Terra Vita Hub

Executive 4-page Institutional Brief

For ministries, MDBs/DFIs, sovereign programmes, auditors, procurement teams and IT/security reviewers.

Page 1 - What Terra Vita Hub is / is not

Terra Vita Hub is governance and MRV infrastructure that keeps institutional decisions reviewable, attributable, and export-ready, without replacing statutory authority, MRV methodologies, lending decisions, or committee judgement.

What it is

- A governed evidence spine for institutional decisions.
- A controlled environment for evidence intake, reviewer routing, conditions, MRV signal mapping, export posture and audit reconstruction.
- A public-to-protected diligence path: public materials explain the model; protected environments prove deployment-specific controls.

What it is not

- Not a statutory authority, MRV methodology approver, lender, investment adviser, rating engine, verifier, or automated decision-maker.
- Not a substitute for committee judgement, procurement review, financial approval, or sovereign decision-making.
- Not a public exposure surface for live programme data, personal data, security configurations, audit logs or residency settings.

Core authority boundary

Boundary	Minimum institutional interpretation
Human authority	All approvals, releases, exceptions and statutory determinations remain with authorised institutions.
MRV authority	MRV signals support review but do not replace approved methodologies or verification bodies.
Financial authority	Funding readiness is governed evidence posture, not a lending, investment or disbursement decision.

Page 2 - Institutional value and failure modes solved

Terra Vita Hub is designed for environments where decisions must survive committee review, auditor reconstruction, donor scrutiny, sovereign oversight and implementation handover.

Failure mode	How the Hub responds
Evidence drift	Evidence remains tied to source, context, programme, reviewer action and export posture.
Unattributed reviewer action	Material actions are identity-bound, role-scoped and time-stamped.
Opaque exceptions	Conditions, overrides, contradictions and escalations are recorded as governed events.
Non-reproducible committee packs	Exports preserve the evidence state, reviewer actions, conditions and unresolved risks at the time of release.
Unclear public/protected boundary	Public pages explain the model; protected walkthroughs demonstrate control evidence and deployment configuration.

Institutional review pathway

- Start with the Institutional Review Summary.
- Circulate the Institutional Pack Cover Memo and this executive brief.
- Use the Procurement-Safe Minimum Evidence Request for procurement, IT/security and vendor-risk review.
- Request a protected walkthrough for RBAC, audit events, evidence lineage, MRV attachment, export snapshots, residency controls and deployment-specific evidence.

Page 3 - Assurance posture

The assurance model has three public layers. Each layer answers a different institutional question.

Layer	Question answered	Institutional function
Governance Spine	Is the operating structure controlled?	Evidence intake, routing, reviewer action, workflow controls, approvals, audit lineage and export readiness.
Institutional Assurance Layer	Can the proof be reconstructed?	Evidence, reviewer attribution, audit trails, controls and assurance artefacts remain linked.
Institutional Review Index	Can the reviewer process itself be trusted?	Reviewer behaviour, consistency, calibration, bias/divergence and cross-programme comparability are governed.

Reliance boundary

Public governance narrative is not a certification or attestation. Formal reliance must be based on protected demonstrations, deployment-specific artefacts, contractual commitments, and independent evidence.

Minimum evidence to request

- Governance configuration: reviewer roles, escalation, overrides and audit-event samples.
- Security and operational assurance: encryption, uptime, disaster recovery and incident response.
- Data residency and lifecycle statement.
- Integration governance and API boundary documentation.
- Evidence lineage demonstration and export snapshot posture.
- Programme-specific configuration and contractual commitments.

Page 4 - Committee route and next steps

Default institutional route

- Read the Institutional Review Summary.
- Circulate the Institutional Pack Cover Memo and Executive 4-page Institutional Brief.
- Issue the Procurement-Safe Minimum Evidence Request for procurement, IT/security and vendor-risk teams.
- Request a purpose-bound protected walkthrough for deployment-specific proof.

Role routing

Reviewer role	Primary materials
Committees and senior decision-makers	Institutional Review Summary; Executive 4-page Brief; Cover Memo.
Procurement, vendor risk and legal	Control Evidence Boundary; Minimum Evidence Request; Operational Assurance.
IT/security and data protection	Operational Assurance; Control Evidence Boundary; integration and residency evidence.
Auditors, DFIs and climate funds	Diligence Evidence Map; IRI Whitepaper; Governance Spine & Assurance Annexes.
Programme teams	Deployment-specific configuration, reviewer groups, escalation pathways and evidence classes.

Final institutional position

Public materials are intentionally conservative. Protected walkthroughs contain the required operational proof. Contractual schedules define enforceable obligations.