Capital Investment Club

Transfer Assessment Evidence Index

Index connecting each TIA conclusion to public evidence or to a classified, controlled evidence record without exposing restricted material.

Status: Draft for external legal and privacy review
Version: 0.9
Supersedes: None - initial publication
Last reviewed: 12 August 2026
Next review: 12 November 2026
Owner: Governance administrator - confirmation required
Approver: Privacy and compliance owner - pending

Document control	Value
Document ID	CIC-PIA-TIA-009
Version	0.9
Superseded version	None - initial publication
Status	Draft for external legal and privacy review
Publication classification	Public
Owner	Governance administrator - confirmation required
Approver	Privacy and compliance owner - pending
Effective date	Pending approval
Last reviewed	12 August 2026
Next review	12 November 2026 or earlier after a material change

Purpose

This index connects public conclusions to evidence without publishing secrets, account details, personal information, private contracts, detailed security architecture, or restricted operational records. It also exposes where evidence is missing so that external readers do not mistake repository inference for confirmed production fact.

Evidence classifications

Classification	Public handling
Public	May be linked or reproduced where licensing and accuracy permit.
Internal	Identify the record class and conclusion; do not publish operational detail.
Confidential	Identify only the evidence ID, owner class, review date, and conclusion where appropriate.
Restricted	Do not publish contents, account identifiers, security detail, secrets, personal data, or request records.

Public evidence

Evidence ID	Evidence	Supports	Status
PUB-01	CIC Privacy Policy (/governance/documents/privacy-policy)	Transparency, data use, sharing, rights, retention, and security baseline	Published; reconcile after provider inventory.
PUB-02	Data Classification, Privacy, and Retention Policy (/governance/documents/data-classification-privacy-and-retention-policy)	Classification, handling, retention, deletion, and evidence expectations	Published.
PUB-03	Third Party Risk Management Policy (/governance/documents/third-party-risk-management-policy)	Vendor classification, diligence, monitoring, evidence, and offboarding	Published.
PUB-04	Access Control Policy (/governance/documents/access-control-policy)	Least privilege, privileged access, support access, service accounts, and reviews	Published.
PUB-05	Incident Response Policy (/governance/documents/incident-response-policy)	Incident triage, containment, investigation, communication, and remediation	Published.
PUB-06	Information Security Policy (/governance/documents/information-security-policy)	Security baseline across data, engineering, vendors, incidents, and monitoring	Published.
PUB-07	Financial Operations and Reconciliation Policy (/governance/documents/financial-operations-and-reconciliation-policy)	Wallet, payment, ledger, posting, duplicate-prevention, and reconciliation controls	Published.
PUB-08	Customer Support and Identity Verification Policy (/governance/documents/customer-support-and-identity-verification-policy)	Authenticated support and purpose-specific access controls	Published.

Evidence ID	Evidence	Supports	Status
PUB-09	Secure SDLC and Change Management Policy (/governance/documents/secure-software-development-and-change-management-policy)	Repository, testing, deployment, secret, and change controls	Published.
PUB-10	EDPB Recommendations 01/2020 (https://www.edpb.europa.eu/documents/recommendation/recommendations-012020-on-measures-that-supplement-transfer-tools-to_en)	EU transfer assessment and supplementary-measure method	Public legal guidance.
PUB-11	European Commission SCC decision (https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=en)	EU standard contractual clauses	Public legal instrument.
PUB-12	ICO transfer risk assessment guidance (https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/completing-a-transfer-risk-assessment/)	UK transfer risk assessment method	Public regulator guidance.
PUB-13	Nigeria Data Protection Act 2023 (https://ndpc.gov.ng/wp-content/uploads/2024/03/Nigeria_Data_Protection_Act_2023.pdf)	Nigeria privacy and cross-border legal framework	Public legislation.
PUB-14	Canada OPC cross-border guidance (https://www.priv.gc.ca/en/privacy-topics/airports-and-borders/gl_dab_090127/)	Canadian accountability and comparable protection	Public regulator guidance.
PUB-15	US Department of Justice CLOUD Act resources (https://www.justice.gov/criminal/cloud-act-resources)	United States lawful-access context	Public government material.
PUB-16	Google Cloud Data Processing and Security Terms (https://cloud.google.com/terms/data-processing-addendum)	Provider contractual framework	Public provider material; CIC execution and scope require controlled evidence.
PUB-17	Google Cloud subprocessors (https://cloud.google.com/terms/subprocessors)	Provider onward-recipient reference	Public provider material; CIC subscription and active services require controlled evidence.

