NOVEMBER 5, 2025

RISK MANAGEMENT FRAMEWORK

Comprehensive Enterprise Risk Taxonomy and Escalation Protocols for Strategic and Programmatic Resilience

CREATED BY
EUSL AB
Care to Change the World

Table of Contents

Risk Management Framework

Preamble and Applicability

This Framework is promulgated under the GSIA Charter and shall be read consistently with Documents 00–16 and the established order of prevalence: mandatory national public law; the GSIA Charter; this Framework; and downstream instruments and annexes. The constitutional allocation of functions remains binding: the GSIA SCE sets risk governance policy and oversight; GSIA Holding AB maintains canonical taxonomies, risk registers, and assurance templates without operational entanglement; GSIA AB executes risk management under SLAs; DESA-class entities act as recipient-operators under Flowhub custody; and Hosted Ownership may be invoked within ring-fenced perimeters subject to non-attachment, negative pledge, discrete ledgers and bank accounts, and an unconditional reversion covenant to the Member upon readiness. Publication remains a control, with lawful redaction and time-limited deferrals by reasoned resolution. Controller/processor roles are explicit; DPIAs apply to risk data; IAM enforces least-privilege and multi-factor authentication; logs are immutable; encryption is mandatory in transit and at rest. Domestication gates—shadowing → dual-key → lead-role → system handover → legal localisation → readiness certification—are embedded in risk governance and verified under Document 09.

Chapter 1 — Enterprise Risk Taxonomy

1.1 Purpose and Constitutional Position. The enterprise risk taxonomy provides a structured classification of risks affecting GSIA's mandate, governance, fiduciary integrity, and programme delivery. It aligns with ISO 31000:2018 principles (ISO 31000) and incorporates governance integration guidance from COSO ERM (COSO ERM Framework), ensuring that risk management is embedded in strategic planning and operational execution.

1.2 Taxonomy Structure. Risks are classified into six primary domains, each with sub-categories and cross-references to control frameworks:

1. **Strategic Risks**
    - Misalignment with GSIA Charter or Agenda 2074 objectives
    - Policy reversals or geopolitical shifts affecting REC or Member commitments
    - Reputational harm from transparency failures or ESG breaches
2. **Governance and Fiduciary Risks**
    - Breach of ring-fencing, negative pledge, or non-attachment clauses
    - Custody failures in Flowhub or equivalent systems
    - Fraud, corruption, collusion, coercive or obstructive practices (Document 11)
3. **Operational Risks**
    - Process breakdowns in procurement, MEL, or domestication gates
    - Technology outages affecting Flowhub, IAM, or MEL repositories
    - Continuity failures (RTO/RPO breaches) per Document 10

4. **Compliance and Legal Risks**
    - Non-conformance with HCAs, DPAs, or statutory localisation mandates
    - Breach of data-protection obligations under GDPR or Schrems II jurisprudence (EDPB Guidance)
    - Sanctions violations or AML/CTF lapses
5. **Financial Risks**
    - Liquidity shortfalls or FX volatility beyond hedging tolerances
    - Counterparty default or downgrade events
    - Misstatement of financial disclosures or MEL-linked tranche logic
6. **ESG and Safeguards Risks**
    - Environmental or social harm from programme activities
    - Gender and inclusion non-compliance
    - Grievance redress mechanism failures

1.3 Risk Attributes and Metadata. Each risk entry in the Enterprise Risk Register includes:

- **Category and Sub-Category** (per taxonomy)
- **Description and Root Cause**
- **Likelihood and Impact Ratings** (qualitative and quantitative)
- **Risk Owner** (GSIA AB, DESA, or Member authority)
- **Control Mapping** (preventive, detective, corrective)
- **KRIs and Thresholds** (KRI Best Practices)
- **Escalation Protocol** (Document 17 Chapter 4)
- **Publication Unit and Redaction Plan**

1.4 Governance Integration. Risk taxonomy is embedded in GSIA's governance architecture:

- **Board and Committee Oversight** (Audit & Ethics; Risk & Treasury Committees)
- **Authority Matrices** linking risk thresholds to countersignature levels
- **Risk Appetite Statements** approved by SCE resolution (DFI Risk Appetite Note)
- **Periodic Reviews** aligned to MEL cycles and tranche logic

1.5 Publication and Transparency. The Enterprise Risk Register and summary dashboards are **published** with lawful redaction. Deferrals for security or market sensitivity are reasoned, time-limited, and recorded in the deferral register with sunset review. EFFORT-style dashboards link risk posture to programme expenditure, financing, Flowhub custody, outputs, results, and transition milestones.

