energy
ESMS	Environmental and Social Management System
E&S	Environmental and Social
FCV	Fragility, Conflict, and Violence
FM	Financial Management
GOGLA	Global Off-Grid Lighting Association
GRS	Grievance Redress Service
GSMA	Global System for Mobile Communications Association
ICT	Information and Communications Technology
IDEA	Inclusive Digitalization in Eastern and Southern Africa
IDPs	Internally Displaced Persons
INGOs	International Non-Governmental Organizations
IPF	Investment Project Financing
IVA	Independent Verification Agency
M300	Mission 300 initiative
M&E	Monitoring and Evaluation
MNOs	Mobile Network Operators
MPA	Multiphase Programmatic Approach
MSMEs	Micro, Small, and Medium Enterprises
PDO	Project Development Objective
PIU	Project Implementation Unit
PrDO	Program development objective
OGS	off-grid solar
OM	Operations Manual
O&M	Operation and Maintenance
RBF	Results Based Financing
REAF	Regional Energy Access Financing Platform
SEA/SH	Sexual Exploitation, Abuse, and Harassment
TDB	Trade and Development Bank
TDF	Trade and Development Fund
UNDP	United Nations Development Program
UNICEF	United Nations International Children's Emergency Fund
WBG	World Bank Group
WFP	World Food Program

1. Introduction

Projects implemented in fragile, conflict-affected and violent (FCV) environments face material security risks that can directly affect people, assets and delivery continuity. Such settings often combine weak governance, fragmented or politicised security actors, non-state armed groups, pervasive criminality and fluid conflict dynamics. In these conditions, security is not ancillary to operations; it is an operational pre-condition.

The Trade and Development Bank (TDB) manages these risks through a security risk management system that is fully integrated with its Environmental and Social Management System (ESMS) and aligned to the International Finance Corporation's (IFC) Performance Standards as the reference framework (particularly PS1, PS2, PS4, and PS7). Where TDB implements operations with external partners (including the World Bank), this Guidance Note provides the common, auditable approach by which security risks are identified, mitigated, contractually cascaded and monitored. For projects co-financed with multilateral institutions—most notably the World Bank—TDB aligns its ESMS with the requirements of the World Bank Environmental and Social Framework (ESF). The ESF sets the international benchmark, particularly through ESS4 (Community Health and Safety) and related guidance on the use of security forces.

This Note applies across FCV countries. For each country in which TDB operates, a country-specific context profile is prepared and appended (see Section 4). Annex A provides an illustrative example (Sudan) showing the expected depth and sourcing of national and sub-national security analysis.

The Note consolidates requirements, TDB ESMS processes and recognised good practice (e.g., IFC PS4, VPSHR, ICoCA) into practical steps for proportionate, site-level Security Risk Assessments and Management Plans (SRAMPs), contractor obligations, monitoring and incident/crisis procedures.

This Note is a live document and will be developed as TDB operations expand across FCV environments recognising the dynamic nature of such environments and the expanding scope of TDB projects.

The objectives of this Guidance Note are to:

- Provide a consistent, transparent, and practical framework for security risk management across all projects
- Ensure that Participating Private Companies (PPCs), contractors, and partners integrate security risk management into project design and delivery, including through appropriate contractual modalities.
- Cascade security obligations down to all project workers and subcontractors, ensuring that international standards apply across the chain of implementation.

- Strengthen compliance with the World Bank's ESF and TDB's ESMS, with clear accountability mechanisms.
- Safeguard project workers, assets, and communities while minimising unintended negative impacts.
- Provide tools and standards for the preparation of project-specific Security Risk Assessments and Security Management Plans (SMPs).

FCV Environments make these objectives more urgent and more complex. Within FCV environments there is not only direct risks of violence, but also a fragmented governance environment where authority is contested, and communities are divided. Project implementers must navigate a landscape where multiple armed groups, de facto authorities, and criminal networks exercise overlapping control. Communities already displaced by conflict or food insecurity may view projects through a lens of grievance or competition for scarce resources. Without careful and responsible security risk management, development interventions risk exacerbating local tensions or becoming enmeshed in the conflict dynamics themselves. This Guidance Note is therefore both a compliance requirement and an operational necessity: it provides the tools for TDB and its partners to operate responsibly in FCV environments, ensuring that development objectives can still be pursued while prioritising the protection of people and the upholding of international standards.

The preparation of this Guidance Note reflects three main drivers. First, the extreme nature of FCV environments demands a tailored approach: weak governance structures, empowered multiple armed actors, and created risks that cannot be managed through generic templates. Second, the International Finance Corporation's (IFC) Performance Standards (PS), to which TDB ESMS benchmarks itself, requires a structured response: under the IFC PS, security risks must be managed proportionately and in line with human rights principles. Third, TDB has an institutional responsibility: to translate SRM requirements into contractual obligations for its clients and partners, ensuring consistency and accountability across complex delivery chains.

In short, this Guidance Note is necessary to respond to FCV Environments unique risks, to meet TDB ESMS compliance requirements, and to provide TDB with a clear framework for cascading good practice across all projects in FCV Environments.

2. Scope and Application of this Guidance Note

This Guidance Note provides a comprehensive framework for the management of security risks in all TDB–financed projects implemented in Fragile, Conflict and Violence-Affected Countries. It is intended to complement TDB's Environmental and Social Management System (ESMS) ensuring that security considerations are addressed systematically, transparently, and in line with international good practice.

2.1. Coverage of Projects and Activities

The Guidance Note applies to all projects, financing modalities, and implementation arrangements where TDB is financing either directly or through its subsidiaries, e.g. the Trade and Development Fund (TDF). This includes:

- Investment Project Financing (IPF) operations supported by the World Bank or other financing entity
- Results-Based Financing (RBF) mechanisms, where disbursement is linked to verified outputs by Participating Private Companies (PPCs).
- Debt, equity, or grant financing extended by TDB to private sector entities delivering project outputs.
- All tiers of contractual partners, including contractors, sub-contractors, suppliers, independent verification agents, and other delivery agents engaged in project implementation.

The Note applies equally to large-scale infrastructure investments, distributed energy and clean cooking projects, and community-level interventions, recognising that the scale of risks may vary but the underlying obligations to safeguard people and communities remain consistent.

2.2. Linkages with TDB's ESMS

This Guidance Note forms part of the broader E&S governance system under which TDB manages its financing operations. It is not a stand-alone instrument but is embedded within:

- TDB's ESMS, which provides the overarching process for screening, due diligence, categorisation, documentation, and monitoring of E&S risks. As with existing annexes on land acquisition, SEA/SH, and distributed renewable energy, this Note represents a specialised annex focusing on security risk management.
- IFC PS, TDB recognises the IFC PS as the Gold Standard for safeguards and in the SRM context particularly:

    - **PS1 — Assessment and Management of E&S Risks** - Requires clients to establish an ESMS, conduct risk and impact assessments, develop management programs, engage stakeholders, and monitor/adapt performance.
    - **PS2 — Labor and Working Conditions** - Requires fair treatment, safe and healthy working conditions, worker protection, and access to grievance mechanisms.
    - **PS4 — Community Health, Safety, and Security** - Requires assessment and management of risks to communities, including from security arrangements, mandates proportional measures, accountable security personnel, and emergency preparedness.

- **PS5 — Land Acquisition and Involuntary Resettlement** - Requires avoiding forced evictions, minimising displacement, and safeguarding livelihoods and housing security.
- **PS7 — Indigenous Peoples** - Requires respect for cultural rights, meaningful consultation, and Free, Prior, and Informed Consent (FPIC) in certain cases.
- **PS8 — Cultural Heritage** - Requires protecting tangible and intangible cultural heritage from adverse impacts, including theft, vandalism, and misuse.

2.3. Alignment with International Good Practice

The Guidance Note also aligns with internationally recognised standards and frameworks relevant to security and human rights, including:

- World Bank ESF and the Good Practice Handbook on the Use of Security Forces.
- The Voluntary Principles on Security and Human Rights (VPSHR).
- The International Code of Conduct for Private Security Service Providers (ICoCA).
- Relevant United Nations instruments, including the UN Basic Principles on the Use of Force and Firearms by Law Enforcement Officials.

These instruments inform the principles of proportionality, accountability, non-discrimination, and respect for human rights that underpin this Note.

2.4. Application in the FCV Context

The Guidance Note applies a "high-risk baseline": all projects in an FCV environment must assume that security risks are material and must therefore prepare proportionate Security Risk Assessments (SRAs) and Security Management Plans (SMPs) as part of project-level ESMS compliance. The Note applies to:

- Direct project activities, including construction, operations, logistics, and worker accommodation.
- Associated facilities, where security risks may arise from infrastructure linked to project operations (e.g., energy transmission, storage, or transport routes).
- Community interfaces, where project workers, contractors, or security personnel interact with local populations, including vulnerable groups.

2.5. Users of the Guidance Note

The primary users of this Guidance Note are:

- TDB staff and management, including the Coverage Officers, Lending Operations Officers, Credit Risk Officers, Legal Officers and E&S Specialists responsible for appraisal, supervision, and monitoring.

- Participating Private Companies (PPCs) and other contractors, who are required to prepare and implement security management instruments proportionate to project risks.
- Independent Verification Agents (IVAs) and monitoring agents, who must verify compliance with security-related requirements.
- Financing task teams, who will review and ratify the adequacy of security risk management measures as part of ESF compliance.

2.6. Binding Nature and Enforcement

This Guidance Note is advised on all TDB-implemented projects in FCV Environments. Obligations arising under this Note will be incorporated into:

- Contractual agreements with PPCs, contractors, and suppliers;
- Loan or grant agreements signed between TDB and private sector recipients; and
- E&S covenants within project documentation.

Failure to comply with the requirements of this Guidance Note may constitute non-compliance with TDB's ESMS, and may result in suspension of disbursements, contractual remedies, or other corrective actions, as appropriate.

3. Guidance Note in Alignment with Existing Frameworks

This Guidance Note does not create a new set of standards. Rather, it consolidates and contextualises the requirements of three interlocking frameworks that govern the management of security risks in projects implemented by TDB in FCV Environments:

- IFC Performance Standards (PS): The IFC PS, particularly PS1, PS2, PS4, and PS7, establish the baseline obligations for clients to manage environmental, social, and security risks. Security risk management is therefore a compliance requirement under the IFC safeguard system, ensuring that risks to workers, communities, and assets are identified, mitigated, and monitored throughout the project cycle.

- TDB Environmental and Social Management System (ESMS): TDB is responsible for integrating ESF requirements into its institutional systems and cascading them to all its clients and project partners. This Guidance Note forms part of the ESMS, alongside other specialised guidance notes on land acquisition, SEA/SH, and distributed renewable energy. It ensures that security risk management is embedded in TDB's due diligence, appraisal, contracting, and supervision procedures.

- International Good Practice: The Guidance Note is aligned with recognised global standards, including World Bank ESF, the Good Practice Handbook on the Use of Security Forces, the World Bank Good Practice Note on Assessing and Managing the Risks and Impacts of the Use of Security Personnel, the Voluntary Principles on Security and Human Rights (VPSHR), and the International Code of Conduct for Private Security

Providers (ICoCA). These frameworks reinforce principles of proportionality, accountability, and respect for human rights, which are especially critical in Sudan's FCV context.

By bringing these three layers together into a single operational tool, this Guidance Note provides clarity and consistency for all stakeholders. It ensures that project implementers understand their obligations, that TDB has a coherent framework for oversight, and that financing entities can be assured of compliance with both its own standards and international best practice.

4. Understanding the Country/Project Context – is it an FCV Environment?

This Guidance Note applies exclusively to TDB-financed projects operating in fragile, conflict-affected, and violent (FCV) environments. Determining whether a project or country falls within this category is a critical first step in the TDB Environmental and Social Management System (ESMS) and is carried out at the deal origination and initial E and S screening stage.

4.1. Assessment and Classification

At origination, the TDB in-house security experts conduct a structured FCV diagnostic assessment alongside the initial Environmental and Social (E&S) screening. This assessment determines whether the country or specific project area qualifies as an FCV environment.

- The assessment uses a structured question set covering governance, security, violence, social dynamics, and economic stressors.
- The outcome of this process is a clear classification by the security expert on whether the project or country is deemed FCV.
- Only if FCV status is confirmed does this Guidance Note become mandatory for project preparation and implementation.

Below can be found the FCV diagnostic assessment questions

Category	Assessment Question
Governance and Institutions	Are government institutions weak, absent, or corrupt?
	Is the state unable to provide basic services (health, education, policing)?
	Is state authority contested by parallel systems (clans, militias, armed groups)?
	Are elections or political processes widely disputed?
Security Environment	Are armed groups, militias, or insurgencies active?
	Are security forces fragmented, politicised, or under-resourced?
	Is terrorism or violent extremism a credible threat?
	Do criminal networks drive insecurity (smuggling, kidnapping, trafficking)?
	Is there large-scale displacement due to conflict or violence?
Violence and Civilian Impact	Is communal or ethnic violence frequent?
	Are civilians or aid workers often targeted?

	Are protests or unrest regularly violent?
	Is gender-based violence widespread in connection with insecurity?
	Do humanitarian actors face restricted or unsafe conditions?
Political and Social Dynamics	Is government legitimacy contested or unstable?
	Are deep ethnic, religious, or clan divisions driving conflict?
	Do external actors (foreign militaries, PMCs, neighbours) shape security dynamics?
	Are there widespread human rights abuses?
	Is recruitment into armed groups common (including children)?
Economic and Environmental Stressors	Is the economy fragile and highly resource-dependent?
	Are unemployment and lack of livelihoods driving insecurity?
	Are climate shocks (droughts, floods, desertification) fuelling conflict?
	Is food insecurity severe or worsening?
	Does the informal/illicit economy dominate local livelihoods?
International Indicators	Is the country on World Bank/IMF/OECD/UN fragility lists?
	Do UN, INSO, or foreign ministry advisories rate the area high/extreme risk?
	Is there an international peacekeeping or sanctions regime in place?
Local-Level Factors	Is the project area more insecure than national averages?
	Are development projects frequently disrupted by security incidents?
	Do local authorities act autonomously from the state?
	Are aid or project staff regular targets of harassment or abduction?
	Are transport routes often blocked by ambushes, checkpoints, or closures?

4.2. Country/Area Context Appendix

For each FCV country in which TDB operates, the in-house security expert will prepare a Country/Area Context Appendix to accompany this Guidance Note before project mobilisation.

- The Appendix establishes national and sub-national baselines to inform Security Risk Assessments (SRAs), Security Risk Assessment and Management Plans (SRAMPs), and donor/partner clearances.
- Each Appendix must follow a standardised structure and remain a living document, updated periodically.

Minimum contents of the Appendix include:

- **National political-security overview** – governance structures, legitimacy, ongoing conflicts.
- **Threat typology and trends** – armed conflict, communal violence, terrorism, criminality, SEA/SH, cyber threats.
- **Actor/authority mapping** – state security forces, non-state armed groups, traditional authorities, community actors.
- **Sub-national profiles** – risk analysis of provinces/states relevant to project operations.
- **Data sources and citations** – UN, ACLED, INSO, humanitarian reports, national media, and ground intelligence (security providers, local authorities, community liaison).

- **Update protocol and version control** – methodology, date-stamping, and record of revisions.

4.3. Methodology and Sources

The Appendix must **triangulate data** across:

- International datasets (UN, ACLED, INSO, World Bank FCV reports).
- National and local media sources.
- Ground-level inputs from security providers, authorities, and community liaison networks.
  All data must be date-stamped and cross-checked for credibility

4.4. Approval and Updates

- Each Appendix must be **approved by the relevant TDB staff** prior to disbursement.
- Updates are required quarterly or immediately following any material change in the security environment (e.g., outbreak of hostilities, political upheaval, or significant deterioration in law and order).

4.5. Example Appendix

Annex A (Sudan) illustrates the required depth and format of a Country/Area Context Appendix. All future Appendices for other FCV countries must follow the same structure to ensure comparability and consistency across projects.

5. Institutional Arrangements

Effective security risk management in FCV environments requires clear institutional roles and responsibilities between the Trade and Development Bank (TDB), its implementing partners, and co-financing institutions. Security considerations must be embedded from project preparation through implementation and monitoring, ensuring that risk mitigation is proportionate, enforceable, and fully integrated with the TDB Environmental and Social Management System (ESMS).

5.1. Relationship with Co-Financiers

For projects co-financed with multilateral institutions—most notably the World Bank—TDB aligns its ESMS with the requirements of the World Bank Environmental and Social Framework (ESF). The ESF sets the international benchmark, particularly through ESS4 (Community Health and Safety) and related guidance on the use of security forces.

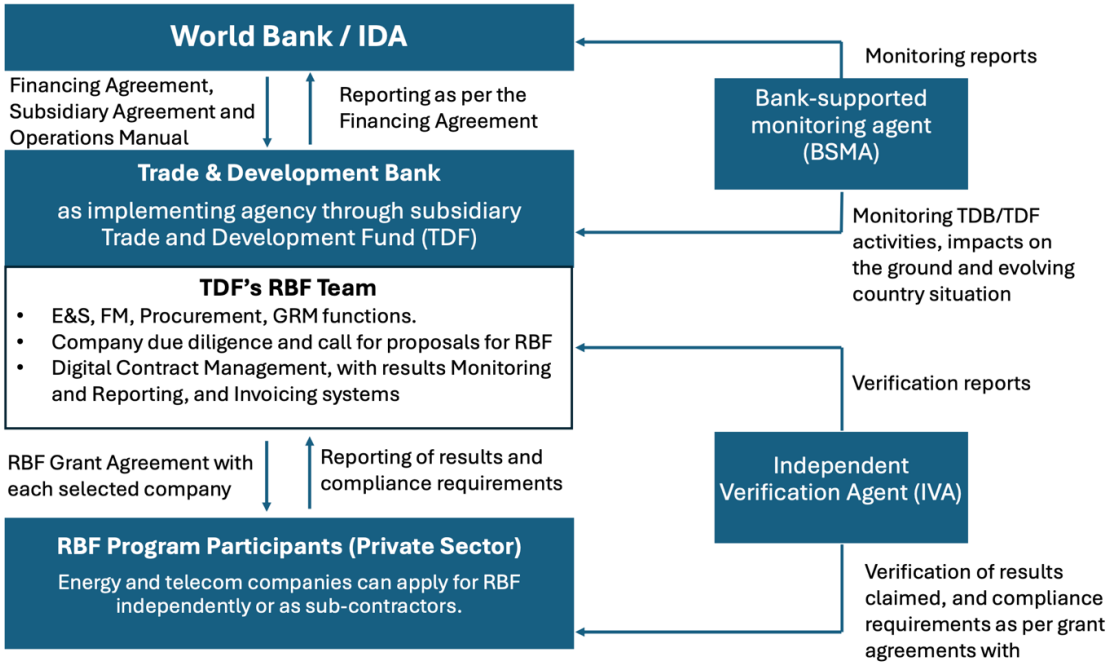
- In practice, this means that any Security Risk Assessment and Management Plan (SRAMP) prepared under TDB oversight must also satisfy World Bank safeguards review and approval processes.
- Where the World Bank is a co-financier, the SRAMP is considered part of the overall safeguards package reviewed by the World Bank regional safeguards team before project effectiveness.
- For projects financed solely by TDB, the same standards apply: SRAMPs are mandatory for all high-risk and substantial-risk projects in FCV contexts, ensuring harmonisation with international good practice.

5.2. Role of TDB

TDB holds overall accountability for ensuring that security risk management is integrated into project design and delivery. Its responsibilities include:

- **Oversight**: Ensuring SRAMPs are developed, approved, and implemented for all FCV projects.
- **Quality Assurance**: Reviewing and clearing SRAMPs through the TDB E&S Unit before financing is disbursed.
- **Capacity Building**: Providing guidance, tools, and training to Project Implementation Units (PIUs) and implementing partners.
- **Monitoring**: Consolidating security monitoring reports from PIUs and ensuring corrective actions are enforced through contractual covenants.

The below diagram shows an example of how World Bank IDA financing flows through TDB/TDF to service providers under Results-Based Financing. Independent Verification Agents confirm results before disbursement, while a Bank-Supported Monitoring Agent oversees compliance. This structure ensures fiduciary, E&S, and security risk management standards are upheld without direct government involvement.



