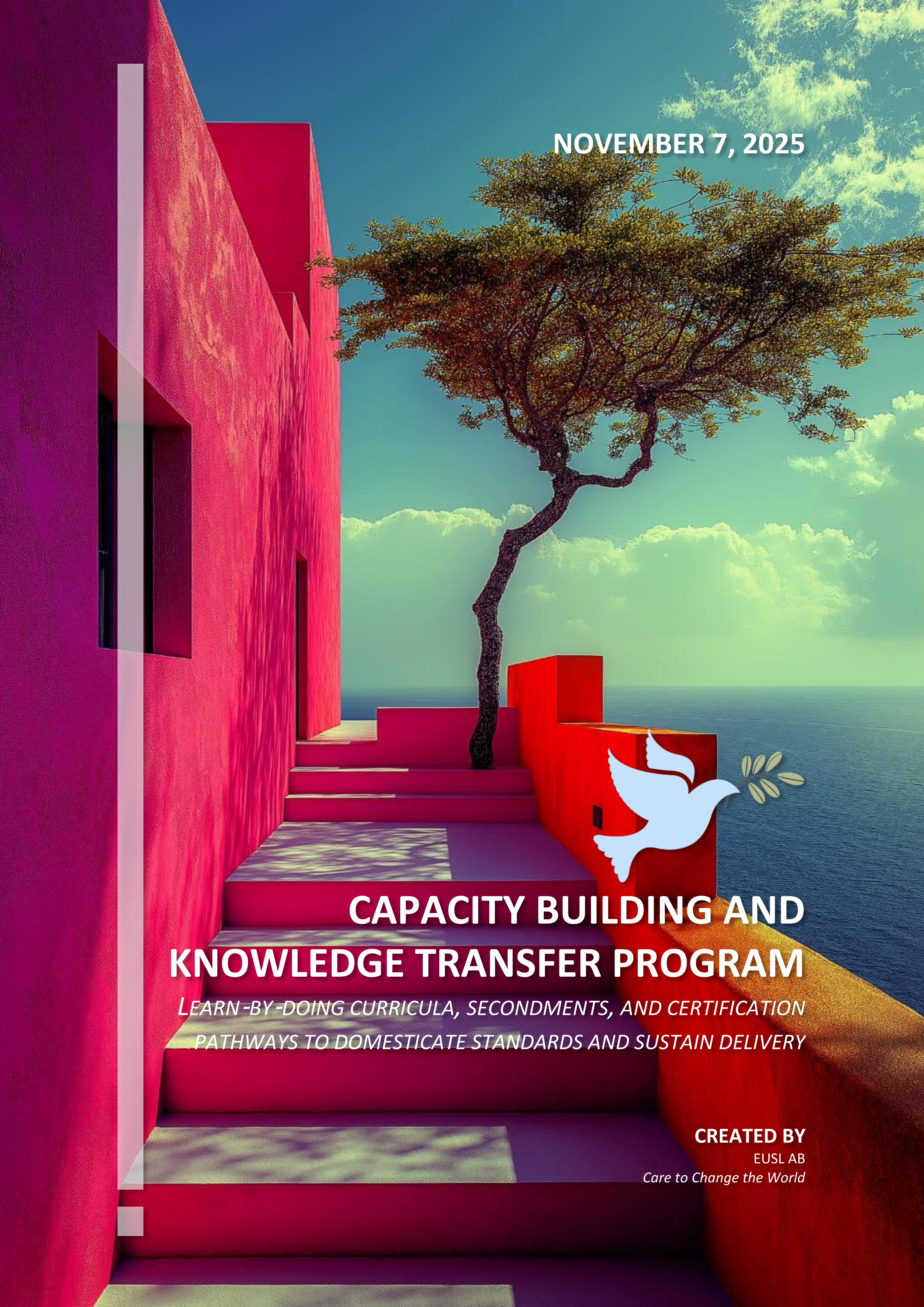

NOVEMBER 7, 2025

CAPACITY BUILDING AND KNOWLEDGE TRANSFER PROGRAM

Learn -by -doing curricula, secondments, and certification pathways to domesticate standards and sustain delivery