1.6 Interfaces and Survivals. This taxonomy interfaces with Document 06 (ESG safeguards), Document 10 (stress testing), Document 11 (sanctions and ethics), Document 12 (digital trust), and Document 13 (financial transparency). Survivals include confidentiality, data-protection obligations, audit and access rights, and IP in templates and methods.

Chapter 2 — Programmatic Risk Controls

2.1 Purpose and Constitutional Position. Programmatic risk controls operationalise the taxonomy at portfolio and project levels, ensuring that risks inherent in GSIA-mandated programmes are mitigated through preventive, detective, and corrective measures aligned with ISO 31000 and OECD development risk guidelines (OECD Risk Management).

2.2 Control Architecture. Controls are structured across three layers:

- **Preventive Controls**: ring-fencing, negative pledge, non-attachment, escrow waterfalls, four-eyes approvals, segregation of duties, countersignature thresholds, IAM least-privilege, encryption, and DPIAs for high-risk processing.
- **Detective Controls**: immutable logging, reconciliations, KRIs, anomaly detection in treasury and MEL systems, procurement integrity audits, and external validation under Document 09.
- **Corrective Controls**: rectification plans tied to tranche logic, interim protective measures (payment holds, scope reduction, step-in), and sanctions enforcement under Document 11.

2.3 KRIs and Early Warning. Programmatic KRIs provide real-time signals of emerging risk (Protecht ERM Guide):

- **Fiduciary KRIs**: unreconciled ledger items > tolerance; delayed escrow releases; repeated authority matrix overrides.
- **Operational KRIs**: missed domestication milestones; RTO/RPO breaches; procurement cycle delays beyond SLA.
- **Compliance KRIs**: overdue DPIAs; IAM recertification gaps; sanctions screening failures.
- **Financial KRIs**: liquidity buffer breaches; hedge ineffectiveness > threshold; FX loss beyond tolerance.
- **ESG KRIs**: unresolved grievances; safeguard non-conformities flagged in MEL verification.

Threshold breaches trigger escalation protocols (Document 17 Chapter 4), including immediate notification to the Risk & Treasury Committee, activation of protective measures, and publication of breach notices with lawful redaction.

2.4 Integration with MEL and Tranche Logic. Programmatic risk controls are embedded in tranche conditions:

- **Pre-Disbursement**: verification of fiduciary controls, safeguards instruments, DPIAs, and MEL baselines.
- **Post-Disbursement**: KRIs monitored continuously; external validation cycles confirm control operation; tranche releases contingent on rectification of findings.

2.5 Data-Protection and Sovereignty. Risk controls governing data flows respect controller/processor allocations and localisation mandates. Evidence escrow and cryptographic integrity artefacts preserve verifiability where export is restricted. IAM, encryption, and immutable logging apply uniformly.

2.6 Hosted Ownership Alignment. Programmatic controls in Hosted Ownership portfolios mirror GSIA standards: discrete ledgers and bank accounts, negative pledge, non-attachment, escrow waterfalls, and reversion covenants. Immunity clauses in HCAs shall not derogate audit or step-in rights; controlled access protocols guarantee evidence availability.

2.7 Publication and Transparency. Control frameworks, KRI dashboards, and rectification dockets are **published** with lawful redaction. Deferrals for security or procurement integrity are reasoned, time-limited, and recorded with sunset review. EFFORT-style dashboards link risk posture to programme expenditure, financing, Flowhub custody, outputs, results, and domestication status.

2.8 Records, Survivals, and Assurance. Control registers, KRI logs, escalation records, rectification plans, and publication units are archived for the longer of Charter, statutory, or covenant periods. Survivals include confidentiality, data-protection obligations, audit and access rights, and IP in templates and methods. Independent validators may be commissioned under Document 09 to opine on control effectiveness and risk posture.