RBF Grant Agreement with each company includes compliance requirements for environmental and social, fiduciary requirements, data reporting, invoicing, payment conditions and legal conditions for disbursement.

This model reflects a deliberate shift toward private-sector-led delivery of services (e.g. renewable energy, telecommunications, agricultural processing), with TDB acting as both financier and risk manager. For example, under the Sudan Energy and Digital Access Project (ASCENT), TDB was the direct recipient of an IDA grant and cascaded responsibilities to private companies via RBF grant agreements. While ASCENT is one illustrative case, the same structure applies across all World Bank–TDB engagements in Sudan which is an FCV environment.

5.3. Oversight and Verification

Given the absence of state-led oversight, the example institutional model above incorporates multiple layers of independent verification:

- Independent Verification Agents (IVAs): contracted by TDB/TDF to confirm that private service providers have delivered agreed outputs before disbursements are released.
- Bank-Supported Monitoring Agent (BSMA): directly contracted by the World Bank to verify both TDB's performance and the integrity of results on the ground.
- Subsidiary Agreements: between TDB and TDF, which allocate responsibilities and ensure that procurement, fiduciary controls, legal frameworks, and E&S management functions are applied consistently across all activities.

This dual-verification framework is particularly critical in fragile and conflict-affected contexts (FCV), where traditional government monitoring structures are absent. In other FCV environments and with other financing partners TDB must look to replicate this level of oversight and verification.

5.4. Implementing Partners and Suppliers

Since TDB does not itself directly implement works or activities, all security obligations must be **cascaded contractually** to implementing partners and suppliers.

- Contractors are required to prepare site-specific LSMPs in response to PIU-approved SRAs.
- Activity-based subcontractors (e.g., survey teams, transport providers) must prepare Activity Security Plans (ASP) for discrete high-risk operations.
- Compliance with SRAMP requirements must be included in all contracts and procurement packages, with clear penalties for non-performance.

5.5. Security Risk Management within Institutional Arrangements

Security risk management forms a distinct and integral component of TDB's ESMS. Under its financing agreements, TDB must:

- Conduct Security Risk Assessments (SRAs) and prepare Security Management Plans (SMPs) proportional to context-specific risks.
- Ensure that all security arrangements (whether provided by public forces, private companies, or community-based mechanisms) are consistent with:

  ✓ IFC Performance Standards
  ✓ the Voluntary Principles on Security and Human Rights (VPSHR); and
  ✓ good international industry practice, including the International Code of Conduct Association (ICoCA)standards.
  ✓ And, where relevant, the WB Environmental and Social Standards

- Establish procedures for the screening, training, and oversight of contracted security personnel, ensuring the avoidance of human rights abuses.
- Report all serious security-related incidents (e.g. civilian harm, unlawful use of force, SEA/SH) to the co-financiers within agreed timelines.
- Apply corrective actions, document lessons learned and integrate findings into continuous ESMS improvement.

5.6. Implications for Project Operations

The institutional arrangement between co-financiers and TDB has several implications for security risk management in the FCV context:

- Direct Responsibility: TDB carries the accountability typically borne by a government counterpart. This includes ensuring proportional, rights-respecting security arrangements across all implementing partners.
- Private Sector Compliance: Private Companies receiving TDB financing are contractually obliged to adopt security measures aligned with good international practice, subject to independent verification.
- Layered Oversight: The dual system of IVAs and the BSMA provides assurance that security commitments are not only written into agreements but are also monitored in practice.
- Adaptation to FCV Environment: Security risks in FCV environments are severe and volatile. The institutional model allows for operational continuity while embedding mechanisms for incident reporting, adaptive management, and accountability.

6. TDB Implementation Unit

The de facto Project Implementation Unit (PIU) for TDB projects in FCV Environments is established upon deal origination.

6.1. Composition and Functions

The PIU is composed of multidisciplinary staff and external support, structured around the following functions:

- **Management Team:** Responsible for launching calls for proposals, contracting service providers, managing grant agreements, and overseeing performance.
- **Procurement and Financial Management:** Dedicated financial staff and internal auditors manage fund flows, maintain designated accounts, and ensure compliance with disbursement and reporting requirements of TDB and its co-financing partners as applicable. Manuals on financial and grant management are prepared and approved by the Bank.
- **E&S Specialists:** Embedded within the PIU through TDB's ESMS, including an ESMS Manager, Coordinator, Lending Operations Champion, and sectoral E&S specialists. They ensure that Environmental and Social Standards (ESS) obligations are integrated into all PIU functions, including security risk management.
- **Independent Verification Agents (IVAs):** Contracted by the PIU to verify outputs before disbursement, ensuring accountability and transparency.
- **Security Risk Management:**

  ✓ Each PIU includes a dedicated suitably qualified security specialist, responsible for: developing and updating Security Risk Assessments (SRAs) and Security Management Plans (SMPs), providing training, ensuring alignment with international standards (IFC PS, VPSHR, ICoCA), and liaising with TDB management on security issues.

- ✓ The international specialist is supported by an internationally accredited local security company, contracted to provide protective services, secure facilities, manage guard forces, and support movement. This partnership ensures global best practice is applied while leveraging local access, legitimacy, and situational awareness.

- **Liaison Functions:** Where required, the PIU also designates Liaison Security Officers to maintain relationships with local authorities, community leaders, and formal security forces, ensuring coordination and deconfliction.

6.2. Accountability and Reporting

The PIU is accountable to TDB management for all fiduciary, E&S, and security risk management functions. It reports on:

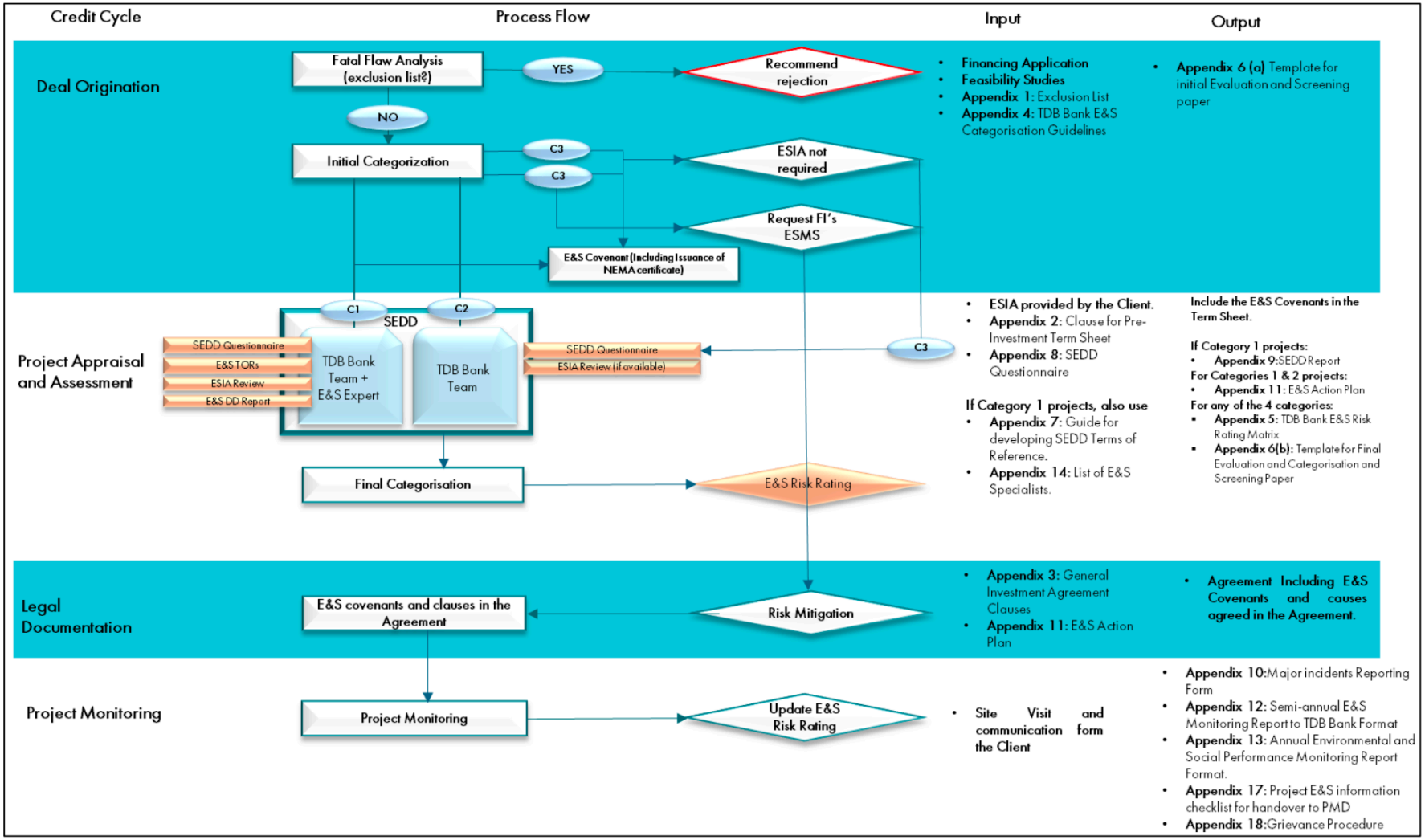
- Financial progress through quarterly Interim Unaudited Financial Reports (IFRs);
- E&S compliance through ESMS reporting requirements; and
- Security performance through incident reporting and monitoring frameworks, aligned with IFC PS, VPSHR, and ICoCA obligations.

7. TDB Environmental and Social Management System

TDB's Environmental and Social Management System (ESMS) establishes a structured, process-driven approach for identifying, assessing, and managing environmental and social risks across all projects. The ESMS applies from deal origination to project completion or exit, ensuring that risks are systematically addressed at each stage of the investment cycle, in line with international standards such as the Equator Principles, the Harmonized EDFI E&S Standards, and relevant IFC Performance Standards.

7.1. Project Categorization and Screening

- At the earliest stage of deal origination, all projects undergo fatal flaw analysis and initial categorisation.
- TDB applies a four-tier classification system (Category 1–4), aligned with IFC practice, to determine the level of risk and the depth of assessment required.
- The screening process uses checklists and templates (Appendix 6A–C) to capture potential environmental, social, and governance risks and to decide whether projects may proceed to appraisal.



Please note that in the above diagram C1, C2, C3 and C4 respectively stand for Category 1, 2, 3 and 4.

7.2. Due Diligence and Appraisal

- Projects that pass screening undergo Social and Environmental Due Diligence (SEDD), which includes:

  ✓ Reviewing Environmental and Social Impact Assessments (ESIAs), Initial Environmental Examinations (IEEs), or equivalent studies.
  ✓ Conducting site visits guided by TDB's SEDD Questionnaire.
  ✓ Producing a SEDD Report with recommendations and an E&S Action Plan (ESAP), where required.

- The ESAP sets out corrective and mitigation measures, timelines, and responsibilities to bring the project into alignment with TDB and international standards.

7.3. Legal Documentation and Covenants

- Once due diligence is complete, E&S requirements are embedded in loan agreements through specific covenants.

- These covenants typically include:

  ✓ Implementation of the ESAP.
  ✓ Compliance with host-country environmental and social laws.
  ✓ Maintenance of grievance mechanisms and stakeholder engagement processes.
  ✓ Reporting requirements, including semi-annual and annual submissions.

- Standard clauses are provided in Appendix 2 and Appendix 3 of the ESMS.

7.4. Implementation and Monitoring

- During project implementation, clients are responsible for operationalising their ESAPs and reporting progress.

- TDB conducts compliance monitoring using defined tools, including:

  ✓ Major Incident Reporting.
  ✓ Semi-Annual E&S Monitoring Reports.
  ✓ Annual E&S Performance Monitoring Reports.
  ✓ Project E&S Information Checklists.
  ✓ Grievance Logs.

- Independent reviews may be required for higher-risk projects (Category 1, and some Category 2), generally every two years.

7.5. Reporting and Completion

- Clients submit regular reports to TDB, which in turn consolidates and reports to lenders, shareholders, and its partners.
- At project completion or exit, TDB reviews overall E&S performance, documents lessons learned and ensures that any residual actions are addressed.

7.6. Review and Continuous Improvement

- TDB reviews and updates its ESMS periodically to reflect lessons learned, emerging risks, and evolving international standards.
- Updates may be triggered by operational changes, client incidents, or shifts in lender/shareholder requirements.

8. IFC Performance Standards and Physical Security

TDB aligns its security risk management with the IFC Performance Standards (2012). While PS4 (Community Health, Safety, and Security) is the anchor for managing security risks to communities, effective practice draws on several Standards in combination. The points below set out how each relevant PS informs the design of SRAMPs, contractor obligations, and monitoring in FCV environments.

8.1. PS1 — Assessment and Management of Environmental and Social Risks and Impacts

What it means for security: PS1 requires a risk-based Environmental & Social Management System (ESMS) with screening, assessment, management programs, organizational capacity, stakeholder engagement, monitoring, and adaptive management. Security risks—identified via contextual analysis and site-level SRAs—must be integrated into the ESMS and addressed through actionable management plans (e.g., the SRAMP), with roles, resources, and performance monitoring clearly defined. This is the foundation for "one system" governance linking the SRAMP to other E&S instruments.

8.2. PS2 — Labor and Working Conditions

What it means for security: PS2 requires safe and healthy working conditions for all project workers, including contracted and community workers. Where security risks may affect workers (e.g., travel to sites, accommodation, guarding interfaces, harassment risks), controls must be embedded in contractor LSMPs/ASPs and worker induction/training, with access to grievance mechanisms and protection from retaliation. Interface procedures with public/private security must protect workers' rights and safety.

8.3. PS4 — Community Health, Safety, and Security (core to security management)

What it means for security: PS4 requires clients to assess and manage risks to affected communities, including those arising from the use of security personnel. Key implications for SRAMPs:

- Conduct security risk assessments that consider community exposure and vulnerabilities; apply proportional mitigation and good international industry practice.
- If security personnel are engaged, implement a Security Management Plan covering vetting (no past abuses), training (conduct, human rights, use of force, SEA/SH prevention), rules of engagement, incident reporting, grievance pathways, and coordination with public authorities.
- Manage relations with public security to promote lawful, proportionate, and accountable conduct; document any support provided and establish protocols for incident referral and follow-up.
- Maintain emergency preparedness and response for security incidents (with community-sensitive communication and drills).
- These PS4 elements map directly to SRAMP sections on threat assessment, proportional controls, contractor cascading, and oversight.

8.4. PS5 — Land Acquisition and Involuntary Resettlement

What it means for security: Resettlement processes must safeguard displaced persons from harm. Security planning should prevent intimidation, forced evictions, or violence; ensure safe access to sites and services; and provide **security of tenure** at resettlement locations. SRAMPs should address risks around demolitions, movements, and site handovers, and align with RAP implementation schedules.

8.5. PS7 — Indigenous Peoples

What it means for security: Interactions with Indigenous Peoples must respect cultural rights and (where applicable) **FPIC** processes. Any use of public or private security in Indigenous territories must be culturally appropriate, rights-respecting, and designed to avoid intimidation or reprisals. SRAMP community-acceptance measures and security-provider training should reflect these requirements.

8.6. PS8 — Cultural Heritage

What it means for security: Projects must protect tangible and intangible cultural heritage from adverse impacts, including theft, vandalism, or conflict-related damage. Security measures for sites (surveillance, access control, escorts for movable artefacts) should be proportionate and coordinated with heritage authorities and communities, and reflected in LSMPs/ASPs where relevant.

8.7. How this integrates with TDB's SRAMP/ESMS

- **Screening & scoping (PS1):** Country/area FCV diagnostics and site-level threat scans determine whether a **SRAMP is mandatory** and define its scope. Outputs feed the ESMS risk register and management programs.

- **Design & proportionality (PS4):** The **SRAMP** translates risk into controls for communities and workers, governs engagement of public/private security, and sets emergency readiness.

- **Worker protection (PS2):** Contractor LSMPs must protect workers from security risks (journey management, accommodation security, conduct at checkpoints) and ensure access to worker GRMs.

- **Resettlement interfaces (PS5):** Where land acquisition occurs, SRAMP measures prevent violence or coercion during RAP implementation and safeguard displaced households.

- **Cultural and Indigenous considerations (PS7, PS8):** Security arrangements are tailored to cultural rights and heritage protection, with appropriate training and engagement protocols.

- **Monitoring & incident management (PS1/PS4):** KPIs, incident reporting, corrective actions, and periodic reviews ensure the SRAMP remains a **living plan** aligned with ESMS change management.

9. TDB Security Risk Management System in FCV environments

9.1. Purpose and Requirement for Project Level Security Risk Assessment and Management Plan (SRAMP)

In contexts of fragility, conflict, and violence (FCV), traditional environmental and social due diligence processes alone are insufficient to manage the elevated risks faced by project workers, affected communities, and implementing partners. To address this gap, the Trade

and Development Bank (TDB) requires that every project financed in FCV environments prepare a Security Risk Assessment and Management Plan (SRAMP).

The SRAMP is a project-specific framework that integrates with TDB's Environmental and Social Management System (ESMS). While the ESMS governs the full cycle of environmental and social risk management — from screening and due diligence to monitoring and reporting — the SRAMP operationalises the security dimension of risk management. It is mandatory for all projects classified as operating in an FCV environment.

SRAMPs must be prepared during the appraisal stage (aligned with Social and Environmental Due Diligence), approved prior to disbursement, embedded in loan covenants, and regularly updated during implementation.

9.2. Core Components of a SRAMP

9.2.1. Introduction and Objectives

The Security Risk Assessment and Management Plan (SRAMP) will start with an introduction stating that it is the central instrument through which the Trade and Development Bank (TDB) addresses security risks in projects delivered in fragile, conflict-affected, and violent (FCV) environments. It will establish a structured framework for systematically identifying, assessing, mitigating, and monitoring security threats that may affect project staff, contractors, beneficiaries, assets, and project continuity.

The requirement for a SRAMP arises directly from the unique challenges of FCV settings. In these environments, governance is often weak, state security actors may be fragmented or politicised, non-state armed groups frequently operate with impunity, and criminality intersects with community tensions and political instability. Against such a backdrop, security is not an ancillary issue but a fundamental operational concern that directly determines whether project objectives can be delivered.

The SRAMP is a mandatory requirement for all projects classified as as operating in an FCV environment under TDB's Environmental and Social Management System (ESMS). It also applies to any project where contextual analysis indicates material exposure to security risks, regardless of ESMS category.

The SRAMP functions in two ways. It is standalone in the sense that it provides a complete operational document, setting out governance arrangements, site-level risk assessments, mitigation measures, contractor obligations, incident reporting protocols, and crisis management procedures. At the same time, it is also integrated within the ESMS, dovetailing with safeguards processes at each stage of the project cycle: security-sensitive projects are identified during screening and categorisation; draft SRAMPs are prepared alongside Social and Environmental Due Diligence (SEDD); the SRAMP is included in

appraisal packages and embedded in legal covenants; during implementation, SRAMP obligations are enforced through PIU oversight and contractor compliance; and finally, at completion, SRAMP effectiveness is reviewed to capture lessons learned.

The objectives of the SRAMP can be summarised as follows: to protect people (workers, contractors, and communities), to safeguard project assets, to enable continuity of operations in volatile environments, to ensure compliance with TDB requirements, to strengthen accountability through reporting and oversight, and to foster positive community relations by designing security measures that minimise harm and build acceptance.

In practice, the SRAMP serves as the reference document for all actors, from PIU staff and contractors to local security providers. It must be prepared during project appraisal, approved by TDB's E&S Unit prior to disbursement, and updated at least annually or sooner if the security environment changes significantly.

9.2.2. Methodology and Approach

The SRAMP methodology follows a structured cycle designed to provide consistency across TDB's portfolio while remaining adaptable to the fluid realities of FCV contexts. It aligns closely with the risk management cycle embedded in the TDB ESMS and reflects the requirements of the IFC Performance Standards.

