Certified Emissions Reduction Technologies Foundation

RISK MANAGEMENT FRAMEWORK

ISO 31000-Based Framework Centred on Environmental Integrity Risk

Document ID: CERT-GOV-006
Version 1.0 (Draft for Consultation)
Date: 2 July 2026
Classification: Public

Document Control

Field	Detail
Document ID	CERT-GOV-006
Title	CERT Risk Management Framework
Version	1.0 (Draft for Consultation)
Status	Draft – pending Board adoption and public consultation
Owner	Audit, Risk and Finance Committee
Approver	Board of Trustees
Review cycle	At least every three years, or upon material change
Related documents	CERT-FDN-001; CERT-GOV-001 (§8); CERT-GOV-005; CERT-GOV-007; CERT-REG-001; CERT-REG-005 (planned)

Version History

Version	Date	Author	Description
1.0	2026-07-02	CERT Founding Secretariat	Initial draft for founding Board review and public consultation.

Table of Contents

1. Purpose, Scope and Approach

1.1 This Framework establishes how CERT identifies, assesses, treats, monitors, and reports risk across the Foundation, implementing Charter reference CERT-GOV-006 and the CFTC guidance expectation that crediting programmes maintain risk management policies.

1.2 Approach. The Framework follows ISO 31000 (principles, framework, process) adapted to CERT's defining feature: the risks that matter most are not primarily financial risks to CERT, but integrity risks to the atmosphere and to market confidence. Over-crediting is CERT's equivalent of a bank's credit default.

1.3 Scope. All activities: standard-setting, registration, issuance, registry technology, accreditation, finance, people, and external environment. Project-level non-permanence risk is treated both here (portfolio view) and operationally in the Buffer Pool Framework (CERT-REG-005, planned).

2. Risk Governance – Three Lines of Defence

Line	Who	Responsibility
First line	Secretariat operational teams	Own and manage risk in daily processes; execute controls; report incidents
Second line	Risk & Compliance function (reports to CEO with dotted line to ARF Committee); anti-bribery function; CISO	Maintain risk registers, methodologies and appetite monitoring; challenge the first line
Third line	Internal audit (outsourced initially), external auditors, independent programme reviews	Independent assurance to the Audit, Risk and Finance Committee and Board

2.1 The Audit, Risk and Finance Committee oversees this Framework (GOV-001 §8); the Board approves risk appetite annually. The Ethics and Integrity Committee owns ethics and conflict risk; escalation paths between the two are documented.

3. Risk Appetite

3.1 CERT has near-zero appetite for: over-crediting and environmental integrity failures; double counting; corruption; and loss or manipulation of registry records.

3.2 CERT has low appetite for: safeguards failures; data privacy breaches; and regulatory non-compliance.

3.3 CERT accepts moderate, managed risk in: innovation (new methodologies, digital MRV, AI-assisted review — always with human accountability); market volume volatility; and jurisdictional expansion. Growth is never pursued at the cost of integrity (Code of Ethics §2.2).

4. Risk Taxonomy

4.1 Integrity Risks (Primary)

Risk	Illustrative drivers	Key mitigations
Over-crediting	Inflated baselines, non-additionality, gamed defaults, uncertainty ignored	Conservative defaults; uncertainty deductions; Standards Committee independence; AI screening; post-issuance audits
Reversal / non-permanence	Fire, disease, harvest, project abandonment (nature-based); storage leakage (engineered)	Buffer Pool (nature-based projects only); proponent replacement obligations for engineered storage; monitoring triggers; remote sensing
Double counting	Cross-registry duplication, Article 6 mis-accounting, double claiming	Unique serials; registry interoperability checks; Article 6 authorisation tagging; retirement transparency
Fraud and misrepresentation	Falsified monitoring data, shell proponents, collusion with VVBs	Identity verification (KYC); duplicate/anomaly detection; VVB rotation; whistleblower channel; sanctions
Verification failure	VVB capacity, capture, or negligence	Accreditation Manual; performance monitoring; spot re-verification; de-accreditation
Safeguards failure	Land-rights violations, absent FPIC, community harm	Mandatory safeguards; grievance mechanism; validation checks; suspension powers

4.2 Institutional Risks

Risk	Illustrative drivers	Key mitigations
Cyber / registry security	Intrusion, credential theft, insider manipulation, ransomware	CERT-GOV-007 ISMS; immutable audit trail; RBAC/MFA; independent penetration testing
Legal / regulatory	Market regulation shifts, consumer-protection claims law, Article 6 rule changes	Regulatory watch; jurisdiction-neutral drafting; ICVCM/CORSIA alignment programme
Financial sustainability	Fee dependence on issuance volumes; concentration	Reserves policy (12+ months operating costs); diversified fee base; no volume-linked pay
Reputational	Media findings against registered projects; association effects	Rapid-response investigation protocol; transparency-first communications; corrective issuance action
Operational / people	Key-person dependence, process error, capacity gaps	Documented SOPs; four-eyes controls; succession planning

Conflict of interest / governance	Capture of committees, related-party abuse	GOV-002 regime; independence screening; public registers

5. Risk Management Process

5.1 Identification. Continuous, via risk workshops (at least annually per function), incident reports, whistleblower intelligence, audit findings, market monitoring, and horizon scanning.

5.2 Assessment. Each risk is scored for likelihood (1–5) and impact (1–5) on inherent and residual bases. Impact scales are defined for four dimensions: environmental integrity (tCO2e mis-credited), market confidence, financial, and legal. The highest dimension governs.

5.3 Treatment. Avoid, reduce (controls), transfer (insurance, contractual), or accept within appetite. Every red (residual score ≥ 16) risk requires a named owner, treatment plan, and quarterly ARF Committee review; red integrity risks are reported to the full Board.

5.4 Monitoring. Key risk indicators (e.g., issuance concentration by methodology/VVB/region, buffer pool coverage ratio, appeal and complaint rates, verification finding rates, security incidents) are tracked on a dashboard reviewed monthly by management and quarterly by the ARF Committee.

5.5 Incident management. Incidents (including near misses) are logged within 48 hours, root-caused, and fed back into methodologies, Rulebook, or controls. Material incidents are disclosed in the Annual Governance and Transparency Report.

6. Buffer Pool Interface

6.1 The buffer pool is CERT's capitalised mitigation of reversal risk for nature-based projects only; non-nature-based projects make no buffer contribution, and engineered-storage reversal risk is instead managed through proponent replacement obligations under Rulebook Clause 10.2A. This Framework requires: (a) an annual actuarial-style adequacy review of buffer coverage against modelled nature-based reversal scenarios (including correlated events such as regional fires); (b) ARF Committee sign-off; (c) publication of the adequacy conclusion; and (d) monitoring of counterparty performance risk on engineered-storage replacement obligations. Contribution rates are set in CERT-REG-005 (planned).

7. Business Continuity and Resilience

7.1 The Secretariat maintains business continuity and disaster recovery plans for registry operations with recovery time objective ≤ 24 hours and recovery point objective ≤ 15 minutes for registry ledger data, tested at least annually (detail in CERT-GOV-007).

8. Reporting and Review

8.1 Quarterly risk report to the ARF Committee; annual risk report to the Board; public summary in the Annual Governance and Transparency Report.

8.2 This Framework is reviewed at least every three years and after any material incident. References: ISO 31000:2018; ISO 37001:2025 (bribery risk); ISO/IEC 27005 (information security risk); ICVCM Assessment Framework; CFTC VCC Guidance (2024).