Chapter 3 — Key Risk Indicators (KRIs) and Escalation Protocols

3.1 Purpose and Constitutional Position. KRIs are forward-looking, quantifiable signals tied to risk drivers that enable timely, proportionate intervention before risks crystallise into incidents or losses. They constitute a mandatory component of GSIA's enterprise risk process under ISO 31000 (communication/consultation; monitoring/review) and are integrated into governance through Board-approved risk appetite statements per COSO ERM.[1] [2]

3.2 Design Criteria and Evidence Standards. KRIs shall be: (i) relevant to the taxonomy and linked to specific causes; (ii) measurable and independently verifiable; (iii) predictive, not merely descriptive; (iv) actionable with defined playbooks; and (v) reviewed at defined intervals. External good practice underscores leading indicators, explicit thresholds, and governance tie-ins to risk appetite.[5] [6] Design and validation follow ISO 31000's "recording and reporting" and "monitoring and review" requirements and, where appropriate, sectoral norms (financial-sector risk plans and compliance risk expectations) without derogating GSIA's non-profit mandate.[1] [7] [8]

3.3 KRI Classes and Threshold Logic. KRIs are grouped to mirror the enterprise taxonomy (Chapter 1), with threshold tiers calibrated to risk appetite (Chapter 4). Each KRI has: a defined normal range, an amber threshold (heightened monitoring), and a red threshold (immediate protective action). Thresholds are reasoned, approved by SCE resolution, and revisited at least annually:

1. **Fiduciary/Custody KRIs.** Examples include unreconciled items beyond tolerance; repeated breaches of four-eyes/countersignature; escrow release delays; attempts to encumber ring-fenced accounts (detected via account monitoring). Ties to Flowhub custody doctrine and negative pledge/non-attachment are mandatory.

2. **Operational/Continuity KRIs.** Examples include repeated RTO/RPO misses; configuration drift rates; failed restore tests; procurement cycle overruns against SLA.

3. **Compliance/Data-Protection KRIs.** Examples include overdue DPIAs; IAM recertification gaps; cross-border transfer exceptions without approved safeguards; sanctions screening

false-negative back-tests. OECD guidance emphasises programmatic and contextual risk visibility; KRI design must therefore track contextual stressors as well.[3] [4]

4. **Financial/Treasury KRIs.** Examples include Liquidity Coverage Ratio shortfalls; hedge ineffectiveness exceeding tolerance; counterparty limit breaches or rating downgrades.
5. **ESG/Safeguards KRIs.** Examples include unresolved GRM cases beyond SLA; repeated safeguard non-conformities in independent validation.

KRI governance reflects best practice on early-warning metrics and escalation pathways in ERM literature and supervisory guidance.[5] [6] [7]

3.4 Data, Controls, and Publication. KRI telemetry is sourced from immutable logs, reconciliations, treasury and custody systems, MEL repositories, procurement platforms, and sanctions/AML tooling. Recording and reporting follow ISO 31000; Board-level summaries align to COSO ERM reporting principles.[1] [2] Methodologies, thresholds, and board dashboards are published with lawful redaction; deferrals for security or market sensitivity are reasoned, time-limited, and logged.[3]

3.5 Escalation Protocols (Authority Matrices). Escalation is tiered and time-bound, with decision rights defined by SCE resolution:

- **Amber Breach (Heightened Monitoring).** Risk owner notifies the middle-office risk function within one business day; enhanced monitoring commences; management prepares a short-form analysis and proposed mitigants.
- **Red Breach (Protective Measures).** Immediate notification to the chair of the Risk & Treasury Committee and Secretariat; activation of protective measures (e.g., payment holds, authority-matrix tightening, step-in for defined processes), consistent with COSO's escalation to governance and with development-finance practice on proportionate mitigation.[2] [3] [7]
- **Sustained or Systemic Red.** Convene incident command with Internal Audit, Compliance/Investigations, and programme leadership; commission independent validation under Document 09; consider tranche suspension and public breach notice with lawful redaction.