Two principles guide the approach. First, all security risk mitigation measures must cascade contractually. Since TDB does not directly implement civil works, mitigation measures must be embedded in contracts and sub-contracts, ensuring obligations flow down through multiple tiers until they reach the individual worker. The construction worker, the local driver, or the trench digger must directly benefit from the protections identified in the SRAMP. Second, risk assessments must be localised. They should be carried out at the lowest feasible level — site, activity, or community — rather than only at national or regional scales. Localised assessments ensure that mitigation measures are proportionate and targeted rather than either excessive or insufficient.

The methodology is organised into five sequential steps:

Contextual Analysis establishes the baseline understanding of the operating environment. This includes political, conflict, socio-economic, and cultural dynamics. The process draws on secondary sources such as UN and INGO reports, incorporates key informant interviews, and maps stakeholders including security forces, non-state armed groups, and local civil society. This analysis links directly to ESMS scoping and screening, ensuring that security risks are considered alongside environmental and social ones.

Threat Identification catalogues the full range of potential security threats, which may include armed conflict, civil unrest, terrorism, criminality, kidnapping, sexual exploitation

and abuse or harassment (SEA/SH), and insider threats. This step aligns with ESS4 and ESS2 obligations by identifying risks to workers, communities, and assets.

Risk Assessment evaluates the likelihood and potential impact of identified threats. Using a five-point risk matrix, risks are scored and rated at the site or activity level. Local specificity is preserved even as assessments are consolidated into a project-wide register. The output is a Security Risk Register that clearly ties mitigation obligations to contractors and sub-contractors.

Mitigation and Management Planning translate assessed risks into practical, enforceable measures. The hierarchy of controls is applied, and mitigation measures are embedded contractually into procurement documents and agreements. Contractors are required to develop Activity Security Plans (ASPs) or Local Security Management Plans (LSMPs) that detail implementation on the ground. Examples include securing transport protocols in logistics contracts, guarding provisions in construction agreements, or SEA/SH training requirements in local labour contracts. These measures are incorporated into the ESCP and monitored as part of ESMS implementation.

Monitoring, Evaluation, and Adaptive Management ensures the SRAMP remains a living document. Contractors submit monthly compliance reports; the PIU Security Specialist conducts site visits and spot checks; PIUs consolidate quarterly findings for TDB. The SRAMP must be formally reviewed at least once per year, or sooner if conditions change materially. Lessons learned at site level are fed back into revised assessments, creating a feedback loop that ensures continuous adaptation.

The outputs of this methodology include a comprehensive Security Risk Register, mitigation measures embedded contractually at every tier, a tiered implementation structure with clear responsibilities, and a monitoring and reporting system that integrates with TDB's ESMS.

9.2.3. Security Context and Threat Environment

Every SRAMP must begin with a clear understanding of the security context in which the project will operate. Without such an analysis, mitigation measures risk being mis calibrated — too light to be effective or too heavy-handed to be sustainable. The responsibility for compiling and maintaining this analysis lies with the PIU's International Security Specialist, who must draw on both international and local sources.

At the national level, the SRAMP should outline the broader security and political environment. This includes the status of armed conflict and political instability, the presence and capacity of state security institutions, the role of non-state armed groups and militias, prevailing patterns of criminality such as banditry or smuggling, and the legal framework regulating security provision. This establishes the "big picture" within which project-specific risks must be situated.

At the sub-national and local levels, the analysis must zoom in on the specific areas where project activities are planned. This requires examining active or recent conflict dynamics, patterns of criminal activity, community disputes relevant to the project (for example, land use or employment issues), and local perceptions of the project itself. Such analysis must be site-specific, as conditions can vary significantly even between neighbouring districts.

The SRAMP must also define the relevant threat typology. Common threats include armed conflict and hostilities, civil unrest, terrorism or sabotage, opportunistic crime, kidnapping or extortion, SEA/SH risks, insider threats, and cyber threats to digital systems. For each threat, the SRAMP should provide a description, an assessment of likelihood and impact, and a statement of its relevance to project personnel, assets, or communities.

Stakeholder mapping complements threat analysis by identifying state and non-state security actors, community leaders, humanitarian and development agencies, and private security providers active in the project area. Such mapping highlights potential partners, risks of collusion, and the possibility of unintended consequences when engaging with different actors.

To ensure transparency and credibility, all contextual and threat assessments must draw on multiple data sources — international datasets such as ACLED, UN OCHA reports, INSO alerts, national media, local authority inputs, community liaison feedback, and contractor site reports. All sources must be cited and dated.

The outputs of this section include a written contextual baseline at national and sub-national levels, a threat matrix summarising identified threats, a stakeholder map, and an annex listing all sources consulted. Within the ESMS, this analysis supports SEDD, informs project risk categorisation, and provides the baseline against which incident reporting and monitoring will be measured.

9.2.4. Security Risk Assessment (SRA)

The Security Risk Assessment (SRA) is the analytical backbone of the SRAMP, turning contextual and threat analysis into a structured evaluation of risks. It must be evidence-based, site-specific, and updated regularly to reflect changing conditions. Generic assessments are inadequate; each SRA must reflect the realities faced by workers and communities in actual project locations. The SRA should be completed by the PIU security specialist.

The purpose of the SRA is fivefold: to identify credible threats, to evaluate vulnerabilities, to assess the consequences of incidents, to prioritise risks through objective scoring, and to create a risk register that serves as the operational reference point for mitigation, monitoring, and reporting.

The SRA process is structured around several components. Threat identification catalogues the full range of threats, describing their actors, methods, frequency, and trends. This draws on both quantitative data and qualitative inputs. Likelihood assessment then determines the probability of each threat materialising, considering historical patterns, activity levels of threat actors, seasonal dynamics, proximity to hotspots, and early warning indicators. A five-point scoring scale is applied, ranging from "rare" to "almost certain." Vulnerability analysis examines how project activities, sites, and people are exposed to these threats, considering factors such as geography, activity type, workforce profile, and public visibility. Impact assessment evaluates the potential consequences of incidents in terms of human safety, assets, operational continuity, and reputation.

These factors combine in a risk scoring process, where likelihood, impact and vulnerability are multiplied to generate a risk rating. Risks are categorised as low, moderate, substantial, high, or extreme, often displayed in colour-coded matrices. Finally, a consolidated risk register is produced, detailing each risk, its score, proposed mitigation measures, responsible parties, and timelines. The register must be treated as a live document, updated monthly by the Security Specialist.

Crucially, whilst the SRAMP incorporates an SRA at the project level, across the states, or regions that the project will operate in, Local SRAs must be conducted at the site level. Each project site or activity location requires its own assessment — for example, each borehole in a water project, each road segment in a transport project, or each storage facility in a logistics chain. These site-level SRAs are then consolidated into a project-wide assessment without losing their specificity.

The initial project SRA must be prepared during project appraisal, with quarterly updates and a full annual review, or sooner if major incidents occur. Responsibilities are shared: the International Security Specialist leads preparation and consolidation, contractors conduct site-level assessments, local security providers contribute data and technical advice, and the PIU Coordinator ensures integration into project decision-making.

The outputs of the SRA include a threat register, a risk matrix, a consolidated risk register, and a summary narrative that highlights red-flag risks requiring urgent attention. Within the ESMS, the SRA complements SEDD by deepening security-specific analysis, informs the ESAP, and provides inputs for risk monitoring.

9.2.5. Security Risk Mitigation Framework

The Security Risk Mitigation Framework is the operational core of the SRAMP. It ensures that the risks identified in the SRA are translated into site-specific management plans and implemented through contractual obligations that are subject to continuous oversight.

The process follows a sequential chain. First, a Local Security Risk Assessment (LSRA) is prepared at the lowest practical level, either by the supplier operating at the site or by the PIU Security Specialist with support from a local security company. The LSRA sets out the threats, vulnerabilities, likelihood, and impact specific to the site and defines the proportional risk mitigation requirements. In response, the supplier develops a Local Security Management Plan (LSMP), which explains in detail how these mitigation measures will be implemented, including resources, timelines, and procedures. LSMPs must cover facility protection, journey management, personnel safety, information security, and community acceptance. Both the LSRA and LSMP are then reviewed by the PIU Security Specialist, who must formally sign them off before implementation begins.

Once approved, the supplier or implementing partner is responsible for executing the LSMP. This ensures that frontline workers — whether construction crews, drivers, or field officers — directly experience the benefits of risk mitigation. Oversight is provided by the PIU Security Specialist, supported by third-party monitoring agents. Non-compliance triggers corrective measures under contractual and ESMS provisions.

Roles and responsibilities are clearly defined. Suppliers draft LSMPs, implement mitigation on the ground, and provide monthly compliance reports. The PIU Security Specialist validates LSRAs and LSMPs, conducts oversight, and reports to TDB. Local accredited security providers may assist with LSRA preparation or provide operational support to suppliers such as guards or escorts, and train staff in LSMP procedures. The TDB ESMS Unit ensures that the LSRA/LSMP process is embedded in project agreements and monitors compliance through reporting.

Contractual cascading is critical. All mitigation measures must flow through procurement packages and sub-contracts, ensuring obligations reach every tier of delivery. Procurement documents must explicitly require LSRAs and LSMPs, mandate implementation of approved measures, and accept oversight and audit mechanisms. This guarantees that even the lowest-level worker benefits from security measures.

Monitoring is continuous. Suppliers confirm implementation through monthly reports, PIU Specialists provide quarterly consolidated reviews to TDB, and escalation protocols apply where compliance falters. Activities may be suspended, or contracts terminated, if mitigation measures are absent.

The outputs of the framework include validated LSRAs, corresponding LSMPs, documented sign-off by PIU, oversight reports, and contractual enforcement records. Within the ESMS, LSRAs serve as the equivalent of site-specific ESMPs, LSMPs operationalise these measures, PIU approvals mirror safeguards clearance gateways, and monitoring is integrated into ESMS reporting cycles.

9.2.6. Risk Levels, Escalation, and In-Extremis Events

An essential part of the SRAMP is defining how security risks are categorised and what actions are required as those risks increase or decrease over time. This provides predictability, consistency, and accountability in decision-making, ensuring that project staff and contractors know what measures apply in each situation.

Security risks are classified according to a five-tier system. At the lowest level, a "low" risk indicates that threats are minimal or unlikely to materialise, and only routine protective measures are necessary. A "moderate" risk level reflects a context where incidents are possible, though not expected to be frequent, requiring supplementary but manageable measures. A "substantial" risk rating indicates that credible threats are present, and incidents are likely unless robust mitigation measures are applied; projects at this level require heightened controls and regular oversight. A "high" risk rating signals an environment where hostile incidents are probable, where operations face regular disruption, and where strict restrictions on movement, close supervision, and continuous security presence are mandatory. The "extreme" risk category represents imminent or ongoing threats that cannot be adequately mitigated; in such situations, all project activities must be suspended or personnel evacuated until conditions improve.

Escalation protocols ensure that risk levels can be raised quickly when conditions deteriorate. A rise in frequency or severity of incidents, the targeting of aid workers, or the withdrawal of state security forces may all constitute triggers for escalation. The PIU Security Specialist is responsible for recommending a change in risk level, with final authority resting with the PIU Coordinator, who must inform TDB's ESMS Unit within 24 hours of the decision. De-escalation, by contrast, can only occur when sustained improvements are evidenced — such as a verified decline in incidents, a successful ceasefire, or enhanced security presence. All changes in risk levels must be justified in writing and recorded in the SRAMP.

In addition, the SRAMP must anticipate in-extremis events — extraordinary, high-impact incidents that threaten life or project continuity. These may include armed assaults on compounds, kidnappings, or mass-casualty incidents resulting from attacks or unrest. In such cases, site-level Local Security Management Plans (LSMPs) guide immediate actions, whether shelter-in-place, movement to safe havens, or evacuation. The PIU's Crisis Management Team is then activated, with the PIU Security Specialist coordinating the tactical response. Host government forces, UN missions, and diplomatic representatives may also be engaged. TDB must be notified within 24 hours of any such event, with the World Bank informed within 48 hours for co-financed projects. A full post-incident review, including root cause analysis and corrective actions, must follow before resuming operations.

9.2.7. Security Approval Gateways

The SRAMP establishes "security approval gateways" as mandatory checkpoints that must be cleared before project activities begin. These gateways integrate security risk management into the wider project cycle, ensuring that activities proceed only when security risks have been assessed, mitigated, and formally authorised.

Approval gateways are triggered at key points: before contractors mobilise to a site, before any high-risk activities commence (such as large-scale construction or sensitive community consultations), and before personnel move into newly assessed areas. No activity can begin unless the gateway has been cleared.

Clearance depends on the completion of several conditions. A Local Security Risk Assessment (LSRA) must first be prepared for the site or activity. The relevant supplier or implementing partner must then draft a Local Security Management Plan (LSMP) in response, specifying how identified mitigation measures will be operationalised. This LSMP must be reviewed and approved by the PIU Security Specialist. In addition, the PIU must confirm that all resources required for implementation — from security guards to fencing and communication equipment — are in place, and that budget allocations are secured.

The PIU Security Specialist maintains a Security Gateway Register, recording all approvals, the dates of LSRA and LSMP completion, the date of clearance, and any conditions attached to approval. This register is auditable by both TDB and the World Bank. Enforcement is strict: contractors attempting to mobilise without gateway approval are in breach of contract and subject to penalties, up to suspension or termination. In this way, the gateway system provides a clear mechanism for ensuring that no project activity proceeds without adequate security risk management.

9.2.8. Contractor Security Requirements

Because contractors and sub-contractors carry out the bulk of project activities, they are the frontline actors in implementing security measures. The SRAMP therefore establishes clear and binding requirements for contractors to ensure that risk mitigation cascades all the way down to the individual worker.

Contractual obligations are central. All procurement documents and contracts must include security clauses that require contractors to comply fully with SRAMP provisions. This includes preparing LSMPs based on approved LSRAs, cooperating with PIU oversight, adhering to the Voluntary Principles on Security and Human Rights, and maintaining zero tolerance for sexual exploitation, abuse, and harassment. Contractors are also required to accept regular audits and spot checks by the PIU and, where applicable, independent monitors.

Before mobilisation, contractors must fulfil several preconditions. They must submit their LSMP for approval, ensure that all staff receive security inductions and site-specific risk briefings, and establish clear reporting lines to the PIU Security Specialist. Contractors must also complete a pre-mobilisation security checklist, covering measures such as guard deployment, vehicle standards, and communications equipment. Only after these steps are verified can mobilisation proceed.

Monitoring and enforcement are continuous. Contractors must provide monthly compliance reports, documenting the implementation of security measures. The PIU Security Specialist conducts spot checks and site visits, while TDB reserves the right to commission independent audits. Where non-compliance is found, corrective action is required. Persistent or serious breaches may result in suspension of work or termination of contracts.

These contractor requirements align directly with the TDB ESMS framework for contractor due diligence and management. By embedding obligations contractually and enforcing them rigorously, the SRAMP ensures that security risk management is not confined to policy documents but is delivered in practice at project sites.

9.2.9. Security Partners, Monitoring & Evaluation, and PIU Security Procedures

Security risk management in FCV environments cannot be managed by project actors alone. It requires coordinated engagement with external partners, robust systems of monitoring and evaluation, and clear internal procedures within the PIU.

Engagement with security partners is essential. Host government forces, where they are present and credible, may provide support, but this engagement must be formalised through Memoranda of Understanding that explicitly commit them to proportional use of force and respect for human rights. The PIU should also maintain active relationships with international and national organisations, such as UN missions or INGO security forums, to benefit from intelligence-sharing and joint contingency planning. At the community level, continuous dialogue with local leaders and structures is vital to building trust and ensuring that security measures are understood and accepted. Where private security providers are engaged, only firms with recognised accreditation and compliance with international standards should be contracted.

Monitoring and evaluation provide the evidence base for adapting and improving security measures. The PIU must establish clear indicators, such as the number and type of incidents, timeliness of reporting, compliance with LSMPs, and completion of training and drills. Contractors are required to conduct daily monitoring and submit weekly updates to the PIU Security Specialist, who consolidates this information into monthly reports. Quarterly reports are provided to TDB, and at least once per year an independent third-party audit must be conducted to evaluate the effectiveness of the SRAMP.

Finally, the PIU must maintain internal Standard Operating Procedures (SOPs) that guide day-to-day operations. These include procedures for movement control, communication protocols, incident reporting, and crisis management activation. SOPs ensure that PIU staff and contractors know exactly what to do in routine situations as well as emergencies. They also provide a reference framework for audits and reviews, demonstrating compliance with both SRAMP and ESMS requirements.

Together, security partnerships, rigorous monitoring and evaluation, and PIU internal procedures ensure that the SRAMP is not static but a dynamic, living system that can adapt to the changing conditions of FCV environments.

9.3. Overlap with TDB's ESMS

The SRAMP is not a parallel system; it is the security "track" of the ESMS and follows the same project-cycle logic—from screening to completion—so that security risks are treated with the same rigor as environmental and social risks.

During screening and categorisation (ESMS 4.1), the initial context scan identifies whether a project operates in an FCV environment or otherwise faces material exposure to security threats. That early flag determines if a SRAMP will be mandatory and the indicative level of effort (e.g., site-specific LSRAs anticipated for multiple work fronts). The screening note should record the rationale, link to any country or state-level analysis, and signal resource needs (International Security Specialist, accredited local provider).

At appraisal and SEDD, security risks are analysed in depth alongside environmental and social risks. A draft SRAMP is prepared to the same evidentiary standard as an ESIA/ESMP: it includes threat and likelihood analysis, site-level vulnerabilities, and a first pass at proportional mitigation requirements. Where construction or field operations are expected, the draft also maps the contractual cascade—which packages will carry security clauses, which contractors must prepare LSMPs/ASPs, and what approval gateways are required before mobilisation.

The outcomes of appraisal are then embedded in legal documentation. Security measures are captured in the ESCP/ESAP (e.g., deadlines for LSRAs/LSMPs, training, incident reporting, independent audits), while the financing and procurement documents carry enforceable covenants and clauses: compliance with the SRAMP and ESS4, mandatory LSMP approval before works start, cooperation with monitoring, VPSHR and SEA/SH obligations, and remedies for non-compliance. These same conditions underpin the security approval gateways, ensuring no high-risk activity proceeds until the prerequisites are in place.

During implementation and monitoring (ESMS 5), security performance is tracked through the same cadence as other E&S commitments. Contractors submit monthly security

compliance reports; the PIU consolidates results and provides semi-annual monitoring to TDB, with material incidents reported within required timelines. Spot checks and third-party verifications are used where risk is substantial or high. Corrective actions feed into the ESAP, and escalation/de-escalation decisions are documented as part of adaptive management. Stakeholder engagement and the GRM capture community concerns related to security providers, checkpoints, or movement restrictions, ensuring security measures remain proportionate and respectful of rights, consistent with ESS4 and ESS10.

At completion and exit, the project conducts a summative review of security management effectiveness alongside the broader E&S evaluation. This includes trends in incident data, timeliness and quality of reporting, the adequacy of LSMPs, the function of gateways and crisis procedures, and any unintended social impacts (e.g., perceptions of over-securitisation). Lessons learned—including adjustments to contract language, training modules, or approval thresholds—are documented and fed back into TDB's ESMS knowledge base for future operations.

In short, the SRAMP provides the operational expression of ESMS requirements for security: it applies the same due-diligence discipline, the same contractual enforceability, and the same monitoring and learning loop to risks that affect worker safety, community protection, and any engagement with public or private security forces.

9.4. Templates and Annexes

To ensure consistency and auditability across projects, this Guidance Note is accompanied by a suite of standard templates that PIUs and contractors must use and tailor to context. Each template is designed to fit naturally into the ESMS document set and to support the SRAMP workflow from assessment to implementation.

SRAMP Master Template. A fillable framework (aligned to ISO 31000 concepts and World Bank FCV practice) that mirrors the structure set out in Section 9.3. It guides teams through context/threat analysis, site-level SRAs, mitigation design, approval gateways, and monitoring arrangements, with prompts for evidence, data sources, and cross-references to ESCP/ESAP items.

Local Security Management Plan (LSMP) Template. Used by suppliers/implementing partners to translate LSRA requirements into site-specific procedures. Sections cover facility protection, journey management, personnel safety, information security, community acceptance, training, and emergency actions; it includes a sign-off page for the PIU Security Specialist and a mobilisation checklist.