CREATED BY

EUSL AB

Care to Change the World

Table of Contents

Capacity Building and Knowledge Transfer Program

Preamble

This Program establishes the legally coherent architecture for capacity development, institutional strengthening, and systematic knowledge transfer across Creativa Center ecosystem entities and counterpart institutions. It operationalizes a staged “build-operate-transfer” modality from SDEP entry to DESA institutionalization and PCPP scale-out, while preserving the separation-of-functions doctrine and ensuring assurance-ready results. The Council for Global Social Advocacy (CGSA) is positioned alongside Agenda 2074 as a co-equal convening and standards-diffusion organ that curates advocacy-ready knowledge and practitioner toolkits; it does not sit under Agenda 2074. All provisions herein align with the UN 2030 Agenda (SDGs), AU Agenda 2063, and climate-alignment under the Paris Agreement, and maintain safeguards equivalence to the World Bank ESF and IFC Performance Standards (2012). Responsible business conduct and human-rights due diligence are embedded pursuant to the OECD Guidelines for Multinational Enterprises (2023) and the UN Guiding Principles on Business and Human Rights. Digital-trust and privacy are non-derogable obligations under GDPR and ISO/IEC 27001, mapped to NIST CSF 2.0 and NIST SP 800-207 (Zero Trust) and enforced with Microsoft enterprise controls (Entra ID, Intune, Purview, Defender, Sentinel). Assurance and evaluation interface with ISAE 3000 (Revised) and, where climate outcomes are claimed, ISAE 3410. This Program shall be read together with Document 06 (ESG Safeguards & Fiduciary Control), Document 08 (Unified MEL), Document 09 (External Validation & Peer Review), Document 11 (Compliance, Audit & Ethics), Document 12 (Data Protection & Digital Trust), and Document 20 (Implementation Roadmap).

Chapter 1 – Learn-by-Doing Curriculum

The Learn-by-Doing Curriculum is the principal modality for institutionalizing capabilities through real-time co-delivery of SDEP modules, progressive establishment of DESA, and preparation for PCPP participation. It is outcomes-based, tranche-linked, and assurance-ready, with competencies and milestones verifiable under the Unified MEL (Document 08) and subject to external validation under Document 09.

The Curriculum is organized into competency tracks corresponding to legally material functions. An ESG & Safeguards Track develops capacity to plan and execute environmental and social management systems at equivalence with the World Bank ESF and IFC Performance Standards, including labor/OHS integration aligned to ISO 45001, community health and safety, stakeholder engagement, and grievance mechanisms consonant with PS1/PS2/PS4. A Fiduciary Integrity & Procurement Track embeds internal control principles per COSO, internal auditing under the IIA IPPF, anti-bribery systems under ISO 37001, compliance under ISO 37301, protected reporting per ISO 37002, and sustainable procurement pursuant to ISO 20400 with open-data publication via OCDS and, where applicable, IATI.

A Digital-Trust & Data-Protection Track operationalizes GDPR and ISO/IEC 27001 through a zero-trust reference architecture mapped to NIST CSF 2.0/SP 800-207 and enforced using Entra ID (conditional access, privileged identity), Intune (endpoint compliance), Purview (DLP, records, eDiscovery), Defender (threat protection), and Sentinel (SIEM/SOAR). A Results & Assurance Track builds MEL design, data quality assurance, and evaluation literacy aligned to Document 08, with preparation for independent assurance under ISAE 3000 and, where relevant, ISAE 3410. A Governance & Legal Track covers Host Country Agreements (Document 16), risk governance (Document 17), and co-financing standards (Document 14).

Delivery is embedded within live operations. Each competency module has entry criteria, on-the-job practicum, performance artifacts (policies, registers, control mappings), and exit criteria tied to tranche conditions under Document 20. For example, procurement readiness is evidenced by a published policy aligned to ISO 20400, functioning segregation of duties, sanctions screening, and first OCDS publications. Digital readiness is evidenced by conditional access baselines, DLP policies, and incident playbooks. ESG readiness is evidenced by a functioning grievance mechanism and approved ESIA/ESMP instruments. Where climate outcomes are claimed, the Curriculum requires GHG methodologies and data lineage suitable for ISAE 3410 assurance.

To prevent dependency and ensure sustainability, the Curriculum mandates a train-the-trainer sub-track and progressive transfer of delivery to local institutions. Progress is reviewed quarterly, documented in the Financial Transparency Register (Document 13, Chapter 5), and peer-reviewed under Document 09. Remedial instruction is triggered when KRIs (Document 17, Chapter 3) breach tolerance (Chapter 4), with corrective action plans linked to tranche re-sequencing.