Timelines, responsible officers, and evidence packs are mandatory; closures require independent verification.[1] [2] [5]

3.6 Hosted Ownership and Hybrid REC Specifics. KRI sets apply at ring-fenced Hosted Ownership perimeters and at hybrid-REC master and country sub-accounts. Breaches at either layer trigger protections locally and, where contagion is plausible, at the portfolio master layer, consistent with OECD guidance on contextual and systemic risk.[3] [4]

3.7 Records, Survivals, and Learning. KRI definitions, thresholds, breach logs, decisions, and verification artefacts are archived per Charter/statutory maxima. Survivals include confidentiality, data-protection obligations, audit and access rights. Lessons learned are issued by GSIA Holding AB as periodic circulars to refine indicators and thresholds.[1] [2]

References (Chapter 3).

[1] ISO 31000:2018 – Risk management — Guidelines (principles; monitoring/review; recording/reporting): ISO 31000.

[2] COSO ERM – Integrating with Strategy and Performance (governance integration; reporting): COSO

ERM Framework.
[3] OECD Development Co-operation – Risk Management (contextual/programmatic risk and transparency): OECD Risk Management.
[4] OECD Framework on Emerging Critical Risks (handling transboundary/systemic risks): OECD Critical Risks.
[5] Secureframe – KRI practices and thresholds: KRI Best Practices.
[6] Protecht – KRI design and early-warning focus: Protecht KRI.
[7] U.S. Treasury Financial-Services Sector Risk Management Plan (illustrative sectoral escalation discipline): Treasury FSS RMP.
[8] Federal Reserve SR 08-8 (rev. 2025) – firmwide compliance risk programs (oversight and escalation): FRB SR 08-8.

Chapter 4 — Risk Appetite and Tolerance

4.1 Purpose and Constitutional Position. Risk appetite and tolerance translate the Charter's public-interest mandate into reasoned, quantitative and qualitative boundaries for risk-taking across GSIA entities, programmes, and Hosted Ownership perimeters. Appetite is set by the GSIA SCE through formal resolution, informed by ISO 31000 principles and COSO ERM guidance on integrating appetite with strategy and performance.[1] [2] Appetite statements bind operational practice, tranche logic, KRI thresholds, and escalation matrices.[4]

4.2 Definitions and Levels.

- **Risk Appetite** expresses the amount and type of risk GSIA is willing to accept in pursuit of objectives (narrative and quantified).
- **Risk Tolerance** defines measurable bounds around key metrics (e.g., LCR floors, hedge ineffectiveness limits, maximum unresolved Class-A findings) that trigger escalation when exceeded. COSO materials emphasise making appetite actionable and embedded in governance and reporting; ISO 31000 stresses alignment with context and objectives.[1] [2] [4]

4.3 Appetite Structure by Taxonomy. Appetite is articulated for each risk domain defined in Chapter 1, with examples below (to be tailored by resolution):

1. **Strategic.** Appetite is low for mandate dilution or material deviations from Charter-aligned objectives; very low for transparency derogations beyond lawful, time-limited deferrals. Tolerances: maximum count and duration of publication deferrals per quarter.[1] [3]
2. **Governance & Fiduciary.** Appetite is very low for breaches of ring-fencing, negative pledge, non-attachment, or four-eyes/segregation controls. Tolerances: zero tolerance for private distribution from ring-fenced funds; numeric limits for late reconciliations and authority-matrix overrides.
3. **Operational/Continuity.** Appetite is moderate-to-low, recognising implementation realities. Tolerances: RTO/RPO breach counts per quarter; maximum acceptable configuration drift rate before change freeze.
4. **Compliance & Legal.** Appetite is very low for data-protection violations, unlawful cross-border transfers, or sanctions breaches. Tolerances: zero tolerance for willful violations; thresholds for overdue DPIAs and IAM recertifications with accelerated closure timelines.[3] [8]

5. **Financial.** Appetite is low-to-moderate for liquidity and FX risk consistent with hedging for risk reduction only. Tolerances: minimum liquidity buffer days; maximum hedge ineffectiveness; counterparty concentration limits; downgrade triggers for enhanced monitoring.[7]

6. **ESG/Safeguards.** Appetite is very low for harmful or rights-abusive outcomes; tolerances include caps on unresolved severe GRM cases and mandatory remediation deadlines consistent with OECD and human-rights benchmarking for DFIs.[3]

4.4 Calibration and Evidence. Appetite and tolerance are calibrated using: (i) historical incident and KRI data; (ii) external benchmarks; (iii) stress-testing scenarios per Document 10; and (iv) DFI risk-appetite constraints relevant to co-financing. OECD guidance on critical/emerging risks informs calibration for systemic exposures.[3] [4] [7] Calibration documents are recorded and published with lawful redaction.