Security Checklist and Audit Forms. Standardised tools for pre-mobilisation verification (guards contracted, access control installed, comms and medevac in place) and for periodic compliance audits. Findings link to corrective-action registers and ESAP updates.

Crisis Management Plan (CMP) Template. A practical playbook for in-extremis events, cross-referenced to LSMPs and PIU SOPs. It defines roles of the Crisis Management Team, notification trees (including TDB/World Bank timeframes), decision logs for escalation/de-escalation, and post-incident review formats.

Each template contains brief completion guidance and model text to set the expected level of detail, along with placeholders for data protection notices, VPSHR/SEA-SH commitments, and linkages to the project's SEP and GRM. Projects may add annexes (e.g., maps, contact lists, route cards, facility diagrams), but the core structure should be retained to preserve comparability across TDB's portfolio and facilitate World Bank review.

9.5. Roles and Responsibilities

Clear definition of roles and responsibilities is critical to the success of SRAMP implementation. Security risk management in FCV environments requires contributions from multiple actors, each of whom must understand their duties, lines of accountability, and reporting obligations.

Trade and Development Bank (TDB). TDB is the custodian of the ESMS and sets the policy framework for security risk management. It ensures that SRAMP requirements are embedded in project documentation, approves the SRAMP as part of safeguards due diligence, and monitors implementation through regular reporting. TDB also commissions third-party audits where appropriate and liaises with co-financiers to confirm compliance in co-financed projects.

Project Implementation Unit (PIU). Each PIU is responsible for day-to-day implementation of the SRAMP. Within the PIU:

- The International Security Specialist provides technical leadership, prepares and validates Local Security Risk Assessments (LSRAs), reviews Local Security Management Plans (LSMPs), and oversees contractor compliance.
- The PIU Coordinator holds overall accountability, ensuring that security risk management is integrated into project planning, procurement, and operations.
- Other PIU staff follow the Standard Operating Procedures (SOPs) on movement, communications, and incident reporting, contributing to a culture of compliance.

Contractors and Sub-contractors. Contractors are the primary implementers of security mitigation measures. They are required to develop LSMPs in response to approved LSRAs, cascade obligations to all sub-contractors, train their staff in required procedures, and submit regular compliance reports. They must cooperate with PIU oversight and accept independent monitoring. Non-compliance exposes them to contractual remedies, including suspension or termination.

Local Accredited Security Providers. Where engaged by suppliers, these providers offer operational support such as static guarding, escorts, or journey management. They may also assist in preparing LSRAs and training contractor staff in LSMP implementation. Only firms with verifiable accreditation and adherence to international standards should be contracted.

Community Stakeholders. While not direct implementers, local communities, traditional leaders, and civil society groups play an important role in shaping the security environment. Their input helps calibrate mitigation measures, and they must have access to grievance mechanisms to raise concerns about security practices.

Third-Party Monitors and Auditors. Independent monitors provide an external check on SRAMP implementation. They verify compliance with LSMPs, audit contractor practices, and assess whether security measures are proportionate, rights-respecting, and effective. Their findings feed directly into TDB's oversight role.

Together, these roles establish a tiered governance system: TDB sets policy and monitors compliance, PIUs provide oversight and technical direction, contractors operationalise measures on the ground, and external partners provide verification and accountability. This division of labour ensures that security risk management responsibilities are clearly allocated and consistently enforced.

10. Use of Security Forces

The decision to employ security forces on TDB-financed projects is never automatic. It must flow directly from the Local Security Risk Assessment (LSRA) process described earlier in this Guidance Note. Where an LSRA determines that passive or non-armed measures are insufficient to reduce threats to an acceptable level, it may recommend the use of security forces as a proportional mitigation measure. Equally, the LSRA must also consider the risks inherent in using security forces themselves—such as the potential for escalation, misuse of authority, or human rights violations—and document how these will be managed.

Before any security forces are engaged on TDB-financed projects, a thorough vetting process must be undertaken to ensure their suitability and integrity. This process should assess individuals' human rights records, past conduct, and affiliations to prevent the involvement of personnel implicated in abuse, corruption, or criminal activity. Vetting should draw on information from credible sources, including host government records where available, community feedback, and independent verification. Only personnel who meet the standards set out in the Good Practice Note on Assessing and Managing the Risks and Impacts of the Use of Security Personnel (GPN, p. 8) should be deployed. The results of the vetting process and any mitigation measures for identified risks should be documented in the LSRA and project security management plan.

10.1. Determining the Requirement

The LSRA must clearly:

- **Justify necessity.** Engagement of security forces is only permissible if a demonstrable threat exists (e.g., armed attacks, persistent banditry, targeted intimidation) that cannot be adequately managed through other means.
- **Define proportionality.** The scope of security support must be tailored to the level of threat and never exceed what is required to safeguard people and assets.
- **Identify risks of engagement.** Potential harms associated with the presence of security forces—such as intimidation of communities, the risk of excessive force, or reputational damage—must be weighed and mitigation measures defined.

Only once these conditions are documented and approved by the PIU Security Specialist can the project proceed to engage security forces.

10.2. Categories of Security Forces

Where justified, two categories may be used:

- **Private Security Providers** (contracted companies providing guarding, access control, convoy escorts, or surveillance). These must be internationally accredited, demonstrate compliance with the Voluntary Principles on Security and Human Rights (VPSHR), and maintain strong internal governance.
- **Public Security Forces** (police, military, paramilitary, or intelligence units). Their involvement is highly sensitive and must be governed through formal arrangements that set clear limits on their role, proportional use of force, and adherence to international human rights law.

10.3. Governance Arrangements

Engagement must always be codified in writing:

- **Private providers** are bound by contracts requiring VPSHR compliance, SEA/SH prohibitions, codes of conduct, and acceptance of PIU and third-party monitoring.
- **Public forces** must operate under a Memorandum of Understanding (MoU) between the PIU and the relevant authority. The MoU must define roles, reporting lines, rules of engagement, and cost-sharing arrangements, and must explicitly commit the forces to lawful and proportionate conduct.

Both contracts and MoUs must be cleared by the PIU Security Specialist and referenced in the project's SRAMP.

Where circumstances prevent the formalisation of a Memorandum of Understanding (MoU) with public security forces, the contracting entity must nonetheless document the agreed scope, command structure, and conduct expectations through alternative means—such as a written record of meetings, an exchange of letters, or inclusion in the LSMP. These records should capture commitments to proportional use of force, respect for human rights, and incident reporting obligations, consistent with the World Bank's Good Practice Note on Security Personnel.

10.4. Training and Preparedness

The LSRA and LSMP process also require that all engaged security personnel receive project-specific induction and refresher training covering:

- Proportional use of force and firearms in line with the UN Basic Principles on the Use of Force and Firearms by Law Enforcement Officials.
- Respect for human rights, including prohibitions on torture, arbitrary detention, and cruel treatment.
- Prevention of sexual exploitation, abuse, and harassment (SEA/SH).
- Rules for interaction with communities and cultural sensitivity.

Training records must be maintained and verified by the PIU Security Specialist.

10.5. Oversight and Community Engagement

Because the deployment of security forces may heighten community concerns, engagement must be accompanied by:

- Consultations with affected communities to explain the rationale for their use, clarify expected behaviour, and address concerns about militarisation.
- Integration with the Grievance Redress Mechanism (GRM), so that community members can confidentially report misconduct or abuse.
- Oversight through routine spot checks, incident monitoring, and reporting, with findings consolidated in quarterly SRAMP updates to TDB.

10.6. Prohibited Practices

The LSRA and LSMP must make clear that certain practices are not permissible under any circumstances:

- Deployment of unvetted, untrained, or underage personnel.
- Excessive or disproportionate use of force.
- Use of security personnel in project-related disputes (e.g., land or labour disagreements).

- Collusion, extortion, or diversion of project security resources for private or political gain.

Any breach of these standards must be reported immediately and trigger contractual remedies, including suspension or termination of the arrangement, referral for investigation, and corrective action within the SRAMP framework.

11. Considering and Investigating allegations of unlawful acts by security forces

Even where the use of security forces is justified by a Local Security Risk Assessment (LSRA) and governed by contractual or memorandum arrangements, there remains a residual risk that security personnel may commit unlawful acts such as excessive use of force, intimidation, theft, or sexual exploitation and abuse/harassment (SEA/SH). These risks are recognised in the SRAMP framework and must be addressed through clear procedures for reporting, investigation, and remedial action.

11.1. Anticipating the Risk

As part of each LSRA, the potential risks arising from the deployment of security forces must be explicitly analysed. This includes:

- The likelihood of abuse by public or private actors based on past conduct.
- The risk of communities perceiving the project as militarised or complicit in state repression.
- The potential for reputational damage to TDB and the World Bank should abuses occur.

Mitigation measures in the LSMP must then include rules of engagement, training, community liaison, and grievance mechanisms designed to reduce the probability of unlawful acts.

11.2. Reporting Allegations

Where allegations arise, a robust reporting system must be in place:

- Immediate recording of all allegations in the project incident log, whether raised by project staff, contractors, or community members.
- Community access to the project's Grievance Redress Mechanism (GRM), with provisions for confidential and survivor-centred reporting, particularly for SEA/SH cases.
- Notification timelines: All serious allegations must be reported to TDB within 24 hours and to the World Bank within 48 hours, in line with ESF requirements for material incidents.

11.3. Initial Review and Escalation

The PIU Security Specialist conducts a rapid preliminary review of any allegation within 72 hours to establish credibility and immediate actions required. Depending on severity, cases are escalated:

- Minor infractions (e.g., failure to follow access control rules) may be addressed through corrective action and retraining.
- Serious allegations (e.g., excessive force, unlawful detention, SEA/SH) must be escalated to TDB and the Bank and referred to relevant national authorities as appropriate.

11.4. Investigation Procedures

Investigations must be independent, timely, and documented. Depending on the case, they may be led by:

- The PIU Security Specialist (for lower-level infractions), or
- An independent third-party investigator engaged by TDB (for severe or sensitive cases).

Investigations must include evidence collection, witness interviews, and a written report with findings, conclusions, and recommendations. The process must be survivor-centred in SEA/SH cases, prioritising confidentiality, safety, and access to support services.

11.5. Remedial Actions

Based on investigation findings, the following actions may be taken:

- Disciplinary measures such as removal of individuals from the project or termination of security contracts/MoUs.
- Corrective measures including strengthened training, revision of LSMPs, or increased monitoring.
- Referral to competent authorities for prosecution where national law has been breached.
- Support to survivors, including access to medical, psychosocial, or legal assistance.

11.6. Disclosure and Learning

While safeguarding confidentiality, the project must ensure that communities are informed of the outcomes of serious cases and of steps taken to prevent recurrence. All cases must also be documented in SRAMP monitoring reports and fed back into the risk management cycle, ensuring that lessons learned are reflected in updated LSRAs, LSMPs, and training modules.

12. Monitoring and Compliance

Effective monitoring and compliance systems ensure that the Security Risk Assessment and Management Plan (SRAMP) is not simply a theoretical document but a living framework that shapes day-to-day practice on the ground. In volatile FCV environments, where risks can escalate rapidly, a layered monitoring structure is critical for maintaining accountability, enabling adaptive management, and ensuring that protective measures reach those who need them most.

12.1. Integration with the ESMS

Monitoring of security risk management is fully integrated into the broader Environmental and Social Management System (ESMS). Just as environmental and labour safeguards are tracked through contractor reports, PIU oversight, and TDB supervision, so too must security performance be subject to regular verification and documentation. This alignment ensures consistency across all safeguard areas and provides a single accountability framework for the World Bank's oversight.

12.2. Contractor Self-Monitoring

Primary responsibility for implementation rests with contractors and sub-contractors. Each must:

- Conduct site-level monitoring of LSMP implementation, including checks on access control, journey management, training, and compliance with codes of conduct.
- Submit monthly security reports to the PIU, recording incidents, compliance status, and any corrective actions taken.
- Report immediately any material incidents (e.g., major security breaches, allegations of abuse by security personnel) through flash reporting channels.

These obligations must be embedded in contracts so that non-reporting constitutes a breach subject to remedy or sanction.

12.3. PIU Oversight

The PIU Security Specialist provides the second tier of monitoring. Their responsibilities include:

- Reviewing and validating contractor reports.
- Conducting spot checks and unannounced inspections at project sites to verify implementation.
- Interviewing staff and community members to triangulate findings.

- Preparing quarterly consolidated security monitoring reports, integrating incident data, trends, and corrective actions, for submission to TDB.

PIU oversight ensures that LSMPs are not only drafted but are being operationalised on the ground.

12.4. TDB Supervision

TDB's Environmental and Social Unit conducts the third tier of monitoring. This includes:

- Desk reviews of PIU quarterly reports.
- Semi-annual supervision missions where feasible, including site visits to high-risk locations.
- Commissioning independent third-party audits annually or more frequently if incidents or risk escalation warrant.
- Reviewing corrective action plans and, where necessary, requiring additional measures or revisions to the SRAMP.

This supervision ensures that projects remain compliant with TDB's ESMS and the World Bank's ESF requirements, particularly ESS4 on Community Health and Safety.

12.5. Indicators and Key Performance Measures

Monitoring must track both outputs and outcomes. Typical indicators include:

- Outputs: number of LSMPs approved; percentage of staff trained; number of site visits conducted; timeliness of incident reporting.
- Outcomes: reduction in security incidents; improved community perceptions of security presence; demonstrated compliance by public or private security forces with project rules of engagement.

These indicators are reviewed semi-annually and form part of project reporting to the World Bank for co-financed operations.

12.6. Managing Non-Compliance

Where monitoring identifies deficiencies, a graduated response is applied:

- Corrective Action Plans agreed with the contractor or PIU, with clear deadlines.
- Suspension of activities where serious risks to personnel or communities exist.
- Contractual remedies such as withholding payments or contract termination in cases of persistent or wilful non-compliance.

All non-compliance cases must be documented, tracked, and reported in quarterly monitoring updates, with escalation to TDB and the World Bank as required.

13. Summary

This Guidance Note establishes the Security Risk Assessment and Management Plan (SRAMP) as the central instrument for managing security risks in Trade and Development Bank (TDB) projects, particularly those implemented in fragile, conflict-affected, and violent (FCV) environments. It translates broad safeguard principles into a structured, enforceable system that ensures security risks are managed with the same rigour as other environmental and social risks under the TDB Environmental and Social Management System (ESMS) and the World Bank Environmental and Social Framework (ESF).

The SRAMP is both standalone and integrated. As a standalone plan, it provides a complete operational framework that includes contextual analysis, threat identification, site-level risk assessments, proportional mitigation measures, contractor obligations, approval gateways, and crisis management arrangements. As an integrated tool, it dovetails with the ESMS at every stage of the project cycle — from screening, appraisal, and loan documentation through implementation, monitoring, and project closure. This dual role ensures coherence, enforceability, and accountability.

The system rests on several critical foundations:

- **Local Security Risk Assessments (LSRAs).** Conducted at the lowest feasible level — site, activity, or community — to ensure proportionality and context-specificity.
- **Local Security Management Plans (LSMPs).** Developed by contractors in direct response to LSRAs and signed off by the PIU Security Specialist before mobilisation.
- **Contractual cascading.** Security obligations are embedded in procurement and sub-contracts, ensuring that protective measures reach frontline workers.
- **Security approval gateways.** No mobilisation or high-risk activity proceeds without documented clearance.
- **Monitoring and compliance.** A tiered system of contractor self-reporting, PIU oversight, TDB supervision, and independent audits ensures accountability and adaptive management.
- **Use of security forces.** Engagement of public or private security actors is permitted only were justified by the LSRA, governed by written agreements, and subject to strict oversight, training, and accountability.
- **Allegations and investigations.** Clear procedures are in place for reporting, investigating, and addressing unlawful acts by security forces, with survivor-centred support for SEA/SH cases.

By embedding these elements into the project cycle, the SRAMP enables TDB to pursue development objectives in high-risk environments without compromising the safety of

workers, communities, or assets. It enhances operational continuity, compliance, and accountability, while ensuring that security measures are proportionate, rights-respecting, and transparent.

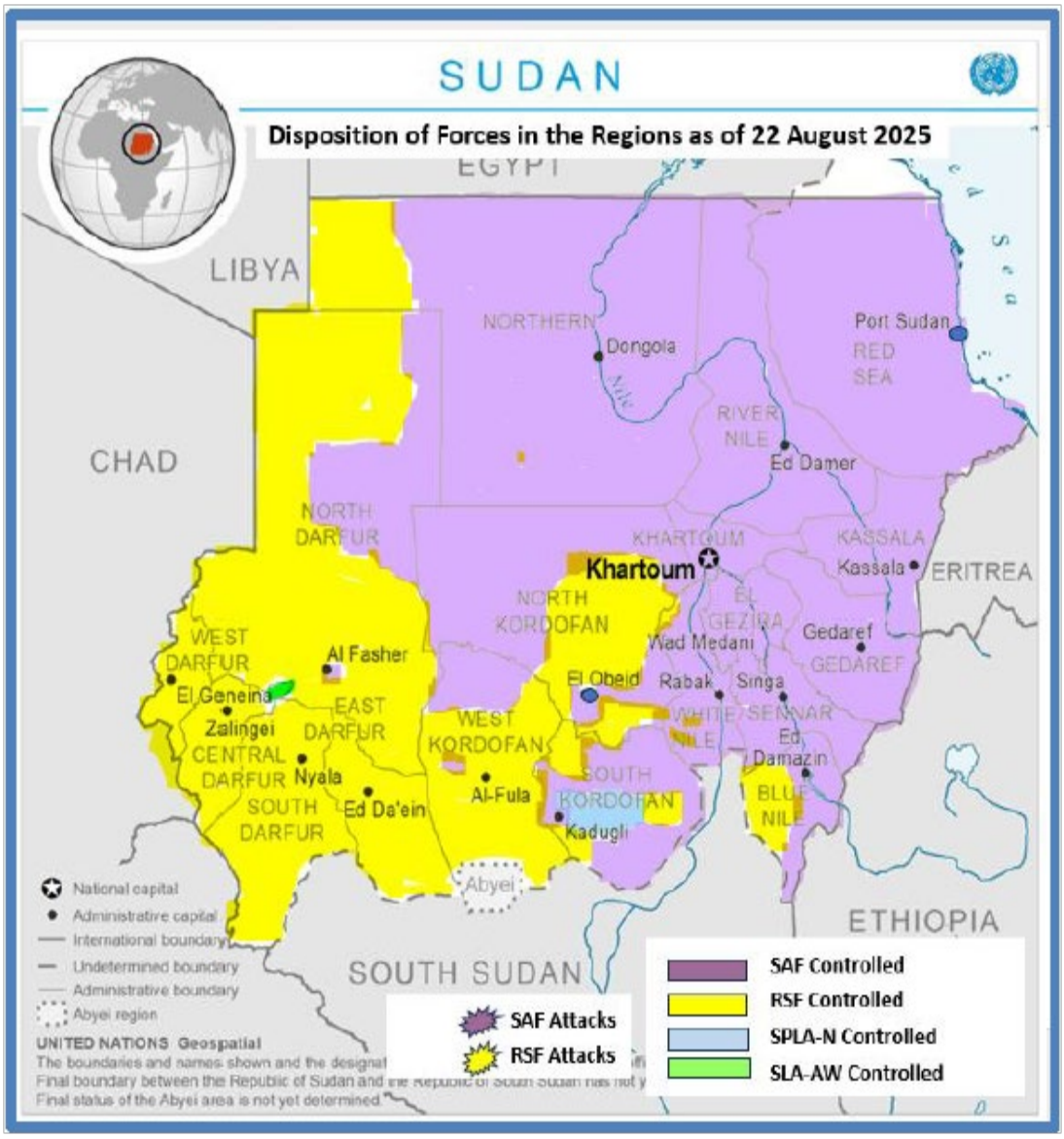
The ultimate aim of this system is to ensure that every individual touched by a TDB project — from a frontline worker digging a trench to a community member attending a consultation — benefits from security risk management that is systematic, enforceable, and fair. In doing so, TDB strengthens its own safeguard framework, upholds World Bank requirements, and contributes to safer, more resilient development outcomes in some of the world's most challenging contexts.

