NOVEMBER 7, 2025

RISK MANAGEMENT FRAMEWORK

ENTERPRISE TAXONOMY, PROGRAMMATIC CONTROLS, AND ESCALATION DOCTRINE ALIGNED TO INTERNATIONAL ASSURANCE STANDARDS

CREATED BY
EUSL AB
Care to Change the World

Table of Contents

Risk Management Framework

This Framework codifies the governance, taxonomy, and control environment for identifying, assessing, mitigating, and assuring risks across Creativa Center and ecosystem entities, from SDEP entry operations through DESA institutionalization and PCPP scale-out. It embeds separation-of-functions between first-line management, second-line risk/compliance/ESG, and third-line internal audit; aligns with international benchmarks for internal control, assurance, and sustainability risk; and integrates digital-trust and cyber-resilience as non-derogable obligations. The Framework is harmonized with COSO Internal Control – Integrated Framework, ISO 31000 Risk Management, the IIA IPPF, and sustainability/ESG safeguards consistent with the World Bank Environmental and Social Framework (ESF) and IFC Performance Standards (2012). Climate-related risk treatment and claims are positioned for external assurance under ISAE 3410, with general non-financial assurance aligned to ISAE 3000 (Revised). Data protection and cyber risk controls follow GDPR, ISO/IEC 27001, NIST Cybersecurity Framework 2.0, and NIST SP 800-207 (Zero Trust), enforceable via Microsoft enterprise capabilities Entra ID, Intune, Purview, Defender, and Sentinel. The Framework shall be read together with Document 06 (ESG Safeguards), Document 08 (Unified MEL), Document 09 (External Validation & Peer Review), Document 11 (Compliance, Audit & Ethics Code), Document 12 (Data Protection & Digital Trust Policy), and Document 13 (Funding & Remuneration Framework).

Chapter 1 – Enterprise Risk Taxonomy

The enterprise risk taxonomy provides a common vocabulary and hierarchical structure to classify risks across strategy, operations, finance, ESG, legal/compliance, and digital-trust domains. It is designed to enable consistent risk identification, aggregation, reporting, and assurance across Creativa's multi-entity architecture, and to maintain equivalence with recognized standards.

Strategic and Mandate Risk. Risks to mandate delivery, policy coherence, and portfolio alignment with national plans and global compacts (UN 2030 Agenda; AU Agenda 2063; Paris Agreement). This class includes country ownership risk, additionality risk in blended operations, and partner concentration risk, and is assessed within the COSO principles for control environment and risk assessment.

Programmatic and Implementation Risk. Risks affecting time, cost, scope, and benefits realization in SDEP/DESA/PCPP operations, including supply-chain fragility, vendor failure, construction delay, value-for-money erosion, and MEL indicator integrity. Treatment aligns with ISO 31000 processes (identify–analyze–evaluate–treat–monitor) and sustainable procurement per ISO 20400.

ESG and Safeguards Risk. Environmental and social risks—including labor/OHS, community health and safety, biodiversity, involuntary resettlement, stakeholder conflict—classified using World Bank ESF and IFC PS typologies (e.g., PS1 assessment and management systems; PS2 labor/OHS; PS4 community safety; PS6 biodiversity). This category integrates human-rights due diligence per the UN Guiding Principles on Business and Human Rights and responsible business conduct under the OECD Guidelines for Multinational Enterprises (2023).

Fiduciary and Financial Risk. Risks related to fraud, corruption, misstatement, liquidity, FX exposure, sanctions, and going-concern for implementing entities. Controls follow ISO 37001 (anti-bribery), ISO 37301 (compliance), internal control under COSO, internal audit per IIA IPPF, and external assurance under ISAE 3000. The governance allocation flows to GSEA (Document 13, Ch. 2) are included in this class for transparency and auditability.

Legal, Regulatory, and Contractual Risk. Risks arising from non-compliance with law, permits, HCA obligations (Document 16), data-protection statutes (GDPR), export controls, sanctions regimes, and contractual covenants, including remedies and step-in exposures.