4.5 Cascading and Embedding. Appetite is cascaded through: (i) authority matrices (payment/hedge limits; countersignature thresholds); (ii) KRI thresholds (amber/red mapping to appetite/tolerance); (iii) tranche conditions (pre-disbursement and subsequent verification gates); and (iv) **contracts** (intercreditor deeds, DPAs, procurement covenants). COSO ERM emphasises aligning performance and reporting with appetite; ISO 31000 requires integration into governance and processes.[1] [2] [4]

4.6 Review, Breach Handling, and Adjustments. Appetite statements are reviewed at least annually, or upon material context change, incident, or systemic shock. Breaches follow Chapter 3 escalation paths. Where repeated breaches imply structural mis-calibration, the SCE may adjust tolerances by reasoned resolution, with a published justification and sunset review; otherwise, corrective action plans and capacity investments are prioritised.

4.7 Hosted Ownership and Hybrid REC Application. Appetite is set at the portfolio master level and tailored to Hosted Ownership perimeters and hybrid-REC/country sub-accounts. Where sovereign constraints require adaptations (e.g., localisation of logs or escrow design), tolerances are localised without diluting ring-fencing, non-attachment, audit/validation rights, or publication doctrine, consistent with OECD development-co-operation risk principles.[3]

4.8 Publication and Registers. The Risk Appetite Statement and Tolerance Register are published with lawful redaction, including metric definitions, thresholds, escalation tie-ins, and review dates. Deferrals are reasoned, time-limited, and sunset-reviewed.

4.9 Records, Survivals, and Assurance. Appetite resolutions, calibration analyses, breach logs, adjustments, and verification artefacts are archived per Charter/statutory maxima. Survivals include confidentiality, data-protection duties, audit and access rights, and IP in templates/methods. Independent validators may be commissioned under Document 09 to assess alignment between appetite, KRIs, and operational controls.

References (Chapter 4).

[1] ISO 31000:2018 – governance integration, monitoring/review: ISO 31000.
[2] COSO ERM – risk appetite, strategy/performance integration: COSO ERM Framework.
[3] OECD Development Co-operation risk guidance & emerging risks framework: OECD Risk Management; OECD Critical Risks.
[4] COSO ERM – guidance on risk appetite/reporting (ERM knowledge hub): COSO ERM Guidance.
[7] U.S. Treasury FSS Risk Management Plan – illustration of tolerance-based escalation and sector stress alignment: Treasury FSS RMP.

[8] Federal Reserve SR 08-8 (rev. 2025) – firmwide compliance risk oversight and escalation: FRB SR 08-8.

Links and references

Core Standards and Frameworks

- **ISO 31000:2018 – Risk Management Guidelines**
  Provides principles, framework, and process for enterprise risk management, applicable to all sectors.
  ISO Official Page
  ISO 31000 Family Overview [iso.org] [iso.org]

- **COSO ERM – Integrating with Strategy and Performance**
  Widely recognized framework for embedding risk management into governance and strategic planning.
  COSO ERM Framework
  PwC Guide to COSO ERM [coso.org] [pwc.com]

Development Finance and Programmatic Risk

- **OECD Risk Management for Development Co-operation**
  Guidelines for managing contextual and programmatic risks in development programs.
  OECD Risk Management Overview
  Framework on Emerging Critical Risks [oecd.org] [oecd.org]

- **DFI Risk Appetite and Safeguards**
  Explains risk appetite constraints and safeguard policies for DFIs like AfDB, Swedfund, Finnfund.
  DFI Risk Appetite Technical Note
  OHCHR Benchmarking Study on DFI Safeguards [donorplatform.org] [ohchr.org]

Key Risk Indicators (KRIs) and Escalation

- **Best Practices for KRIs**
  KRIs as early-warning metrics for enterprise and programmatic risk.
  Secureframe Guide
  Protecht ERM Blog
  BDO Risk Blueprint