Chapter 2 – Secondments and Exchanges

Secondments and exchanges institutionalize bidirectional learning and accelerate domestication of standards. They are governed by formal secondment agreements with precise scope, duration, IP, confidentiality, data-protection, and conflict-of-interest clauses, preserving the separation-of-functions doctrine and auditability.

Inbound Secondments place host-government or REC personnel within Creativa ecosystem teams (e.g., SUDESA, DESA PMO, GSCA institutions) to co-deliver SDEP/DESA/PCPP workstreams under supervision. Inbound secondees have access commensurate with role, enforced through least-privilege and conditional access controls in Entra ID, device compliance via Intune, and data governance through Purview. Personal data and official records are handled in compliance with GDPR and ISO/IEC 27001, with security monitoring by Defender and Sentinel.

Outbound Secondments assign Creativa personnel to ministries, RECs, or public entities to establish or strengthen country systems, always under functional immunities defined in Document 16 and with explicit non-interference boundaries. Outbound secondees implement capacity plans derived from Chapter 1 tracks, ensuring safeguards equivalence (World Bank ESF; IFC PS), fiduciary integrity (COSO; IIA IPPF), anti-bribery (ISO 37001), compliance (ISO 37301), whistleblowing (ISO 37002), and sustainable procurement (ISO 20400).

Exchanges are time-bound, reciprocal placements between analogous institutions (e.g., Nordic agencies under EUSL and partner country DESA teams) to transfer tested dossiers: procurement templates, ESG instruments, zero-trust blueprints, MEL indicator libraries, and co-financing clause sets (Document 14). Each exchange culminates in a Knowledge Transfer Dossier containing policies, standard operating procedures, control maps, and training assets licensed for reuse, with publication of non-sensitive artifacts in governed repositories. Where climate or nature outcomes are implicated, exchange deliverables include methods and data pipelines suitable for ISAE 3410 positioning.

Performance management is integral. All secondments and exchanges have learning objectives, on-the-job deliverables, and verification artifacts mapped to MEL indicators (Document 08) and KRIs (Document 17). Quarterly reviews verify attainment; deficiencies trigger remedial measures or rotation. To prevent conflicts, secondees sign annual conflict-of-interest and confidentiality declarations, and their activities are subject to internal audit under the IIA IPPF. Funding and per diem arrangements follow Document 13 (Chapters 3–4), with disclosures recorded in the Financial Transparency Register (Document 13, Chapter 5).

Finally, to ensure institutionalization rather than individualization, secondments and exchanges require the creation or enhancement of local training units capable of continuing delivery independent of Creativa support. Completion is certified only when host institutions can evidence sustained operations—policies in force, systems monitored, audits passed, and open-data disclosures maintained—consistent with the standards cited above and with the tranche logic and domestication milestones of Document 20.

Chapter 3 – Certification Pathways

Certification pathways establish the evidence-backed credentials that counterpart institutions and Creativa ecosystem entities must hold to execute and assure SDEP, DESA, and PCPP mandates. The regime is tiered, outcome-based, and auditable, integrating external standards and accredited third-party certification.

The baseline comprises four credential families. First, Safeguards & ESG Certification attests to systems equivalent to the World Bank ESF/IFC PS, with OHS and environmental controls substantiated through ISO 45001 and ISO 14001 certification where material. Second, Fiduciary, Anti-Corruption & Compliance Certification requires internal control maturity aligned with COSO, internal audit conformance to the IIA IPPF, and management-system certification under ISO 37001 Anti-Bribery and ISO 37301 Compliance, supported by protected reporting aligned with ISO 37002. Third, Digital Trust & Privacy Certification requires an ISO/IEC 27001-certified ISMS with cloud and privacy extensions (ISO/IEC 27017; ISO/IEC 27018; ISO/IEC 27701) and GDPR accountability. Fourth, Sustainable Procurement Certification institutionalizes ISO 20400 practices and open contracting publication commitments (OCDS/IATI) for transparency.

Credentials are issued at three levels to reflect institutional role and risk. The Practitioner level evidences competency to deliver under supervision, with artifacts such as approved ESMPs, grievance logs (IFC PS1/PS2/PS4), and published procurement notices in OCDS format. The Lead Implementer level validates the ability to design and operate controls end-to-end, including a functioning ISMS with zero-trust enforcement mapped to NIST CSF 2.0/SP 800-207, and rate-card-based cost controls consistent with Document 13. The Lead Assessor/Auditor level certifies competence to independently test and opine on systems in line with ISAE 3000/ISAE 3410 and ISO/IEC 17021-1 requirements for management-system certification bodies (ISO/IEC 17021-1).