Appendix A – Sudan Security Context

13.1. Broader Security Context

Sudan has been engulfed in a devastating civil war since April 15, 2023, when a power struggle between the national army (Sudanese Armed Forces, SAF) and the paramilitary Rapid Support Forces (RSF) erupted into open conflict. The violence swiftly spread from the capital Khartoum to multiple regions of the country. Intense urban battles, heavy aerial bombing, and artillery shelling have devastated Khartoum and other major cities, causing massive civilian casualties and displacement. As of mid-2025, tens of thousands of people have been killed and over 12 million displaced by the conflict, making it one of the world's largest humanitarian crises. Basic services have collapsed in war-torn areas; over 70% of health facilities in conflict zones are not functioning, and millions face acute food insecurity and famine risks.

The war has effectively split the country along geographic lines. The SAF controls much of the north, east, and central regions (including parts of Khartoum and the Red Sea coast), while the RSF dominates most of the western Darfur region and portions of the south. This has led to de facto rival power centers: the army has operated a provisional administration out of Port Sudan on the Red Sea, whereas the RSF and allied tribal militias have established their own local authorities in Darfur. Both sides have been accused of severe human rights abuses, including indiscriminate attacks on civilians, extrajudicial killings, and sexual violence. The RSF and allied Arab militias, in particular, carried out ethnically-targeted atrocities in Darfur – notably against the non-Arab Masalit community in West Darfur – in what observers have likened to a campaign of ethnic cleansing. Hundreds of villages and entire city districts (especially in West Darfur) have been burned or looted, and thousands of civilians killed in Darfur alone.



Adding to the volatility, other armed groups have exploited the security vacuum. In southern areas, the rebel Sudan People's Liberation Movement–North (SPLM-N al-Hilu faction) ended its ceasefire and clashed with government forces in South Kordofan and Blue Nile states. Tribal militias and communal self-defense groups have taken up arms in several regions, either aligning with one of the main warring parties or pursuing local agendas. In Darfur and Kordofan, long-standing tribal conflicts over land and resources (Arab vs non-Arab communities, pastoralists vs farmers) have re-ignited amidst the chaos. Eastern Sudan has seen rising tensions as well – for example, in late 2024 a clash in Port Sudan between the army and a local Beja militia marked the first violence in the previously peaceful east. Overall, lawlessness and criminality have surged across Sudan: looting of businesses and homes is widespread (even UN aid warehouses have been ransacked), and armed robbery and banditry threaten transport routes.

Humanitarian conditions are dire nationwide. Millions of civilians are trapped in active combat zones like Khartoum and Darfur, with limited access to food, water, or medical care. Relief operations are hampered by insecurity and bureaucratic obstruction – at least 19 aid workers have been killed in the line of duty as of August 2023. Over 3.3 million Sudanese have fled to neighboring countries (especially Chad, Egypt, South Sudan), raising regional security concerns. Those who remain internally displaced often shelter in informal camps that themselves have been targeted by violence (e.g. recent deadly strikes on IDP camps in River Nile and North Darfur states). The longer the conflict drags on with neither side decisively prevailing, the greater the risk that Sudan's security will further fragment, with localized conflicts multiplying and neighboring states feeling the spillover of arms and fighters. International mediation has so far failed to secure a durable ceasefire. In sum, Sudan faces a highly fluid and perilous security environment characterized by multi-faceted armed threats – from conventional warfare between well-armed factions to communal violence and rampant criminality – posing severe risks to any humanitarian or development operations in the country.

13.2. Key Security Threats

Given the above context, the following key security threats have been identified as most relevant to operations in Sudan. These threat types are defined below, along with their typical characteristics (drawing on examples from recent conflict dynamics):

- **Complex Attack:** A coordinated, multi-modal assault by hostile forces employing a combination of weapons (e.g. small arms, grenades, rockets) to maximize casualties. This could involve, for example, an attack on a project site or convoy where assailants use explosives or heavy weapons (such as RPG-7 rockets) followed by gunfire to overrun the location. In Sudan's current war, complex attacks might be carried out by well-armed groups (e.g. an RSF unit or extremist militia) against compounds or convoys associated with the government or international agencies. The assailants' aim is to cause maximum fatalities and/or destroy the target facility.

- **Revenge Killings:** Cyclical retaliatory violence, often rooted in tribal or personal feuds, which can be triggered or exacerbated by project activities or political events. In Sudan, decades of conflict have fostered local vendettas – for instance, one community avenging an earlier attack by another. If a project is perceived to benefit one group, it might reignite dormant grievances leading to targeted murders of individuals from a rival group. These killings can escalate into broader communal clashes, drawing in armed militias and potentially spiralling into prolonged feuds.

- **Ambush:** A surprise attack on vehicles or convoys, often on remote roads or river routes, by armed actors lying in wait. The motive may be robbery or intent to harm. In Sudan, both highway banditry and military ambushes have been prevalent – e.g. RSF fighters or bandits setting up improvised roadblocks to assault and loot civilian convoys. Ambush

scenarios assume the attackers may attempt to kill or injure all passengers and steal assets. Recent examples include armed bandits targeting travel routes (such as the Khartoum–Madani or Darfur supply roads), making any overland movement high-risk.

- **Civil Unrest:** Spontaneous or organized violent disturbances, riots, or protests that can engulf an area and pose a threat to personnel caught in the vicinity. This includes tribal clashes and urban riots. In Sudan, the collapse of authority has led to frequent community-level fighting – for example, clashes between rival ethnic groups or angry protests over shortages that turn violent. Such unrest can rapidly turn an operational area into active conflict, endangering project staff who have no stake in the dispute. A scenario might involve local civilians protesting against authorities or NGOs, leading to rock-throwing, roadblocks, or even gunfire in and around project sites.

- **Hijacking:** The forcible seizure of vehicles (or boats) and their passengers by armed actors, typically to steal the vehicle or cargo, and sometimes to demand ransom. In Sudan's lawless climate, hijackings are a known hazard – armed militia or criminal gangs may intercept project vehicles to steal equipment or commandeer aid convoys. Such incidents carry the risk of violence; the attackers might kill or injure drivers and passengers during the hijacking. There have been reports of aid trucks looted at gunpoint on routes out of Port Sudan and other areas, illustrating this threat.

- **Intimidation/Extortion:** Attempts by armed groups, criminal elements, or even local security forces to intimidate staff or extort money, goods, or services. This could range from militiamen demanding "taxes" or fees at checkpoints, to threats against staff if bribes are not paid. With Sudan's economy in collapse, looting and extortion have become rampant – RSF fighters, for example, systematically looted businesses in Khartoum and have extorted civilians for safe passage. For project teams, this threat means they may face armed individuals pressuring them for cash, equipment, or access, under threat of harm. Fatalities are not the intent in most extortion cases, but violence can occur if demands are refused, and severe psychological trauma or injury is possible.

- **Gender-Based Violence (GBV) & Sexual Exploitation/Abuse (SEA):** The use of sexual violence as a weapon of terror or opportunistic sexual crimes in the conflict environment. In Sudan's war, numerous cases of rape and sexual violence – particularly by RSF and allied militias – have been documented, targeting women and girls in conflict areas. GBV may occur during attacks on communities or displacement camps. Sexual exploitation and abuse, on the other hand, refers to abuses of power for sexual ends – for instance, armed actors or even authority figures coercing vulnerable individuals (including potentially project beneficiaries) into sexual favours in exchange for protection or aid. These acts cause severe physical and psychological harm. All project staff must be alert to the high risk of GBV/SEA in Sudan, both among the population and as a potential threat to female staff.

- **Kidnapping:** The abduction of personnel by armed groups, criminal gangs, or extremists, often with the aim of obtaining ransom or leveraging political concessions. In Sudan, kidnapping has been a lesser-used tactic historically, but the current chaos increases the risk. Criminal gangs or desperate militia could kidnap aid workers or local staff for ransom. There is also the risk of abduction of local community members for recruitment or as hostages. For example, in Darfur's past conflicts, armed groups periodically kidnapped foreigners to bargain with the government. Under current conditions, an incident could involve militants detaining project staff to pressure their organization or to demand money.

- **Armed Robbery / Raid:** An armed incursion into project sites, offices, or residences with intent to steal property or cash, potentially using violence. This could take the form of looters or rogue fighters raiding a compound or work site known to store valuable equipment. Sudan's war has seen countless raids – e.g. RSF troops raiding banks, warehouses, and private homes in Khartoum. A raid on a project compound would likely involve weapons and the possibility of staff being injured or killed if they resist. It assumes not just theft, but also potential physical harm in the process.

- **Compound Takeover / Hostage Situation:** The worst-case scenario of an armed group outright seizing control of an operational site or camp and taking personnel hostage. In Sudan, scenarios could include either faction over-running a base in a contested area or an unruly militia occupying an NGO or PPC office, holding staff until their demands are met. Given the prevalence of armed militias, a worksite could be overrun if located in an insecure zone. This threat entails an armed group taking control and potentially using hostages as human shields or bargaining chips. An example would be if, say, RSF fighters storm a contractor's compound they suspect of aiding the army, detaining staff inside.

- **Politically Motivated Armed Conflict:** The broader risk of being caught in outbreaks of fighting between organized armed groups (SAF vs RSF, or rebel factions) in the project area. In Sudan, full-scale battles can erupt with little warning in contested towns or strategic sites. This threat recognizes that even if project personnel are not targeted, they may become collateral damage during an armed clash or offensive. For instance, if fighting resumes in a ceasefire zone or a new front opens near a project site (such as the conflict spreading into a previously stable state), project staff could be injured by stray gunfire, shelling, or airstrikes. Essentially, it is the risk of the war itself intruding on operational areas, as has happened in places like Gezira and Blue Nile when conflict unexpectedly spread there.

These threats often overlap – for example, a "compound raid" might evolve into a hostage situation, or an ambush might be followed by acts of extortion. The volatile environment in Sudan means the threat landscape can shift rapidly, so continuous monitoring and adaptive

risk assessments are critical. Below, we detail how these threats manifest across Sudan's states, as each region faces a unique mix of security challenges.

13.3. Threats Specific to Sudan's States

The security situation varies widely across Sudan's 18 states. Each state's profile is outlined below, including a brief description of the state, recent significant security incidents (with sources), and a summary of key threats in that area. This state-by-state analysis highlights localized risks that may impact operations:

13.3.1. Khartoum State (Capital: Khartoum)

Description: Khartoum State covers the capital's tri-city area (Khartoum, Omdurman, Bahri) at the Blue–White Nile confluence. Formerly Sudan's administrative and economic hub, it is now the core of the SAF–RSF war. Since April 2023, urban combat has centred on the presidential palace, army HQ, and airport. The RSF spread into residential areas, using civilian sites as cover, while the army launched air and artillery strikes in populated districts. Entire blocks in Khartoum and Omdurman were destroyed, with about 61,000 deaths by early 2025. Government institutions largely collapsed, law and order broke down, and looting spread as many residents fled. By late 2024, SAF regained some sites including the Presidential Palace, though RSF retained control over significant parts of Omdurman and surrounding districts. Humanitarian conditions remain dire: millions face scarce water, power, and health services, with unstable communications.

Significant Security Incidents:

- **April 2023 – Outbreak of War:** Fighting erupted across Khartoum on April 15 as RSF and SAF clashed. Battles near the airport, military HQ, and neighbourhoods killed over 300 civilians and injured thousands. Hospitals were shelled, and 12 of 20 facilities in Khartoum/Omdurman closed by April 18 [1] [2] [3].

- **September 2023 – Market Airstrike:** An SAF strike on Gorro market in southern Khartoum killed at least 40 civilians and wounded dozens, the city's deadliest single incident since war began. Images showed bodies in the street; SAF denied responsibility, blaming RSF [4] [5] [6].

- **September 2023 – Omdurman Shelling:** Artillery strikes devastated residential areas of western Omdurman, killing at least 51 civilians. With hospitals shut and no official response, volunteers struggled to collect bodies and aid the wounded [7] [8].

- **March 2025 – Mosque Attack:** RSF shelled a mosque in East Nile during evening prayers, killing 5 and injuring dozens. The strike highlighted ongoing heavy fighting in Khartoum's outskirts despite SAF advances [9] [10].

Summary: Khartoum remains unstable and dangerous. Fighting continues at lower intensity: SAF holds central areas while RSF strikes from the periphery. Civilians face constant risk from shelling, airstrikes, and stray fire, with thousands killed or injured. Law and order has collapsed, with gangs looting homes, and kidnappings have been reported amid the chaos. Water and electricity are sporadic, worsening the crisis. Any presence risks crossfire, bombardment, or looting. Despite partial SAF control, the city remains a conflict zone with vast humanitarian needs. Without a settlement, Khartoum will stay fractured, with drone and missile strikes posing ongoing threat.

13.3.2. North Darfur State (Capital: El Fasher)

Description: North Darfur, with its capital El Fasher, covers Sahelian plains and part of Jebel Marra. Its population includes Arab nomads and groups like the Fur and Zaghawa. A centre of the 2000s Darfur war, it still hosts many displacement camps. In the current conflict, El Fasher stayed under army control while the RSF seized rural areas and surrounded the city. By mid-2023, RSF and allied militias held Kutum and Kabkabiya, forcing civilians into El Fasher. Fighting reached the outskirts, with artillery and street clashes. Communications were disrupted in 2023, and by early 2024 aid groups described worsening conditions. The RSF maintained pressure, while drone strikes in 2025 hit Sudanese infrastructure such as fuel depots and power stations.

Significant Security Incidents:

- **March 2025 – Tora Market Airstrike:** A Sudanese army strike hit Tora market, 40 km from El Fasher, killing dozens [11]. Rights groups claimed "hundreds" may have been killed, circulating videos and accusing the SAF of a war crime [12] [13].
- **May 2024 – Displacement Camp Attack:** The RSF attacked Zamzam camp, triggering mass flight; violence also reached Abu Shouk. Aid groups reported "tens of thousands fled a displacement camp in El Fasher" [14]. By August 2024, famine was declared in camps under siege [15].
- **August 2025 – Abu Shouk Massacre:** RSF fighters stormed Abu Shouk camp, killing at least 40 and injuring about 19 [16] [17]. Witnesses said residents, including women and children, were shot at close range. The attack, after months of siege conditions, marked further escalation.

Summary: North Darfur is mostly under RSF influence, with some army holdouts. Supported by Arab militias, the RSF has imposed rule through violence, often against non-Arab displaced groups. Massacres in camps and villages have been reported. El Fasher faces siege conditions, with shelling and supply blockages. Civilians face shortages; by late 2023 over half the population was projected in crisis or emergency hunger. Drone warfare has escalated: the RSF used drones against army positions and infrastructure in Sudan, while army strikes hit markets and villages. Humanitarian access is minimal, and aid workers face

RSF hostility and crossfire. Without peace, North Darfur will remain volatile, leaving civilians and agencies highly vulnerable.

13.3.3. South Darfur State (Capital: Nyala)

Description: South Darfur, centred on Nyala, stretches from the Marra highlands to semi-arid savannah. It is one of Sudan's most populous states and a major front in the 2000s Darfur conflict. Its population includes Arab Rizeigat and non-Arab groups such as the Fur and Dinka, with many Fur displaced during earlier violence. When war resumed in 2023, Nyala became a central battleground: the RSF, rooted in the state (its leader Hemedti is Rizeigat), moved to seize the city as the army dug in. By summer, tank and artillery clashes devastated neighbourhoods. RSF secured most of Nyala by late 2023, leaving markets, hospitals, and homes in ruins, and driving out over 600,000 civilians.

Significant Security Incidents:

- **August 23, 2023 – Nyala Market Strike:** A shell hit civilians sheltering near Taiba bridge, killing 35–39 and wounding dozens [18][19]. Many, mostly women and children, were buried in a mass grave amid shelling [20]. Observers saw the strike as emblematic of indiscriminate SAF–RSF shelling.
- **Late August 2023 – Nyala Crossfire:** In the following week, at least 60 more were killed in clashes [21]. RSF occupied neighbourhoods while SAF fired heavy weapons, shells hitting homes. By mid-September, civil society groups warned deaths since April had reached the hundreds, though confirmation was limited.
- **October 2023 – Hospital Air Strike:** Local sources reported an SAF strike near Nyala Teaching Hospital, said to have killed about 20 including patients and staff. The blast damaged the hospital as RSF staged nearby attacks. While unverified, accounts align with later documented SAF airstrikes in Nyala, including one killing 25 in a day [22].

Summary: South Darfur has been engulfed by war, with Nyala – Sudan's second-largest city – largely under RSF control after fierce urban battles. The humanitarian toll is catastrophic: the city was cut off from aid, supplies ran out, and only one hospital functioned by late 2023. RSF and allied militias looted homes, markets, and warehouses. Rural areas remain insecure, with banditry and ambushes along roads leaving Nyala. Unlike West Darfur's overt massacres, South Darfur's conflict has been less directly targeted, though tensions persist, including between Rizeigat and Dinka near the South Sudan border and among Arab clans in RSF-held areas. Human rights groups warn conditions in remote communities are severe but under-reported. Ceasefires in Nyala repeatedly collapsed, and RSF presence dominates; reports say movement often requires their approval, with harassment of civilians. Until a stable ceasefire holds, South Darfur will remain an active warzone, with risks from stray artillery to RSF commandeering NGO vehicles and facilities.

13.3.4. West Darfur State (Capital: El Geneina)

Description: West Darfur borders Chad, with El Geneina as capital. Its Masalit farming population around Geneina and surrounding Arab nomads have long clashed. The state experienced communal violence before 2023, and after the SAF–RSF war it quickly unravelled. RSF and allied militias carried out what observers call organized ethnic massacres against Masalit civilians. From April–June 2023, Geneina was devastated: Masalit districts burned, thousands killed, and Governor Khamis Abakar was abducted and assassinated after accusing the RSF of genocide. By July, the city lay in ruins, with 450,000—mostly Masalit—fleeing into Chad.

In November, RSF struck the last Masalit areas, including Ardamata, killing about 800 in one week per the UN, while locals claimed over 1,300. Satellite imagery showed towns destroyed and mass graves near Geneina. By 2025, West Darfur was reported to be under RSF and allied militia control, but with no functioning government and civilians largely displaced or in hiding.

Significant Security Incidents:

- **June 15, 2023 – Assassination of Governor Abakar:** Governor Khamis Abakar was kidnapped and killed hours after accusing the RSF of genocide in Geneina [23] [24]. Footage showed men in RSF uniforms detaining and executing him [25]. His death was widely viewed as leaving Masalit civilians without protection.

- **April–June 2023 – El Geneina Massacres:** RSF and allied militias besieged Geneina, burning Masalit districts and camps and killing thousands [26] [27]. On May 28, at least 28 Masalit were executed in Misterei, much of it destroyed [28] [29]. By late June, Geneina's hospital was attacked and four lawyers killed [30] [31]. The UN warned these atrocities could amount to crimes against humanity [32].

- **November 2023 – Ardamata Massacre:** RSF fighters overran Ardamata IDP camp, executing hundreds of Masalit [33] [34]. UNHCR estimated 800 deaths in days [35]; survivors described door-to-door killings, looting, and mass arson [36] [37]. This was reported as effectively depopulating Masalit communities in Geneina.

Summary: West Darfur has endured genocidal-level violence and remains extremely dangerous. RSF and allied militias dominate, with the Masalit population largely displaced. Reports describe Arab militias operating with impunity in the absence of law, and inter-communal tensions remain high. Analysts warn that outsiders, especially internationals, would likely face suspicion from RSF fighters.

The state is saturated with weapons, looting is common, and humanitarian access is almost impossible; many non-Arab aid workers were evacuated or killed. Key risks include extreme

violence, looting, and possible targeting of foreigners in a lawless environment. Insecurity also extends across the border, with displacement into Chad and instability along routes. West Darfur is now among the world's most insecure areas, where even heavy security cannot prevent mass violence or war crimes.

13.3.5. Central Darfur State (Capital: Zalingei)

Description: Central Darfur, home to the Jebel Marra mountains, includes Fur, Masalit, and Arab communities. Zalingei, the capital, long hosted IDP camps. Fighting reached the state later than in parts of Darfur, but by mid-2023 RSF and allied militias besieged Zalingei, cutting roads; by June the city faced shortages and clashes on its outskirts. Hamidiya and Hasahisa camps were attacked and cut off, with communications largely lost. When access resumed, the UN reported RSF shelling displaced camps in late 2023. In November, Hasahisa camp was stormed, shelters burned, and survivors fled into town. Humanitarian sites, including Zalingei Hospital, were repeatedly looted. By April 2024, Zalingei lay in ruins, civilians hiding in abandoned buildings.

