

# Institutional Review Summary

PDF-ready public summary for ministries, DFIs, climate funds, sovereign programmes, auditors, procurement teams, and fiduciary reviewers.

Terra Vita Hub provides a controlled governance environment for institutions that require traceable, evidence-bound decision processes. The platform strengthens institutional decision integrity without replacing statutory authority, regulatory mandates, financial decision-making, or approved MRV methodologies. All final approvals remain with ministries, competent authorities, and designated committees.

Public pages define the governance architecture, authority boundaries, control domains, and reviewer route. They do not expose live evidence, security configurations, logs, residency controls, or deployment-specific settings. Formal reliance requires a purpose-bound protected walkthrough and, where applicable, deployment-specific artefacts.

**Public governance clarity + protected operational proof + deployment-specific contractual commitments = the basis for institutional reliance.**

## Committee-Ready Institutional Review Summary

Area	Institutional summary
Purpose of the platform	Governance and MRV infrastructure used to maintain attributable, evidence-bound decision processes. The platform is not a decision-maker; it provides the controlled environment in which authorised institutional actors make, record, and defend their own decisions.
Governance spine	Identity and access control, evidence and lineage, routing and conditions, MRV signal governance, and audit reconstruction remain stable across sectors and deployments.
Institutional control boundary	Public pages are not certifications, SOC/ISO attestations, contractual guarantees, or deployment evidence. Formal reliance requires protected walkthrough evidence, deployment-specific artefacts, contractual commitments, and third-party assessments where required.
Operational and security assurance	Reviewers should evaluate security posture, operational reliability, data lifecycle, sovereignty, integration surfaces, risk and safeguards interfaces, and support/incident-response posture.

## Governance Spine Domains

Domain	Institutional meaning
Identity & Access Control	Individually attributable reviewers, roles, permissions, and privileged actions.
Evidence & Lineage	Governed intake, attachments, provenance, timestamps, and programme context.
Routing & Conditions	Reviewer actions, escalation logic, threshold breaches, overrides, contradictions, and exceptions.
MRV Signal Governance	Evidence-to-indicator pathways without replacing approved methodology authority.
Audit Reconstruction	Chronological replay of decisions, reviewer actions, export posture, and material events.

## Formal Reliance Requires

- Protected walkthrough: RBAC, audit events, evidence lineage, MRV attachments, reviewer actions, and export posture.
- Deployment-specific artefacts: residency configuration, security packs, incident response / BCDR evidence, and control settings.
- Contractual commitments: DPA, SLA, security responsibilities, retention, deletion, sovereignty, and support obligations.
- Third-party assessments where required by procurement, institutional policy, law, or supervisory route.

## Operational and Security Assurance Domains

Domain	Review focus
Security posture	Encryption, privileged access, environment isolation, monitoring, access logging, vulnerability management, and security assessment evidence.
Operational reliability	Continuity, RPO/RTO, incident response, uptime posture, support paths, escalation, change management, and deployment controls.
Data lifecycle	Retention, destruction, withdrawal, derived-data handling, rejected or overridden evidence, lineage preservation, and export boundaries.
Sovereignty	Region locking, tenancy isolation, export controls, jurisdictional constraints, residency configuration, and support-access limitations.
Integration	API surfaces, identity federation, evidence ingress/egress, registry connectors, committee-pack formats, and integration audit logs.
Risk and safeguards	ESG/IFC/ESS alignment where applicable, safeguard evidence objects, grievance and incident routes, and risk-register interfaces.

## Diligence Evidence Map

- Identity attribution: every material action tied to actor, role, programme context, and timestamp.
- Evidence lineage: evidence objects remain linked to source, context, MRV signal, reviewer action, and decision posture.
- Routing and conditions: escalations, contradictions, overrides, unresolved risks, and exceptions remain visible and attributable.
- Export snapshots: committee packs preserve state at time of release.
- Sovereignty controls: residency, retention, access, export, and isolation rules are deployment-configured and reviewable.
- Audit reconstruction: decision chain can be replayed from intake through review, escalation, export, and closeout.

## Institutional Suitability

Terra Vita Hub is suitable for institutions requiring multi-reviewer integrity, traceable evidence chains, condition-based approval pathways, sovereign-grade data governance, reconstructable committee or funding decisions, and MRV-informed but authority-preserving workflows.

It is not a regulated financial institution, investment advisor, methodology approver, statutory authority, verifier, or rating engine.

## Final Position

The platform's institutional claim becomes complete only when the governance spine is tested against protected proof: identity, evidence, routing, MRV, audit, export, sovereignty, and deployment isolation must remain connected throughout the decision chain.

The public pages are intentionally conservative. The protected environment contains the required evidence. The contractual layer defines enforceable obligations.

## Companion Public Materials

Material	Purpose
Institutional Review Index	Public entry point for the review sequence and assurance materials.
Diligence Evidence Map	Defines what reviewers can test publicly and what must be verified in protected review.
Control Evidence Boundary	Separates public narrative from deployment-specific control evidence and contractual commitments.
Operational Assurance	Sets out security, reliability, data lifecycle, sovereignty, integration, support, and safeguards review domains.
Governance Spine & Assurance Annexes	Detailed annex pack for sovereignty, identity, audit/RLS, MRV attachment, and deployment architecture.
IRI Whitepaper	Reviewer-assurance and meta-governance layer for consistency, calibration, bias/divergence, and oversight.