Academic and research interfaces observe recognized quality-assurance norms. Where UCE/UACE partner with universities for formal credit or micro-credentials, programs align with the European Standards and Guidelines for Quality Assurance (EHEA ESG) and editorial integrity under COPE. These ensure integrity of assessment, recognition, and publication: ESG (EHEA); COPE Guidelines.

Digital and vendor-specific credentials are permitted as ancillary qualifications. Role-based Microsoft certifications may be mapped to Digital Trust tracks (e.g., security, compliance, identity), recorded against personnel profiles and tied to access privileges: Microsoft Credentials. Ancillary credentials do not substitute for the mandatory management-system and safeguards qualifications but strengthen competency evidence.

Accreditation, independence, and renewal are codified. External certifications must be issued by accredited bodies per ISO/IEC 17021-1 and renewed on a triennial cycle with annual surveillance. Internal credentials are renewed biennially with CPD requirements. Any lapse or scope reduction triggers risk escalation under Document 17 (Chapter 3) and may gate tranche releases per Document 20. Claims related to climate or nature outcomes that are used in public communications or financing instruments must be positioned for assurance under ISAE 3410 and disclosed in line with Document 13.

Chapter 4 – Digital Learning Platforms

Digital learning platforms are the delivery substrate for the Learn-by-Doing Curriculum and Certification Pathways. They must be secure by design, standards-interoperable, accessible, and auditable, with governance anchored in Document 12 (Data Protection & Digital Trust) and Document 13 (Financial Transparency).

The authorized stack comprises Microsoft 365 services and open standards. Microsoft Teams provides synchronous and asynchronous instruction, office hours, and cohort collaboration (Teams Overview). Viva Learning aggregates learning content and LMS integrations, enabling curation, assignments, and analytics (Viva Learning). SharePoint serves as the controlled content repository for syllabi, SOPs, and controlled documents with versioning and retention (SharePoint Introduction). Power Platform enables low-code workflows for enrollment, assessments, and credential issuance mapped to MEL indicators (Power Platform). Identity, device, data, and threat controls are enforced via Entra ID (conditional access, PIM), Intune (endpoint compliance), Purview (DLP, information protection, records, eDiscovery), Defender (threat protection), and Sentinel (SIEM/SOAR).

Interoperability follows education technology standards. Content and tracking must support SCORM and xAPI for portability and telemetry (SCORM – ADL; Experience API (xAPI) – ADL). Tool integration uses LTI and Open Badges for external courseware and credential portability (LTI – 1EdTech; Open Badges – 1EdTech). Where verifiable digital credentials are issued, the platform may adopt W3C Verifiable Credentials to enable cryptographically secure, privacy-preserving attestations (W3C VC Data Model 2.0).

Security, privacy, and accessibility are non-derogable. Platforms must maintain an ISO/IEC 27001-aligned ISMS with cloud privacy and security controls (ISO/IEC 27017; ISO/IEC 27018; ISO/IEC 27701), zero-trust enforcement under NIST CSF 2.0/SP 800-207, and GDPR-compliant data governance. Accessibility follows WCAG guidance for inclusive design and delivery (W3C WCAG).

Assessment, proctoring, and records are evidence-ready. High-stakes assessments must have identity assurance, proctoring, and anti-plagiarism controls commensurate with risk, with logs retained according to Records of Processing Activities and retention schedules under GDPR and Purview governance. Learning analytics and completion records are mapped to MEL indicators (Document 08) and are discoverable for external assurance under ISAE 3000. Where climate-related curricula underpin public claims, relevant data pipelines are designed for ISAE 3410 assurance positioning.

Open-data and transparency expectations apply. Non-sensitive curriculum metadata, participation statistics, and procurement for learning content or services shall be published in machine-readable form, favoring OCDS for procurements and IATI where aid funds are used (OCDS; IATI). Beneficial ownership of major learning vendors is disclosed consistent with Document 13. Academic QA linkages are maintained for UCE/UACE partnerships under ESG (EHEA) and COPE guidance to protect integrity in research-adjacent training (ESG (EHEA); COPE Guidelines).

Operational continuity is assured. Learning environments must have business-continuity and disaster-recovery plans aligned to ISO 22301, with tested RTO/RPOs, periodic failover tests, and incident-response runbooks integrated with security operations. All incidents trigger Document 17 escalation where thresholds are breached, with notifications and corrective actions recorded in the Financial Transparency Register (Document 13, Chapter 5).