Significant Security Incidents:

- **June–July 2023 – Siege of Zalingei:** RSF and militia fighters cut off Zalingei and repeatedly attacked its outskirts. Humanitarian compounds were looted in late June (including WFP warehouses), and in early July the main power station was destroyed, plunging the town into darkness (sources: NGO situational reports). Dozens of civilians were reported killed in shelling around the IDP camps during this period (exact tolls unknown due to communications blackout). The Darfur Bar Association noted **Zalingei was under total siege** with no aid in or out[38].

- **August 2023 – Camp Massacre Reports:** Local networks (via Radio Dabanga) reported that in August 2023 armed militias massacred at least 200 people in the Sirba area of Central Darfur (on Zalingei's periphery) during a series of raids[39]. This included the killing of community leaders and burning of villages, mirroring the tactics in West Darfur. (Sirba locality straddles West and Central Darfur, and violence spilled over).

- **November 2023 – Hasahisa Camp Assault:** After the fall of Geneina, RSF/allied forces intensified attacks in Central Darfur. In early November, Hasahisa IDP camp (just outside Zalingei) was overrun survivors recounted how militants besieged the camp, then entered and killed whoever they found. The UN stated Hasahisa camp had been "besieged by RSF" by November, and thousands of residents were forced to flee into Zalingei town for shelter[40]. MSF imagery from April 2024 showed Hasahisa camp completely abandoned and destroyed[41][42].

Summary: Central Darfur's security is dire, though less reported than West Darfur. The RSF captured Zalingei in late 2023 and now controls the city and its surroundings. Governance is militia-based, with RSF commanders and allied Arab tribal leaders exercising power, while lawlessness prevails. Many Fur communities, historically dominant in Jebel Marra, have retreated into rebel-held areas under Abdel Wahid's SLA faction, which has largely remained outside the SAF–RSF war but could still affect future dynamics. Civilians in Zalingei are at RSF mercy, facing looting, sexual violence, and abductions during and after the siege. Displaced people who fled into the city live in desperate conditions; MSF reported in April 2024 that hundreds of children were treated for malnutrition and war wounds in makeshift clinics. Access remains perilous, with conflict-ridden roads and restricted air routes. Central Darfur thus mirrors West Darfur's "do not travel" profile.

13.3.6. East Darfur State (Capital: Ed Daein)

East Darfur, bordering South Sudan, is dominated by Arab pastoralist tribes, chiefly the Rizeigat (Hemedti's tribe) and the Ma'aliya. These groups fought bloody clashes from 2013–2017. When war began in April 2023, the RSF swiftly seized Ed Daein and key routes, reportedly facing limited resistance. The state became a rear base and supply corridor toward Kordofan.

Though initially calmer than West and South Darfur, violence soon resurfaced. Skirmishes between the Rizeigat, including RSF-aligned elements, and the Ma'aliya persisted, including deadly August 2023 clashes in Abu Karinka that killed dozens. Reports suggested some RSF fighters sided with their clans. By 2025, East Darfur remains under RSF administration. Ed Daein serves as a logistical hub with less war damage than other Darfur capitals, but rural areas continue to face tribal unrest and banditry.

Significant Security Incidents:

- **August 2023 – Rizeigat vs. Ma'aliya Clashes:** In mid-August, a major tribal battle erupted in Um Rakuba, Abu Karinka locality. Triggered by a livestock theft, armed Ma'aliya and Rizeigat fought over three days, despite the deployment of some RSF as nominal peacekeepers. At least 47 people were killed in the initial clashes, and subsequent reprisal attacks pushed the toll into the hundreds[43][44]. Whole villages were reportedly torched. This violence underscored that even with RSF in charge, age-old tribal conflicts in East Darfur remain deadly.

- **October 2023 – Clashes in Shearia:** Another bout of fighting occurred between Ma'aliya and Rizeigat in Shearia locality (northern East Darfur) over grazing land. Radio Dabanga reported one clash in early October left 6 dead and many wounded[45]. The conflict was eventually "contained" after local elders intervened, but tensions stayed high. These periodic flare-ups have disrupted movement along roads

and forced local administrations (aligned with RSF) to declare temporary states of emergency.

- **June 2025 – Ambush on South Sudan Border Convoy:** In June 2025, an NGO convoy moving from East Darfur towards the South Sudan border (Kafia Kinji area) was ambushed by unidentified gunmen. The attackers robbed the convoy of vehicles and supplies at gunpoint. While no one was killed, this incident highlighted banditry risk in East Darfur's remote south. (Source: internal security reports, June 2025).

Summary: East Darfur is relatively stable under RSF control and not a frontline in the SAF–RSF war. Ed Daein functions as an RSF hub and has seen less destruction than other Darfur capitals.

The main risks are tribal conflict and insecurity. Rizeigat–Ma'aliya feuds, and occasional clashes with other groups, can erupt suddenly with heavy weapons, drawing in large numbers and endangering civilians and aid workers. Banditry also affects the state, with reports of ambushes on routes toward South Sudan. Travelers have described demands for payments at RSF or militia checkpoints. With widespread arms, militias may target convoys suspected of aiding rivals. Overall, East Darfur avoids major battles but faces persistent localized violence under RSF-dominated order.

13.3.7. North Kordofan State (Capital: El Obeid)

Description: North Kordofan links Khartoum to Darfur, with El Obeid a key transport and garrison hub. The population is largely Arab and Nubian Sudanese, and the city has often been associated with army influence. When war broke out, RSF units advancing from Darfur sought to cut SAF supply lines. By May 2023, fighting reached El Obeid. In June, SAF entrenched at its base using air and artillery while RSF controlled roads and besieged the city. RSF also attacked Al-Rahad garrison. Though SAF retained El Obeid, RSF dominated rural areas and highways. By late 2023, El Obeid was army-held but isolated, while banditry surged on the Khartoum–El Obeid Road. In August 2025, RSF raids in northern villages displaced over 3,000 families and killed 18 civilians. North Kordofan has remained volatile, with shifting frontlines and insecurity.

Significant Security Incidents:

- **June 14, 2023 – Battle of El Obeid:** After weeks of siege, the SAF launched an offensive to repel RSF in El Obeid. Witnesses described airstrikes and artillery bombardment inside the city as the army targeted RSF-held neighbourhood's[46][47]. The RSF, meanwhile, controlled checkpoints and roads, even negotiating with local tribal leaders to manage security in some quarters[48]. On June 14, heavy clashes occurred and by the next day the army claimed it had secured central El Obeid, though fighting continued the outskirts. At least dozens of civilians were killed during these battles (precise figures unknown, but

the Sudanese Doctors Union reported 958 total civilians killed nationwide by mid-June, including those in Kordofan)[49].

- **September 17, 2023 – El Fula Clashes:** (West Kordofan's capital El Fula, but indicative of Kordofan theatre) Clashes erupted between SAF and RSF in El Fula, with RSF fighters briefly overrunning parts of the town (including a police station) before withdrawing. This incident, noted in a UN Security Council report, showed RSF's ability to strike even deeper in Kordofan[50]. It caused panic along the Kordofan/Darfur border and likely led to reinforcements being diverted, impacting North Kordofan's security forces.

- **August 2025 – Village Raids in North Kordofan:** Over early August, RSF elements carried out coordinated raids on 66 villages in eastern North Kordofan (around Umm Rawaba), according to the Sudan Doctors Network[51]. They reportedly drove out thousands of residents, looted properties and livestock, and killed 18 civilians[52]. Many displaced fled into neighbouring White Nile state[53]. This campaign of intimidation suggests the RSF attempting to secure Kordofan's hinterlands and punish communities seen as pro-army.

Summary: North Kordofan remains a fractured frontline. SAF holds El Obeid and likely key sites like the airbase, while RSF dominates much of the countryside and main routes. Travelers between Khartoum and El Obeid face RSF checkpoints and bandit hold-ups, making movement dangerous. The state faces both conventional conflict, with risk of renewed battles for El Obeid, and irregular insecurity from ambushes, hijackings, and militia activity. Banditry, a longstanding issue in the region, has worsened during the war. El Obeid has also received large numbers of people fleeing Darfur and Khartoum, adding strain on local resources and heightening tensions. RSF's presence adds unpredictability: they have looted and displaced civilians, as in August 2025, though not destroyed towns as in Darfur. For operations, El Obeid offers relative calm under SAF, but surrounding areas are RSF-held or lawless. Road ambush risks are significant. Overall, security is tenuous, requiring caution and real-time intelligence.

13.3.8. South Kordofan State (Capital: Kadugli)

Description: South Kordofan, centred on the Nuba Mountains, has long been contested due to the SPLM-N (al-Hilu) rebellion. Its population includes Nuba groups (often SPLM-N aligned) and Arab Misseriya pastoralists. Since 2011, SPLM-N controlled much of the rural Nuba Mountains, while SAF held towns like Kadugli. When the SAF–RSF war began in 2023, RSF advanced from Darfur toward Kadugli, while SPLM-N renewed attacks on army positions. By June 2023, clashes in Blue Nile and South Kordofan raised fears of a broader front. RSF attacked Kadugli in mid-June but were repelled, while SPLM-N surrounded the city claiming to shield civilians. Kadugli remained under SAF control but was increasingly pressured by its isolation near rebel-held areas. On August 16, SPLM-N shelled Kadugli, killing civilians and ending its ceasefire with Khartoum. Sporadic SAF–SPLM-N clashes followed, and

humanitarian conditions in rebel areas, already dire from years of blockade, deteriorated further.

Significant Security Incidents:

- **June 2023 – SPLM-N Offensive:** In the third week of June, the SPLM-N (al-Hilu) rebel group launched coordinated attacks on Sudanese army positions in South Kordofan, breaking a long truce. One attack targeted an SAF base near Kadugli on June 16, with shelling hitting parts of Kadugli town and causing civilian panic[54]. Another rebel attack occurred in Dilling area. These incidents marked the revival of the "Two Areas" war; hundreds of civilians fled Kadugli and other towns into SPLM-N zones or northwards.

- **August 2023 – Kadugli Shelling:** On August 16, Kadugli came under artillery fire from SPLM-N forces positioned in the Nuba hills[55]. UNITAMS (UN mission) reported this shelling and condemned it. The shelling killed at least 3 civilians (according to local media) and led to a temporary evacuation of Kadugli's remaining humanitarian staff. The SPLM-N likely aimed to pressure SAF to abandon some outposts. This was accompanied by intensified fighting on Kadugli's outskirts between SAF and SPLM-N.

- **January 2024 – Road Ambush in Rashad:** In early 2024, an SAF logistics convoy moving between El Obeid and Kadugli was ambushed in the Rashad locality (likely by SPLM-N or allied militia). Several army trucks were destroyed and 7 soldiers killed (as per a Sudanese Tribune report). The convoy was carrying food supplies; after this, road movement to Kadugli virtually halted due to ambush risk.

Summary: South Kordofan faces overlapping conflicts involving SAF, RSF, and SPLM-N, with the latter entrenched in much of the Nuba Mountains. Areas such as Kauda and Heiban have long been under SPLM-N administration, now further isolated as Khartoum is preoccupied. Kadugli and other government pockets remain flashpoints, at risk from SPLM-N offensives and occasional RSF activity from Darfur or allied militias. This makes Kadugli especially volatile: aid operations could be caught in crossfire or exposed to raids. The state also has a record of Nuba–Misseriya clashes, which could resurface if security deteriorates. SAF prioritizes holding Kadugli, but renewed battles cannot be ruled out. Landmines and UXOs remain from earlier wars. Humanitarian needs are severe in SPLM-N areas, where services are scarce and prolonged isolation has deepened hardship. Access requires negotiating with SPLM-N and navigating SAF restrictions, making any operation highly challenging.

13.3.9. West Kordofan State (Capital: Al-Fulah)

Description: West Kordofan, reinstated in 2013, lies between South Kordofan and Darfur. It produces oil near Heglig and is mainly inhabited by Misseriya, with some Rizeigat grazing. The state has experienced historical conflicts linked to Darfur and the South Sudan border, including Misseriya–Dinka disputes in Abyei. In September 2023, RSF attacked SAF in Al-Fulah, but the

army repelled them. RSF reportedly moved through parts of the state, contributing to local insecurity. With SAF redeployments, banditry and looting increased along key roads, including the Khartoum–El Obeid–Muglad corridor. Inter-communal tensions flared, such as Misseriya–Nuba clashes around Lagawa. By 2025, West Kordofan faces low-intensity insecurity: sporadic SAF–RSF clashes, tribal militias vying for influence, and threats to oil infrastructure, which so far remain intact.

Significant Security Incidents:

- **September 17, 2023 – Attack on Al-Fulah:** RSF units launched an assault on Al-Fulah, clashing with the army at a military post and the governor's office. The clashes lasted a day, with gunfire in the town and some shells landing in residential areas (causing at least a few civilian injuries as per local media). The UN noted this incident as the first major fighting in West Kordofan[56]. The RSF withdrew to avoid overstretch, but it demonstrated the town's vulnerability.

- **October 2023 – Tribal Clashes in Lagawa:** In early October, conflict erupted in Lagawa between armed Misseriya youths and local Nuba residents, reportedly over a land dispute and rumours of Nuba siding with SPLM-N. This led to dozens of casualties and the burning of several villages around Lagawa (reports by Radio Dabanga and NGO protection briefs). SAF troops were absent, and the violence was contained only after elders negotiated a truce. This underscored how communal violence can ignite without state control.

- **May 2025 – Ambush near Abyei Road:** An armed group (unclear affiliation, possibly bandits or rogue RSF) ambushed a convoy of commercial trucks near the Abyei junction in southern West Kordofan. The attackers looted fuel and goods; two drivers were killed in the attack (source: humanitarian security incident database, May 2025). This area, near the disputed Abyei region, has long been volatile and is now even less secure with the war's overflow.

Summary: West Kordofan is marked by partial lawlessness. SAF retains main towns such as Al-Fulah, En Nahud, and Meiram, while RSF elements and allied militias are reported to move through rural areas. The state's terrain makes clandestine movement easier for armed groups. Security concerns include the possibility of renewed SAF–RSF clashes, tribal violence involving heavily armed Misseriya, and banditry on major roads. Oil facilities near Heglig remain under SAF guard, though they could become flashpoints if fighting spreads. Proximity to Abyei, where UN peacekeepers are stationed, adds further risk. Though not a constant frontline, conditions can shift quickly, requiring contingency planning and careful community engagement for any operations.

13.3.10. Blue Nile State (Capital: Ed Damazin)

Description: Blue Nile, in Sudan's southeast bordering Ethiopia and South Sudan, has a diverse population (Ingessana/Berta, Hausa, others) and was an SPLM-N (Agar faction) stronghold. The 2020 Juba Peace Agreement gave it autonomy, with Malik Agar joining Sudan's Sovereignty Council. Though relatively calm entering 2023, tribal tensions had resurfaced after Hausa–Berta clashes in 2022 killed hundreds.

When the SAF–RSF war began, Blue Nile saw limited fighting. The Agar faction, aligned with SAF, helped keep the state largely out of the wider conflict. In late June 2023, SPLM-N (al-Hilu) attacked Kurmuk near the Ethiopian border, marking the state's first war-related clash. The UN reported hundreds fleeing into Ethiopia during those battles.

RSF presence remained minimal. Local unrest persisted: Hausa–tribal fighting in Ganis village killed five on April 5, 2023. Ethiopia's instability also spilled over, with Tigrayan and Benishangul refugees in camps and occasional border skirmishes. By 2025, Blue Nile has been comparatively calmer than many states, though unresolved grievances and rebel threats remain.

Significant Security Incidents:

- **April 2023 – Tribal Clash (Hausa vs Funj):** On April 5, just before the national war erupted, a clash between Hausa and Funj tribespeople in Blue Nile's Wad al-Mahi locality left 5 dead[57]. It started over a land dispute. This incident is part of the earlier ethnic strife that killed hundreds in mid-2022, reminding that ethnic grievances are unresolved.

- **June 26, 2023 – Kurmuk Fighting:** Residents and activists reported that SPLM-N (al-Hilu) rebels attacked Kurmuk (southern Blue Nile) around June 25–26[58]. Hundreds of civilians crossed into Ethiopia for safety[59]. The details are scant (media could not confirm casualty figures), but this suggested the Hilu faction was testing government defences. SAF later stated it repelled the attack, but tensions between the army and SPLM-N remained high afterwards.

- **September 2023 – Border Skirmish:** In mid-September, a Sudanese border guard patrol exchanged fire with Ethiopian militiamen along the Blue Nile/Ethiopia frontier (near Geisan). No official death toll given, but local sources said 2 Sudanese soldiers were injured. This raised alarms about the volatile border, though both governments played it down. (Source: Addis Standard quoting Sudanese officials, Sept 15, 2023).

Summary: Blue Nile has so far avoided the full-scale battles seen elsewhere, partly due to Malik Agar's alignment with SAF and the absence of a strong RSF presence. Government control of Damazin and key towns remains intact, but the state is fragile. The June 2023 Kurmuk raid showed the risk of renewed SAF–SPLM-N conflict. Meanwhile, inter-ethnic grievances linger, as seen in the April 2023 tribal clash. Ethiopia's instability adds pressure, with refugee

inflows and occasional border skirmishes. As of 2025, Blue Nile is calmer than most war-affected states, but risks persist — localized violence, smuggling, and the possibility of a new rebel front.

13.3.11. White Nile State (Capital: Kosti)

Description: White Nile State, just south of Khartoum along the White Nile, borders South Sudan. It is an agricultural hub (sugar plantations, crops) and houses a large refugee population from South Sudan. The capital Kosti (twin town Rabak) lies on the Nile and is a key transit point to South Sudan. White Nile has remained under SAF control throughout the current war and has not seen frontline combat. However, the state has absorbed hundreds of thousands of people fleeing Khartoum and other war zones, straining local resources. The influx of IDPs has heightened ethnic and social tensions in some areas. In May 2023, for instance, tribal clashes erupted in Kosti between local groups and newcomers: what began as a quarrel over a stolen cell phone escalated into fighting between Nuba and Fellata (West African origin) youths, leaving 5 people dead (4 men and 1 woman) and homes burned. Police intervened but unrest flared for three days. This indicates that even distant from the main war, White Nile has its own security issues. Additionally, crime rates have risen – Kosti saw increased incidents of theft and armed robbery, possibly due to the economic desperation of IDPs. White Nile's border with South Sudan poses a potential risk too: while relations are mostly peaceful, smuggling and armed bandit crossings occur (there have been past instances of South Sudanese armed youth raiding into White Nile for cattle, though infrequent). In late 2024, cholera and disease outbreaks in crowded camps (like at Khor Al-Waral refugee camp) led to unrest, with refugees staging protests over aid shortages – local authorities worried these could turn violent.

Significant Security Incidents:

- **May 8, 2023 – Kosti Tribal Clashes:** Over several days, violence between Nuba and Fellata communities in Kosti resulted in 5 deaths and many injured[60][61]. The trigger was reportedly a petty theft altercation that spiralled into ethnic revenge attacks. By May 9, police had restored order, but a number of houses were attacked and a vehicle torched during the melee[62]. This incident underscores the volatility that sudden social stresses (like an IDP influx) can bring.

- **July 2023 – Protest at Joda Border:** Approximately 200 Sudanese (White Nile locals and Khartoum IDPs) protested at the Joda border crossing into South Sudan, demanding to be allowed to evacuate south. When border officials restricted crossing, there was a scuffle and some protestors started throwing stones. South Sudanese border guards fired warning shots; in the chaos, one man was accidentally shot and killed (reported by Radio Tamazuj, July 15, 2023). This highlights how desperate conditions can spark unrest with cross-border implications.

- **April 2025 – Displacement Camp Tensions:** In April 2025, at a large IDP camp near Al-Jabalain, fights broke out during an aid distribution between host community members and IDPs over who should receive supplies first. Sticks and knives were used; 2 people were killed and several wounded (as per an internal UN security memo, April 2025). The army imposed a curfew around the camp afterwards. This shows ongoing friction over resources.