Digital-Trust, Cybersecurity, and Data Risk. Identity compromise, unauthorized access, data loss, operational technology vulnerabilities, ransomware, and cloud misconfiguration. Controls are mapped to NIST CSF 2.0 functions (Identify–Protect–Detect–Respond–Recover), ISO/IEC 27001 Annex A controls, and Zero Trust per NIST SP 800-207, implemented via Entra ID (identity governance/conditional access), Intune (endpoint compliance), **Purview** (DLP/records/eDiscovery), **Defender** (threat protection), and **Sentinel** (SIEM/SOAR).

Reputational and Stakeholder Risk. Risks of diminished trust from beneficiaries, governments, DFIs, and the public due to performance failure, opacity, or ethics breaches. Monitoring integrates stakeholder grievance data (IFC PS1/PS2/PS4), media analysis, and Document 18 (Communications & Advocacy) protocols.

Climate and Nature-Related Risk. Physical, transition, and liability risks tied to climate change and biodiversity loss. Where climate claims or GHG outcomes are reported, assurance is aligned to ISAE 3410; biodiversity and resource-efficiency obligations reflect IFC PS6 and Paris alignment.

Security and Continuity Risk. Personnel and site security, civil unrest, disaster events, and business continuity. Treatment follows ISO 22301 Business Continuity and duty-of-care principles, aligned with OHS controls under ISO 45001.

The taxonomy is hierarchical: Classes → Categories → Risk Statements → Controls → Metrics (KRIs). It supports aggregation and heat-mapping at entity and portfolio levels, with reporting to governance bodies and external partners under Document 09.

Chapter 2 – Programmatic Risk Controls

Programmatic risk controls are the codified treatments that reduce the likelihood and impact of risks identified in the taxonomy when executing SDEP modules, standing up DESA institutions, and scaling PCPP pipelines. Controls are designed to be preventive, detective, and corrective, and to be independently testable under internal audit and external assurance.

Governance and Segregation of Duties. First-line program teams own risk; second-line ESG/compliance/digital-trust functions set policy, challenge, and monitor; third-line internal audit (IIA-conformant) provides independent assurance. This tri-line model aligns with **COSO** principles and is mandatory for all implementing units, with component-specific elaborations permitted but not weaker than the baseline in Document 11.

Safeguards Integration and Screening. At concept note and pipeline gate (Document 14), each operation is screened using World Bank ESF and IFC PS criteria and assigned a safeguards category driving the depth of ESIAs/ESMPs, labor/OHS plans, and community engagement. Human-rights due diligence follows UNGPs and OECD Guidelines expectations. No-go triggers include unresolved critical risks to life/safety, prohibited practices, or unmitigable rights impacts.

Sustainable Procurement and Vendor Controls. Procurement adopts ISO 20400 principles with life-cycle costing, sanctions screening, beneficial ownership checks, and conflict-of-interest declarations. Contracting embeds ESG covenants and audit/inspection rights, with open-data publication in OCDS format and, where applicable, IATI disclosures (Document 13, Ch. 5).

Financial Integrity and Anti-Corruption. Controls include segregation of approvals, documented rate cards, prohibition of success fees tied to public awards, periodic reconciliations, and anomaly detection. Systems comply with ISO 37001 (anti-bribery) and ISO 37301 (compliance). External assurance under ISAE 3000 is scheduled for material non-financial statements; climate claims, if any, follow ISAE 3410.

MEL-Embedded Controls. Indicators, baselines, targets, and verification sources are defined at design and monitored under the Unified MEL (Document 08). Results are tied to tranche releases (Document 20), with independent validation per Document 09. Data quality controls (DQAs) ensure accuracy, completeness, and timeliness, and are themselves subject to audit.