Summary: White Nile State is relatively stable in military terms – it is firmly in SAF hands and has not been directly attacked by RSF. Daily life continues more normally here than in bombed-out war zones. However, it is under immense humanitarian pressure as a rear-area sanctuary. The huge displacement into White Nile (including many from Khartoum and Darfur) creates the risk of social unrest, crime, and inter-communal violence. The Kosti clashes demonstrate that communal harmony can be fragile. Additionally, the economy of White Nile is hit hard – fuel and commodity shortages (due to war disruptions) sometimes spark localized protests or highway robbery incidents on the main Khartoum-Kosti Road. For project operations, White Nile might serve as a logistical base (given relative security), but one must remain alert to community grievances and petty crime. Security threats here are more internal/local: riots in crowded aid settings, theft, the possibility of opportunistic violence. One also cannot rule out RSF infiltration or sabotage attempts – though not reported so far, RSF agents could try to disrupt the vital Nile River port at Kosti which is a supply route. Moreover, White Nile's proximity to Khartoum means if the capital fighting shifts or if SAF were to collapse mini riot/conflict could spill into northern White Nile. As of now though, the state functions as a comparative safe zone needing support for the displaced. Ensuring good relations with local authorities (SAF-aligned) and community leaders is key to mitigating conflict in White Nile. The state exemplifies how the indirect impacts of war (mass displacement, competition for aid) can create serious security concerns even away from the frontlines.

13.3.12. Sennar State (Capital: Singa)

Description: Sennar is a small agricultural state along the Blue Nile, just downstream of Blue Nile State. Its capital Singa and the larger town of Sennar (site of a major dam) are the main urban centers. The population is predominantly Arab Muslim farmers. Sennar has not seen active combat in the SAF-RSF war; it lies east of Khartoum and has been under solid SAF control. However, it borders conflict-affected areas (Blue Nile to the south, Gezira to the north). In late 2023, as RSF forces pushed south of Khartoum, there were fears they might penetrate Sennar, but instead they captured Wad Madani in Gezira and stopped. Sennar has been relatively quiet, serving as a transit area for people fleeing Khartoum toward Ethiopia. One impact was a heavy influx of IDPs into Sennar's towns and villages, straining local services. This has led to occasional tensions – for example, there were reports in October 2023 of Sennar residents protesting high food prices and blaming IDPs, though it didn't turn violent. Historically, Sennar also has some ethnic diversity (there are Fellata communities and others) and has seen minor tribal incidents. In September 2023, Radio Dabanga noted a clash in East Sennar between local farmers and nomads over cattle trespassing, resulting in 2 deaths – a typical seasonal dispute. Overall, Sennar's security environment during the war has been one of latent tensions

but no major violence. It remains an SAF rear area with checkpoints on roads to monitor any RSF infiltration.

Significant Security Incidents:

- **July 2022 – (Pre-war) Ethnic Riot:** (For context) In mid-2022, a spillover of Blue Nile's ethnic conflict led to protests by Hausa communities in Sennar. In one incident in Sennar town, a riot on July 19, 2022, led to 3 people killed by security forces. This is before the current war but is indicative of underlying ethnic strains (Hausa vs others) that could resurface.

- **September 2023 – Farmer-Nomad Clash:** In Sennar's Dinder locality, in Sept 2023, Arab nomadic herders clashed with local farmers after cattle entered farms. Two farmers were shot dead and several huts burned (reported by Dabanga on Sept 20, 2023). The local authorities deployed police to calm the situation. This shows that even with war elsewhere, resource conflicts persist in Sennar's rural areas.

- **March 2024 – Security Sweep Arrests:** Sennar authorities arrested a cell of 5 individuals allegedly plotting to sabotage the Sennar Dam, accusing them of RSF links (source: Sudan Tribune, Mar 2024). No attack occurred, but this incident reveals government concern about sabotage threats to critical infrastructure in Sennar.

Summary: Sennar remains relatively stable and largely untouched by direct fighting. The main security issues here stem from being a support zone and the ripple effects of the war: a heavy IDP presence (which could fuel disputes or crime), and the risk of sabotage or covert RSF activity given its proximity to conflict fronts. The SAF likely has a strong grip on Sennar (to protect the dam and agricultural assets), so an open RSF attack is unlikely unless the front dramatically shifts. That said, banditry on highways is a mild concern – some reports of robberies on the Khartoum-Sennar Road at night have emerged, as policing has thinned due to war redeployments. Inter-communal relations need monitoring; latent grievances (like Hausa marginalization or farmer-herder tensions) could flare up, especially under economic stress. From an operational perspective, Sennar might function as a relatively safe base for accessing Blue Nile or Gezira, but teams should still implement basic security precautions. These include community engagement to defuse any resentment toward aid recipients, and coordination with local security forces who remain active. In sum, Sennar is calm but not immune: it's a place where the war's secondary effects – refugees, resource scarcity – could spark localized issues. Maintaining that calm will depend on continued effective local governance and no spillover of active combat into the state.

13.3.13. Al Jazirah (Gezira) State (Capital: Wad Madani)

Description: Al Jazirah (Gezira) is Sudan's central agricultural heartland, lying just south of Khartoum between the Blue and White Niles. It's home to the massive Gezira Scheme irrigation project. The capital Wad Madani is Sudan's second-largest city and a key economic center. For the first six months of the war, Gezira was a refuge for people fleeing Khartoum and remained peaceful. However, by late 2023, the conflict spread into Gezira. As RSF pressure on Khartoum persisted, they maneuvered into Gezira from the south. In October 2023, violence was reported "spreading south of Khartoum towards Gezira", and by December 2023 the RSF seized control of Wad Madani, the state capital, in a shocking development. This effectively opened a new front; Wad Madani had been hosting many displaced and its fall caused further panic and displacement. Under RSF occupation, reports indicated RSF fighters looted government offices and some businesses but attempted to administer the city with allied local leaders. Meanwhile, rural Gezira saw insurgent-style attacks: for example, in June 2024 the RSF attacked Wad al-Nawara village (northern Gezira), killing at least 100 civilians. This massacre was one of the deadliest in central Sudan and was viewed as the RSF eliminating perceived pockets of resistance. By mid-2024, a large portion of Gezira (including its western parts) remained contested, though there were unconfirmed reports that the army launched operations in 2024 to encircle Wad Madani. The status as of 2025 seems to be that RSF retains strong influence in Gezira, and much of the state, especially the capital, has not returned to government control.

Significant Security Incidents:

- **October 2023 – Fighting Near Madani:** As the RSF moved toward Gezira, skirmishes erupted on the outskirts of Wad Madani. In mid-October, villages north of Madani saw clashes; an estimated 20 civilians died in crossfire (per local activists). This was a prelude to wider violence and signalled the war's expansion[63].

- **December 2023 – Fall of Wad Madani:** The RSF launched a swift assault on Wad Madani in early December. Within days, they overwhelmed police and any SAF units and took control of the city[64]. Residents reported street fighting and sniper fire as the army retreated. After capture, RSF hoisted their flags on government buildings. More than 10,000 people were killed in Sudan by that point in the war[65], and Madani's fall added to that toll (exact Madani casualties unknown, but believed to be in the hundreds). This was a major strategic and psychological blow to the government.

- **June 2024 – Wad al-Nawara Massacre:** On June 20, 2024, RSF forces attacked Wad al-Nawara, a large village in northern Gezira, executing civilians and burning homes. Approximately 100 people were killed (including many women and children)[66]. The UN humanitarian chief cited this attack when warning of the conflict's brutality in new areas. It was one of the worst atrocities in Gezira state and caused an outcry, with many survivors fleeing further south.

Summary: The incursion of war into Al Jazirah upended its status as a safe haven. Gezira is now a frontline region, especially its northern half. The RSF's occupation of Wad Madani demonstrates their reach into the country's center. This poses serious security concerns: large numbers of RSF fighters (likely battle-hardened from Khartoum) are present, and they have reportedly fortified positions. Civilians in Madani live under a climate of fear, with reports of arbitrary arrests, looting, and even incidents of gender-based violence by occupying forces (though less systematically reported than Darfur). The continued RSF presence also means ongoing conflict – the army will likely attempt at some point to reclaim this key city, which would result in heavy fighting. For any operations, Gezira is highly risky now. Whereas in mid-2023 one could work in Gezira relatively safely, by 2025 it entails navigating an active conflict zone with an occupying force. Risks include potential combat operations resuming (if SAF offensives occur), indiscriminate violence by RSF (the June 2024 massacre shows their willingness to terrorize locals), and all the hazards of a lawless environment (robberies, harassment at checkpoints, etc.). Additionally, explosive remnants of war might be an emerging threat in areas of heavy fighting around Madani. On the other hand, southern parts of Gezira might still be under SAF and quieter, but they border conflict zones. The overall summary is that Gezira's security has deteriorated from stable to volatile. It's a stark example of how Sudan's conflict continues to spread. Any program in Gezira now would likely need to coordinate with RSF authorities (in Madani) or operate only in SAF-held pockets – both scenarios fraught with difficulty. Until the balance of power shifts or a truce is reached, Al Jazirah remains in the grip of conflict, a dramatic change from its previous role as Sudan's breadbasket and refuge.

13.3.14. Red Sea State (Capital: Port Sudan)

Description: Red Sea State covers Sudan's northeastern coast, including the critical Port Sudan city (the country's main seaport) and a predominantly Beja ethnic population in the hinterland. Remarkably, for much of the war, Red Sea State – and Port Sudan in particular – was peaceful and became the de facto administrative center for Sudan's internationally recognized government. Thousands of Khartoum evacuees, foreign diplomats, and aid agencies relocated to Port Sudan, which served as a lifeline for humanitarian imports. However, starting May 2025, the conflict dramatically encroached via air: the RSF, having acquired armed drones, opened a new front by striking Port Sudan with drones. In early May 2025, over consecutive days, drones hit Port Sudan's strategic facilities, including fuel depots, the port's container terminal, and the main power station, causing massive fires and citywide blackouts. This represented a major escalation and ended Port Sudan's status as a safe haven. Aside from these external attacks, internal Red Sea politics have also posed risks. The local Beja community has a history of protests over marginalization – notably, they blockaded the port in 2021. In late 2024, some Beja tribal elements, frustrated with the army's dominance, reportedly armed themselves. In November 2024, clashes were reported in Port Sudan between an army unit and a Beja militia (linked to a faction of the Beja High Council), marking the first local armed confrontation. Though small-scale, it signaled potential for Red Sea State's own grievances to ignite. The army quickly contained that incident, but tensions remain.

Significant Security Incidents:

- **May 4–7, 2025 – Drone Blitz on Port Sudan:** Over four days, the RSF launched sustained drone strikes on Port Sudan, targeting critical infrastructure. One strike on May 6 torched the country's largest fuel storage site, sending up an enormous plume of black smoke and knocking out fuel supplies[67][68]. Another strike hit an electricity substation, causing a citywide power outage[69][70]. The Port Sudan airport was also struck, as were port facilities[71][72]. At least 6 people were killed and dozens injured in these strikes (according to Reuters and local officials). This was unprecedented, as it was the first direct attack on Port Sudan since the war began, and it imperilled humanitarian operations dependent on the port.

- **November 2024 – Army vs. Beja Militia Skirmish:** A **shootout in Port Sudan** occurred between Sudanese army troops and armed men from a Beja tribal militia (reportedly affiliated with a renegade local leader). This happened near a military warehouse in the city's outskirts on a night in November. Gunfire lasted a couple of hours; 3 soldiers and 2 militants were reportedly killed (per Africa news)[73]. The incident heightened anxiety that eastern tribal tensions could boil over and complicate the war.

Summary: Red Sea State's security context has shifted from calm to potentially threatened on two fronts: external attacks by RSF drones and internal unrest by local actors. Port Sudan, once a secure operating base, is now within reach of RSF long-range capabilities. The May 2025 drone offensive opened a worrying chapter – it demonstrated that even the seat of the government's rump administration is not off-limits to attack. This means any facility or convoy in Port Sudan could be a target for aerial attack going forward, including humanitarian warehouses or offices. Mitigation (e.g. dispersal of assets, hardening of shelters) is necessary for such threats. Meanwhile, tribal stability in Red Sea is a concern. The Beja community's grievances (over political representation and economic benefits) persist; if they escalate protests or militancy, it could disrupt port operations (as seen in 2021) or even result in armed confrontations as in late 2024. However, local Beja leaders have also declared they don't want war in the east and will protect the region as a refuge, suggesting a division of opinions within the community. For operations, Red Sea State still offers the largest logistics hub (Port Sudan) and a functioning civil administration, but the risk profile has risen. Key threats: air/drone strikes (a new reality in 2025), the possibility of civil unrest or riotous protests, and opportunistic crime given the influx of people (there have been incidents of theft targeting aid shipments reported). Additionally, one cannot ignore that if the war stalemates, factionalism within the army or local power struggles (e.g. between army/security and Beja groups) could make Red Sea a secondary conflict zone. In summary, Red Sea State now demands security measures almost as robust as inland conflict states: aerial threat detection, community engagement with Beja leaders to ensure no misunderstandings, and contingency plans for evacuation if Port Sudan becomes unsafe. It remains critical to Sudan's aid pipeline, so maintaining relative peace here is of utmost importance – but that peace is no longer guaranteed in the face of expanding conflict dynamics.

13.3.15. Kassala State (Capital: Kassala)

Description: Kassala, bordering Eritrea and Ethiopia, is known for its picturesque Taka Mountains and its mix of Beja, Arab, and other groups. Before the war, Kassala had episodes of tribal tension (including protests by Beja) but was generally stable. During the current conflict, Kassala has stayed under government (SAF) control and did not experience fighting. However, like other eastern regions, it has felt indirect impacts. Kassala city became a waystation for people fleeing Khartoum towards Egypt (via Port Sudan) or Ethiopia. Security forces in Kassala have been on high alert to prevent RSF infiltration or arms smuggling. One notable challenge has been the Eritrean border: there were concerns early in the war that Eritrean fighters or opposition might take advantage, but no significant cross-border incidents occurred. The more salient issue has been refugee flows – Kassala hosts long-standing Eritrean refugee camps, and new arrivals from Khartoum also settled. This has put pressure on resources and could stir local discontent. Additionally, Kassala saw some tribal demonstrations in solidarity with the army: for instance, in May 2023, hundreds of Beja tribesmen rallied in support of the SAF and to denounce the RSF. Those were peaceful but underline how eastern Sudan's tribes are watching the conflict. Another facet: smuggling and human trafficking, which have historically plagued Kassala's porous borders, may be on the rise as governance weakens – reports indicate increased movement of weapons and people through Kassala's borderlands since mid-2023 (per a Chatham House analysis on border conflict). Overall, Kassala remains non-violent but fragile, with heightened security measures in place.

Significant Security Incidents:

- **May 2023 – Pro-Army Rally:** In the first weeks of the war, Kassala city saw large pro-army demonstrations. On May 5, 2023, hundreds of Beja tribesmen marched, some demanding arms to fight the RSF[74]. The protest was orderly, but speakers warned they would resist any RSF incursion. This illustrated support for SAF but also the potential for tribal mobilization.

- **Jan 2024 – Border Shootout:** In January 2024, a clash was reported between Sudanese border guards and unknown armed persons (suspected traffickers) near Kassala's Lukdi border post. Two traffickers were killed and one Sudanese policeman injured (source: Sudan Tribune Jan 22, 2024). This highlights how criminal violence at the border continues amid the war.

Summary: Kassala so far stands as one of Sudan's quieter states in terms of direct conflict. SAF retains full control, and the RSF has not attempted any attack there (likely due to lack of local presence and the distances involved). This makes Kassala relatively safer for now. However, underlying issues require caution. Tribal politics (especially Beja grievances and youth militancy) could suddenly erupt, especially if they feel sidelined in any political process or if economic conditions worsen. Also, refugee and IDP pressures can create friction with host communities. Security forces in Kassala are stretched – prioritizing border security and policing

smuggling, which means internal security could suffer. For operations, Kassala might be a viable area to work (it's accessible and infrastructure is intact), but risk factors include theft and smuggling networks, and the possibility of becoming a flashpoint if, for example, a local protest turns against foreign organizations (as the August 2025 mini riot showed). Additionally, any spillover from neighboring Eritrea or Ethiopia (though currently unlikely) could change the calculus. In summary, while Kassala is calm compared to war-torn states, it is in a delicate balance: the state could remain peaceful with careful management, or instability could creep in via border insecurity or local unrest. Continuous engagement with community leaders and monitoring of border areas will be key to maintaining the security that exists.

13.3.16. Gedaref (Al Qadarif) State (Capital: Al-Qadarif)

Description: Gedaref lies south of Kassala, bordering Ethiopia (particularly the Amhara region). It is an agricultural breadbasket, known for sesame and sorghum production, and the locus of the al-Fashaga border dispute with Ethiopia. Gedaref's capital Al-Qadarif has remained under SAF authority and hasn't witnessed fighting during the current war. However, Gedaref has been directly impacted by external conflict – during Ethiopia's Tigray War (2020–2021), tens of thousands of refugees crossed into Gedaref, and skirmishes erupted over al-Fashaga, a fertile border strip long farmed by Ethiopians but claimed by Sudan. In late 2020 and again in late 2021, the Sudanese army and Ethiopian militias exchanged deadly clashes in that area, resulting in Sudan asserting control over much of Fashaga. By 2022, Sudan held Fashaga (a "Sudanese victory" in that conflict), but the situation remains a latent conflict – Ethiopian militias occasionally stage incursions. During Sudan's current war, vigilance on the Gedaref-Ethiopia front remained high to guard against any opportunistic move by Ethiopia or local armed groups, though Ethiopia has been preoccupied with its own issues and relations somewhat improved in 2023. Internally, Gedaref has a diverse population (including many refugees/IDPs). It saw some Hausa vs other tribe tensions in 2022 akin to Blue Nile's conflict, and solidarity protests thereafter. In the current timeline, no major violence in Gedaref has been reported, but minor incidents occur, like cattle raiding on the border or refugee camp security problems. One significant development: the Sudanese war diverted attention and troops, which some feared could create a security vacuum in Fashaga. In July 2025, local sources reported Ethiopian farmers (possibly backed by militia) re-entering parts of Fashaga to plant crops, leading to a standoff with Sudanese troops – fortunately not escalating to firefight, but it shows the dispute is alive (source: Africa Intelligence, July 31, 2025).

Significant Security Incidents:

- **June 2022 – Al-Fashaga Clashes:** (Pre-current-war) On June 22, 2022, Ethiopian militia attacked a Sudanese outpost in Al-Fashaga, killing 7 Sudanese soldiers, which led Sudan to angrily reinforce the area. This was prior to the 2023 war but is crucial context for ongoing tensions[75]. It set the stage for Sudan's robust stance in Fashaga.

- **October 2023 – Border Skirmish:** Sudanese farmers in Fashaga reported an armed confrontation with Ethiopian gunmen on October 5, 2023. No fatalities were officially reported, but shots were exchanged, and a tractor was burned (reported by Dabanga). This incident occurred while Sudan's central government was distracted by war, hinting that local actors took advantage.

- **July 2025 – Tense Fashaga Standoff:** Sudanese military sources observed hundreds of Ethiopian farmers, escorted by Amhara militia, resettling parts of Fashaga in planting season[76]. Sudanese troops confronted them; a tense standoff ensued for days until high-level talks eased it (no open fighting). However, both sides have since kept armed patrols close by, keeping the border on edge.

Summary: Gedaref is stable internally for now – the war's fronts haven't reached here, and SAF remains in charge. But it is a state where international border conflict is the primary security concern. The al-Fashaga dispute means there is always a risk of clashes with Ethiopian forces or militias. If Sudan's internal conflict continues, Sudanese army capacity to hold Fashaga might wane, possibly emboldening Ethiopian hardliners – a scenario that could spark a localized interstate conflict. Within Gedaref, the presence of large refugee camps (hosting Tigrayan and other refugees) also poses management challenges; there have been reports of sporadic violence or crime in/around camps (e.g., theft, assaults), though not widespread. For project operations, Gedaref would likely require focus on border security: strict movement controls near the frontier and good liaison with Sudanese border guards. Threats include potential cross-border incursions, landmine risks in border farmlands (from past conflicts), and to a lesser extent, ethnic tensions (e.g., between refugees and locals or between tribes as seen in 2022). It's also worth noting banditry can occur on the highway linking Gedaref to Khartoum or Port Sudan if overall lawlessness increases – though nothing major reported yet, the deterioration elsewhere could eventually inspire opportunists in eastern Sudan. In conclusion, Gedaref's security is closely tied to border stability. As long as Sudan-Ethiopia relations are managed (and as of mid-2025, both countries seemed cautious not to escalate), Gedaref should remain peaceful. But any misstep or if Khartoum's hold weakens drastically, it could become a hotspot. The state exemplifies how Sudan's war could have secondary fronts (here, an international one) if conditions worsen. For now, it remains a relatively safe area to operate, with the caveat of monitoring that contentious border.

13.3.17. Northern State (Capital: Dongola)

Description: Northern State spans the vast desert regions along the Nile north of Khartoum up to the Egyptian border. It is sparsely populated (mostly Nubian communities along the Nile and nomads in the desert). The capital Dongola and other towns like Wadi Halfa are the main settlements. In the current conflict, Northern State saw one of the war's first flashpoints: the RSF's presence at the Merowe airbase. In April 2023, just as fighting began, RSF units occupied the Merowe base (which hosted Egyptian military personnel for training), leading to a confrontation with SAF. The RSF captured around Egyptian 200 soldiers there on April 15. Egypt swiftly

coordinated with Sudan's army, and within days those soldiers were handed back and SAF reasserted control of Merowe. After that incident, Northern State has been free of major battles – the RSF pulled back from Merowe area. The state has largely remained under SAF authority and is relatively calm. However, it has strategic importance: it hosts key infrastructure like the Merowe Dam and Merowe airfield, and it's the route for evacuations to Egypt. The Merowe episode showed the possibility of foreign entanglement – it briefly raised tensions with Egypt (which has been very wary of RSF). Also, Northern State has had instances of local unrest historically (for example, anti-mining protests). During the war, an interesting development has been increased smuggling and movement across the Libya border (neighboring far northwest): with Sudan's borders less monitored, arms trafficking through Northern State's desert may have risen (though specific reports are scant due to remoteness). Additionally, Northern State has dealt with being a transit for thousands of people fleeing to Egypt; Wadi Halfa border crossing was overwhelmed at times, which in mid-2023 led to some chaotic scenes (long queues, fights over scarce transport, etc.). No significant violence was reported from that, but it underscores humanitarian pressures.

Significant Security Incidents:

- **April 15–18, 2023 – Merowe Standoff:** RSF fighters occupy Merowe Airbase on April 15, detaining Egyptian troops on-site[77][78]. SAF threatens force; a tense standoff ensues. By April 18, the RSF agrees to release the Egyptians and withdraw under pressure[79][80]. While resolved relatively peacefully, it was a critical incident with potential for escalation involving a foreign power.

- **May 2023 – Anti-RSF Protests in Merowe:** After RSF's pullback, local residents in Merowe reportedly held rallies supporting the army and condemning the RSF's incursion (reported in local media, May 2023). These were peaceful, but demonstrators demanded increased protection for Northern State and Merowe dam from any future attacks.

- **Sept 2023 – Civilian Convoy Accident at Wadi Halfa:** Under wartime evacuation conditions, a tragic accident occurred when an overcrowded truck carrying fleeing families overturned near Wadi Halfa, killing 8 and injuring dozens (reported by SUNA, Sept 2, 2023). While not a security attack, it highlights the risks of chaotic mass movement in the region.

Summary: Northern State remains under firm SAF control and generally quiet. The primary security concern at the moment is strategic: ensuring key assets (dams, airfields) are secured against any RSF raids or acts of sabotage. After the initial Merowe clash, the RSF has not mounted further operations in the far north – likely due to extended supply lines and Egyptian deterrence (Egypt made clear Merowe was a red line). Hence, the direct threat of conflict has been low. Instead, Northern State's challenges are logistical and humanitarian: coping with large-scale evacuations through Wadi Halfa and monitoring the long borders with Egypt and Libya for smuggling or infiltration. Smuggling of gold and weapons has historically occurred in

these deserts; the lawlessness of war could increase that, raising risk of banditry. Additionally, Northern communities might grow restive with the war's economic impact (fuel shortages, inflation). But so far, no significant unrest has been noted beyond pro-army demonstrations. For operations, Northern State is relatively permissive – SAF would likely welcome aid especially for transit centers at Wadi Halfa. The environment is not violent, though extreme climate and distances pose their own "security" issues (heat stroke, vehicle breakdown in desert, etc.). One must also consider UXO risk around former military areas like Merowe if any conflict occurred (though likely minimal since RSF left without a fight). In summary, Northern State is one of the safest regions currently, with the caveat that a sudden strategic move by RSF (e.g., attempting to disrupt the Sudan-Egypt corridor) could change that, albeit such a move would provoke Egypt's involvement. The Merowe incident's quick resolution suggests major threats here are *contained*. Thus, project activities can proceed with standard precautions, focusing more on safety and logistics than combat-related dangers. Nonetheless, continuous coordination with SAF is essential, given the presence of Egyptian forces and heightened sensitivities around infrastructure.

13.3.18. River Nile State (Capital: Ed-Damir)

Description: River Nile State lies just north of Khartoum, named after the Nile, that flows through. It includes cities like Atbara (an important railway junction and industrial town) and the capital Ed-Damir. River Nile has been under SAF control and did not become a battleground itself, but it has significant strategic value (it hosts key military installations and connects Khartoum to the north). Throughout the war, River Nile was relatively stable until early 2025 when the conflict's reach extended via technology: the RSF began targeting infrastructure in government-held areas with drones/missiles. In April 2025, a drone strike by the RSF hit the Atbara area, specifically an IDP camp and a power facility, causing civilian casualties. This was a shocking event for River Nile State, which until then had only heard the war rumble from afar. At least 11 people were killed in that displacement camp attack near Al-Damar (Ed-Damir) and many more injured. It also knocked out electricity for the fourth time in that area since war began, indicating previous attempts to target the grid. Meanwhile, River Nile State has also faced waves of IDPs (especially from Khartoum's nearby Omdurman areas) who have resettled in places like Atbara, potentially adding social pressures. There was at least one significant civilian protest in Atbara in late 2024 related to water shortages and power cuts – perhaps partly war-related – which was resolved peacefully. Historically, Atbara is known as the "cradle of Sudan's uprisings" (strong union presence), but during this war the populace has been largely pro-army or focused on survival. Another security note: Atbara hosts a major weapons factory complex (Giad industrial zone); speculation existed that RSF might sabotage or strike it. No direct attack has happened on it, though.

Significant Security Incidents:

- **April 26, 2025 – Drone Strike on Atbara Camp:** A suspected RSF drone bombed a camp of war-displaced civilians about 3 km from the Atbara power station, River Nile state, killing

11 people (including 9 children) and injuring 23[81]. The strike also damaged the power station, knocking out electricity across River Nile and Red Sea states yet again[82]. This was the first mass-casualty incident in River Nile State from the war and marked a deadly escalation with deliberate targeting of civilians.

- **March 2024 – Attack on Atbara Power Grid:** According to Middle East Monitor, in March 2024, the RSF launched a drone that hit the main Atbara power transmission station, causing a large fire and statewide blackout (no casualties reported in that instance)[83][84]. This foreshadowed the later April attack.

- **June 2023 – Atbara Rail sabotage thwarted:** Early in the war, in June, Sudanese authorities claimed they foiled an attempt by "saboteurs" to damage the railway line near Atbara (perhaps RSF sympathizers trying to disrupt army logistics). A small explosion on tracks was discovered and neutralized (source: Sudan Tribune, June 14, 2023). This indicates potential for sabotage operations in River Nile due to its transport infrastructure.

Summary: River Nile State has become another area exposed to the war through long-range attacks. The RSF appears intent on wreaking economic havoc by striking power infrastructure and sowing terror by hitting civilian camps, as seen in April 2025[85][86]. This means even behind SAF lines, populations are vulnerable. For project planners, this translates to needing contingency plans for aerial threats (e.g., early warning, if possible, hardened shelters for staff in Atbara/Ed-Damir) – a relatively new concern in humanitarian operations. Apart from that, River Nile faces similar dynamics to other relatively stable states: lots of IDPs strain services, possibly causing tensions; indeed, the camp that was attacked existed because so many fled there from Khartoum. Managing those IDPs and supporting host communities will be key to preventing unrest. Crime is another aspect – Atbara has had increased petty crime and a few armed robbery incidents as economic conditions decline (nothing highly organized reported). Being an industrial hub, if the war drags on, factories in Atbara might shutter, leading to worker protests or vandalism. In addition, the presence of key assets (power stations, railway, arms factories) means security is tight – project movements might be surveilled by military intelligence concerned about sabotage. Coordination with authorities is thus essential to avoid misidentification (especially with drone warfare afoot – any unusual communications or movement could raise suspicion). In sum, River Nile State has shifted from a safe logistical artery to a region under intermittent attack and psychological pressure. It underscores that nowhere is completely out of reach. Nevertheless, by mid-2025 the frequency of strikes is limited (not daily), so day-to-day life continues albeit with anxiety. Maintaining operations in River Nile is feasible, but teams should exercise vigilance for air-raid alarms and ensure blast protection at bases (e.g., sandbagging, avoiding large IDP gatherings without mitigating measures). The resilient communities of Atbara, known for their activism, might also become valuable allies in identifying threats – e.g., they reportedly keep watch for drones. Engaging them could integrate community-based early warning to enhance safety for all.

Annex A - Template for SRAMP (Security Risk Assessment and Management Plan)

14. Introduction

Describe the purpose of the SRAMP, the requirement under the TDB ESMS, and why security risk management is critical in FCV environments. Note that the SRAMP consolidates both Security Risk Assessment (SRA) and Security Management Plan (SMP).

15. Project Background

15.1. Overview of the Project

Summarise the PDO, scope, and geographic coverage of the project.

15.2. Project Components

Outline the key components and activities of the project.

15.3. Implementation Arrangements

Explain how the project is structured institutionally, with PIU, Steering Committees, and support from TDB.

15.4. Project Locations

List the project states/regions where activities will be carried out, with a map if possible.

16. Security Risk Management Requirement and Responsibility

Describe obligations under the ESMS and Cofinancing partner requirements for security risk management. Explain how PIU, TDB, and contractors share responsibilities for security.

17. Objectives of the Security Risk Assessment (SRA)

State the objectives: to identify security risks, assess their severity, and define mitigation measures proportionate to risks. Emphasize protection of workers, PAPs, and assets.

18. SRA Methodology

18.1. Framework

Reference ISO 31000 and IFC PS and ESMS FCV practice.

18.2. Likelihood and Impact Scoring

Define how risks are scored, including descriptors and a risk matrix.

18.3. Risk Levels

Describe how risk scores translate into management actions (low → extreme).

19. Broader Security Context

Provide a narrative on the national security situation, conflict history, and current risks. Cite authoritative sources (UN, ACLED, local government).

20. Key Security Threats

List and describe generic threat categories (e.g., ambush, complex attack, GBV, kidnapping, civil unrest), with clear definitions.

21. Threats Specific to Project States/Regions

21.1. State/Region Profile

- **Context:** Geography, demographics, history of conflict.
- **Significant Incidents:** Three to four recent examples with sources.
- **Summary:** Key risks for project operations.

Repeat for each state/region.

22. Risk Matrix Summary

Present a summary of risk scores by state or project area (tables/matrix).

23. Security Risk Mitigation

Describe how risks will be mitigated proportionately. Link mitigation to threat types and risk levels.

24. Goals and Approach

24.1. Stakeholder Engagement

How communities and local leaders will be engaged in risk management.

24.2. Project Grievance Redress Mechanism

Integration of security issues into the GRM.

25. International Standards and Good Practices

Reference UN Voluntary Principles, IFC PS on security forces, and ISO standards.

26. Governance of the SMP

26.1. Security Infrastructure

Describe PIU structures (Security Specialist, advisors, contractors).

26.2. Security Policy Architecture

Explain internal policy documents, escalation protocols, and integration with ESMS.

26.3. Roles and Responsibilities

List responsibilities of PIU, contractors, TDB, third-party monitors.

27. Security Risk Assessment Outputs

27.1. Local Security Risk Assessments

Explain requirement for site-level SRAs and updates.

28. Risk Levels and Mitigation Measures

Provide guidance on what measures are required for each risk level (low, moderate, substantial, high, extreme).

29. Escalating and De-escalating Security Postures

Define the process for adjusting security measures as risks rise or fall.

30. In-Extremis Events

Outline response measures for extreme events (mass casualty, compound attack, hostage-taking).

31. Local Security Management Plan (LSMP)

Define requirements for contractors to prepare LSMPs, aligned with PIU SRAs.

32. Activity Security Plan (ASP)

Describe ASPs for specific high-risk activities (missions, convoys, construction).

33. Project Approval Process

33.1. Security Gateways

Explain mandatory security "gates" in the project cycle (screening, approval, monitoring).

34. Contractor Security Requirements

34.1. Procurement

Security criteria in tendering.

34.2. Security Checklist

Standard compliance checklists.

34.3. Activity Security Plan

Mandatory submission for approval.

34.4. Security Audit Process

How audits are conducted.

34.5. Monitoring and Evaluation
KPIs and review.

34.6. Security Exercises
Testing preparedness.

34.7. Training
Mandatory training for workers and guards.

35. Security Partners
List engagement with government forces, private security providers, and community structures.

36. Weekly Security Community of Practice (COP)
Describe weekly security coordination forums, participants, and reporting.

37. PIU Security Procedures
Detail operational procedures for the PIU Security Specialist (travel clearance, site visits, reporting).

38. Crisis Management Plan
Requirements for project-specific Crisis Management Plan (CMT, communication, evacuation).

39. Annexes (Templates)
- Annex A: Security Risk Assessment Methodology
- Annex B: Activity Security Plan Template
- Annex C: Local Security Management Plan Template
- Annex D: Security Checklist
- Annex E: Security Audit Process
- Annex F: Monitoring & Evaluation Process
- Annex G: Security COP TORs
- Annex H: PIU Security Procedures
- Annex I: Crisis Management Plan
- Annex J: Flash Message Reporting Template
- Annex K: Hostage & Extortion Plan
- Annex L: In-Extremis Reporting Process
- Annex M: Contractors List (example)
- Annex N: Security Stakeholder List

Annex B – Local Security Management Plan Template

40. LOCATION

- *Provide a description and mapping showing the precise geographical area covered by the SMP*
- *Within this area denote locations of project activity – work sites, frequently used locations, infrastructure – include numbers and composition of project personnel and main activities*

41. CONTEXT

Provide a summary in prose of the security environment including:

- *recent history in the security context,*
- *summary of main protagonists,*
- *local factors that drive conflict,*
- *current security situation*

42. FRIENDLY FORCES

Provide a list of all friendly security forces with points of contact, contact details, locations and perceived strength, use photographs where possible.

43. KEY LOCAL STAKEHOLDERS

Provide a list of all known local stakeholders pertinent to project activity, including relevant contact information of individuals, their area of influence, and the reason they have an impact on the project, use photographs where possible.

44. MALIGN ACTORS

Provide a list of all known Malign Actors pertinent to project activity, including relevant contact information of individuals, their area of influence, and the reason they have an impact on the project, use photographs where possible.

45. TACTICS, TECHNIQUES AND PROCEDURES

Detail current TTPs of malign actors, use case studies with photographs if available.

46. ACCESS AND ROUTE MAPPING

Using mapping denote which routes which are accessible or deemed too dangerous/impassable, and show which areas are accessible or not.

47. AREAS OF CONTROL MAPPING

Visually represent which areas are controlled by which groups and which areas are controlled by the government, by anti-government elements, or contested.

48. PRIVATE SECURITY COMPANIES

Provide a list of prequalified Private Security Companies with contact details and capabilities

49. THREAT SCENARIOS

Provide a full list, in tabular format, of all identified threat scenarios within the area of concern, for each Category of project affected personnel (Cat A, Cat B, Cat C) with their risk scores/risk levels and the required risk mitigation measures for each.

Annex C – Supplier Security Questionnaire

Name of Contractor: **Date:** **Name of Respondent:**				
No.	Criteria	Yes	No	Comment/ Explanation
	General Security			
1.	Does the Contractor conduct security risk assessments prior to all activity?			
2.	Is there a continuous review process of the security risk assessments in place?			
3.	Are all Security protocols linked to these risk assessments, i.e. does the level of risk identified directly impact on which security mitigation measures are employed?			
4.	Does the Contractor have a clear, formal and transparent internal Security hierarchy with clearly denoted security responsibilities?			
5.	Does the Contractor employ a full-time security professional to manage and mitigate risk for its personnel in South Sudan?			
6.	Do Contractor staff responsible for security have the authority to take or demand corrective action?			
7.	Is there an effective procedure to escalate or deescalate security Contractor posture?			
8.	Does the Contractor maintain SOPs for the Security of personnel, property, and infrastructure?			
9.	Are all Contractor personnel aware of their responsibilities within these SOPs?			
10.	Does the Contractor hold and maintain communication protocols, are these robust enough to ensure communication with all personnel during emergencies? i.e. can the Contractor reach all of its personnel all of the time?			
11.	Does the Contractor hold and maintain movement protocols, are these implemented effectively and are they linked to Security Risk Assessments?			
12.	Are Contractor staff who are responsible for security obliged to take action for all project missions?			
13.	Does the Contractor maintain access mapping?			

Annex D – Crisis Management Plan (CMP) Template

50. Introduction

Define what constitutes a crisis in the project context. Describe the purpose of the CMP, the formation of a crisis committee, and the guiding principle of protecting life and safety.

51. The Crisis Committee

List the core composition of the crisis committee and their functions.

51.1. PIU Project Coordinator

Acts as leader of the committee, senior spokesperson, and liaison with government. Responsible for overall direction, convening the committee, and suspending project activity if necessary.

51.2. Secretary

Keeps the crisis logbook, manages records, maintains contact lists, ensures communication lines are open, and supports committee administration.

51.3. Safeguards Officer

Advises on legal and safeguard obligations, supports planning for recovery, and ensures TDB expectations are met.

51.4. Stakeholder Engagement Officer

Manages crisis communications internally and externally. Ensures early engagement with security partners, clears external messages, and provides information to stakeholders.

51.5. Security Officer

Conducts first assessments of incidents, recommends suspension of activities if needed, ensures immediate risk reduction, and establishes internal communication systems.

52. Manage the Crisis

Outline the sequence of immediate actions once a crisis is declared.

- **Acknowledgement:** Make a rapid assessment and declare the crisis.
- **Call in members:** Convene appropriate crisis committee members.
- **Initiate logbook:** Start and maintain a crisis logbook of decisions and contacts.

- **Gather facts:** Collect information on what happened, where, who was involved, and potential impacts.
- **Evaluate:** Assess injuries, risks, liabilities, and operational impact.
- **Inform:** Communicate regularly with stakeholders.
- **Act decisively:** Implement decisions and maintain clear communication.
- **Debrief:** Conduct an immediate evaluation of actions after the crisis phase.

53. Standing Agenda

Provide the standard agenda for crisis committee meetings during an incident.

- **Roles and Responsibilities:** Confirm members and roles.
- **Facts and Assumptions:** Clarify what is known and unknown.
- **Objectives:** Define immediate objectives to resolve the crisis.
- **Scenarios:** Develop worst-case and most-likely scenarios.
- **Response Options:** Identify and select appropriate responses.
- **Action List and Priority:** Agree on tasks, prioritisation, and sequencing.
- **Stakeholders:** Identify and prioritise stakeholder engagement needs.
- **Review:** Regularly review progress and schedule next meeting.

54. Crisis Logbook

Maintain a structured logbook to record all decisions, contacts, and information flows.

- **When:** Date and time of decision or contact.
- **Type:** Internal/external communication or decision.
- **What:** Short description of action or message.
- **Who:** Name of responsible person.

55. Summary

Reaffirm that crisis response is the top priority, requiring dedicated focus, allocation of resources, and postponement of non-essential tasks.