Digital-Trust and Cyber Controls. Identity and access are enforced by Entra ID conditional access and privileged identity management; endpoints are governed by Intune; data protection, retention, DLP, and eDiscovery are enforced via Purview; advanced threat protection is provided by Defender; telemetry and incident orchestration run through Sentinel. Control mapping aligns to NIST CSF 2.0, ISO/IEC 27001, and Zero Trust (NIST SP 800-207). Personal data processing adheres to GDPR principles of lawfulness, purpose limitation, and minimization (Document 12).

Business Continuity and Field Safety. Each program maintains a Business Continuity Plan consistent with ISO 22301, with scenario playbooks (e.g., cyber outage, civil unrest, epidemic), minimum service levels, and recovery time objectives. OHS measures follow ISO 45001; environmental management adheres to ISO 14001 where relevant.

Contractual Remedies and Step-In Rights. Co-financing and vendor contracts include cure periods, corrective action plans tied to MEL metrics, and step-in provisions to protect essential services. Material ESG breaches, corruption findings, or systemic data-protection failures trigger escalation per Document 11 and corrective actions under Document 06, with disclosures in the Transparency Register (Document 13, Ch. 5).

Transparency and Grievance Mechanisms. Publication of awards, disbursements, and performance summaries is mandatory (Document 13), with accessible grievance channels meeting IFC PS standards (notably PS1/PS2/PS4). Whistleblowing protections follow ISO 37002; retaliation is prohibited and sanctionable.

Assurance and Testing Cadence. Control effectiveness is tested via periodic internal audits (IIA IPPF), external peer review (Document 09), and, where material, independent assurance engagements (ISAE 3000/3410). Findings translate into risk register updates, KRI thresholds, and, if necessary, risk appetite adjustments (Chapter 4 to follow).

Chapter 3 – KRIs and Escalation Protocols

Key risk indicators constitute the early-warning instrumentation of this Framework. They are defined at enterprise, portfolio, and program levels, aligned to the taxonomy in Chapter 1 and embedded into tranche logic and milestone reviews under Document 20. Indicator design follows ISO 31000 principles of relevance, reliability, and responsiveness, with thresholds calibrated to the risk appetite and tolerance defined in Chapter 4 and governance oversight aligned with COSO and IIA IPPF.

KRI classes and exemplar thresholds are established as follows in narrative form. Strategic and mandate KRIs monitor divergence from national plans and global compacts, including the UN 2030 Agenda, AU Agenda 2063, and NDC trajectories under the Paris Agreement. Triggers include material deviation of

outcome indicators or portfolio concentration beyond approved bounds, prompting rebalancing or pipeline re-sequencing under Document 14.

Programmatic KRIs measure schedule variance, cost growth against life-cycle baselines, contractor performance, and value-for-money erosion, anchored in sustainable procurement practice per ISO 20400. Breach of cost or schedule thresholds necessitates corrective action plans, enhanced supervision, or step-in execution rights pursuant to contract clauses and Document 20.

Safeguards and ESG KRIs, grounded in World Bank ESF and IFC PS, track incidents related to labor and OHS, community health and safety, biodiversity, resettlement, and grievance volumes and resolution times. Breaches escalate to second-line ESG, require documented mitigations under Document 06, and, where material, trigger external peer review per Document 09.

Fiduciary and financial KRIs address fraud/corruption signals, unexplained variances, overdue reconciliations, FX exposures, and liquidity buffers. Control design references ISO 37001 and ISO 37301, with independent testing under ISAE 3000 where material. Confirmed breaches invite suspension of disbursements, targeted audits, and, if required, claw-backs.

Legal, regulatory, and contractual KRIs capture permit delays, non-compliance notices, and HCA deviation risks (Document 16), with immediate legal triage and remediation plans. Digital-trust and cyber KRIs, mapped to NIST CSF 2.0 and ISO/IEC 27001, monitor identity compromise attempts, endpoint posture, DLP violations, and mean-time-to-detect/respond, enforced via Entra ID, Intune, Purview, Defender, and Sentinel.

Reputational and stakeholder KRIs include surge thresholds in grievances and adverse media correlated against MEL performance (Document 08). Climate and nature-related KRIs track deviations in emissions-reduction or resilience outputs; where climate claims are public, escalation triggers assurance under ISAE 3410. Security and continuity KRIs, aligned with ISO 22301 and ISO 45001, track incident rates, near-misses, and readiness test results.

Escalation follows a four-tier protocol. Tier 1 constitutes first-line containment and corrective action within management authority, with documentation in the risk register and notification to second-line functions. Tier 2 activates second-line challenge, enhanced monitoring, and, where relevant, targeted audits; material issues are flagged for governance review. Tier 3 engages the governance body for decisions on tranche re-sequencing, scope adjustment, or partial suspension, with required disclosures in the Financial Transparency Register (Document 13, Chapter 5). Tier 4 is exceptional and involves program pause or termination, step-in rights activation, and, if indicated, referral to authorities, always preserving due process and contractual obligations. Throughout escalation, the external validation cadence under Document 09 is used to corroborate findings and recommendations.

Chapter 4 – Risk Appetite and Tolerance

Risk appetite articulates the aggregate level of risk Creativa and its ecosystem entities are willing to accept in pursuit of mandate objectives; tolerance specifies quantitative and qualitative bounds within which risks may vary without triggering re-authorization. The regime is designed and reviewed in accordance with COSO Internal Control and ISO 31000, and it is operationalized through the MEL-linked tranche logic in Document 20 and assurance mechanisms in ISAE 3000 and ISAE 3410 where climate outcomes are implicated.

The enterprise appetite is conservative-to-moderate for fiduciary integrity, legal and compliance, and digital-trust risks, reflecting non-derogable duties under GDPR, ISO/IEC 27001, NIST CSF 2.0 and NIST SP 800-207, and zero tolerance for corruption as codified in ISO 37001 and enforced through Document 11. Appetite is moderate for programmatic and schedule risks typical of complex implementation environments, provided mitigations are credible and value-for-money remains demonstrable under ISO 20400 and the OECD DAC criteria. Appetite is targeted and conditional for ESG risks: operations may proceed where the safeguards architecture meets or exceeds World Bank ESF/IFC PS equivalence and residual risks are bounded by verifiable mitigation.

Tolerance bands are set through KRIs. Fiduciary deviations beyond immaterial thresholds precipitate immediate containment and, if persistent, tranche holds; any substantiated corruption triggers automatic Tier 3 or Tier 4 escalation. Cyber tolerance is narrow: identity compromise rates, mean-time-to-detect/respond, and DLP incident counts have strict upper limits aligned with the referenced NIST and ISO controls and enforced via Microsoft Entra ID, Intune, Purview, Defender, and Sentinel. Schedule and cost variance tolerances are calibrated by project criticality and contingency planning; persistent breaches necessitate scope optimization or re-baselining under governance oversight.

Climate and nature-related tolerances are structured to ensure consistency with national NDCs under the Paris Agreement and biodiversity safeguards under IFC PS6. Where operations claim mitigation or adaptation outcomes, tolerance for under-delivery is narrow and compels remedial investment or reallocation; public claims may require external assurance (ISAE 3410).

Risk appetite is reviewed annually, or ad hoc upon systemic shocks, by the governing body on recommendation from the Chief Risk Officer. Adjustments require documented rationale, back-testing against historical KRI data, and disclosure in the Transparency Register (Document 13, Chapter 5). Component entities (e.g., SUDESA, DESA units, GSCA/PCGG institutions, GSIA, GSEA, GSDA, CGSA/SLUC/Agenda 2074, WOSL Group) may adopt stricter appetites and narrower tolerances commensurate with their sectoral exposures; however, they may not adopt looser parameters than those stipulated herein.

Finally, linkage to incentives and sanctions is explicit. Management compensation and variable fees shall not reward risk externalization or appetite breaches; per Document 13, success-fee constructs tied to public awards are prohibited. Material breaches of appetite or tolerance invite corrective actions under Document 06, intensified audit under the IIA IPPF, and, where warranted, disclosure and remedy activation consistent with co-financing covenants (Document 14).