Controlled evidence requirements

Evidence ID	Controlled evidence class	Supports	Current state
CTL-01	CIC legal-entity, establishment, registration, and role matrix	Applicable law, exporter, controller/processor, contract selection	Confirmation required.

Evidence ID	Controlled evidence class	Supports	Current state
CTL-02	Named governance owner and delegate register	Accountability and approvals	Confirmation required.
CTL-03	Active provider and product reconciliation export	Complete transfer inventory	Confirmation required.
CTL-04	Cloud service, project, storage, backup, region, support, and access export	T-01, T-02, T-15 and TR-03	Confirmation required.
CTL-05	Database provider, cluster, region, backup, encryption, access, DPA, and subprocessor pack	T-03 and TR-02	Confirmation required.
CTL-06	Executed provider contract, DPA, security exhibit, and deletion terms	Contractual safeguards	Confirmation required per active provider.
CTL-07	Completed SCC, UK IDTA/Addendum, Nigerian safeguard, Canadian protection, or adequacy/certification record	Lawful transfer mechanism	Confirmation required per transfer.
CTL-08	Provider and subprocessor location inventory with retrieval dates	Jurisdiction and onward-transfer analysis	Confirmation required.
CTL-09	Financial and identity product field maps and activation decisions	T-06 to T-10 and TR-04	Confirmation required.
CTL-10	Communications provider/channel map and template minimization review	T-05 and TR-06	Confirmation required.
CTL-11	Video, voice, screen, recording, consent, routing, storage, retention, and deletion export	T-12 and TR-05	Confirmation required.
CTL-12	Workforce/contractor location, role, contract, training, device, and access inventory	T-16 and TR-07	Confirmation required.
CTL-13	Restricted-field encryption, key, rotation, recovery, and plaintext-necessity matrix	TR-10 and technical safeguards	Partial implementation evidenced; controlled verification required.
CTL-14	Privileged and Restricted-data access certification	Access-control effectiveness	Operating evidence required.
CTL-15	Audit, masked reveal, correction, appeal, compliance-reporting, and notification test evidence	Application privacy controls	Implementation evidence exists; production effectiveness review required.
CTL-16	Retention schedule, dry-run, authorized deletion, provider deletion, and backup evidence	TR-11	Partial design evidenced; approval and operating record required.
CTL-17	Subprocessor change subscriptions, notices, deadlines, assessments, and decisions	TR-08	Confirmation required.

Evidence ID	Controlled evidence class	Supports	Current state
CTL-18	Government-request policy, provider transparency material, request history, and CIC case records	TR-12	Provider evidence required; case records remain Restricted.
CTL-19	Integration suspension and fallback runbooks	TR-14	Documented process required; technical feasibility confirmation required.
CTL-20	Credential rotation attestations and relevant access/log review	TR-18	Open; values must never be included.
CTL-21	Privacy, security, business, executive risk, and counsel approvals	Final decision	Pending.

Source-code evidence boundary

Repository evidence can establish that:

- a service is deployed through a named cloud platform;
- a dependency, route, workflow, model, environment-variable name, or adapter exists;
- selected application controls and tests have been implemented;
- governance documents and deployment workflows exist.

Repository evidence cannot by itself establish that:

- an optional integration is active in production;
- a named provider is the contracting legal entity;
- a provider account uses a particular storage or support region;
- current DPA, SCC, IDTA, certification, or subprocessor terms are executed and applicable;
- production controls operate effectively over time;
- no government request, incident, exception, or out-of-band disclosure occurred.

Evidence integrity and access

Controlled records must be stored in an access-restricted governance location. Record retrieval or test date, source, owner, classification, retention, linked risk/action, and review date. Integrity hashes may be retained where proportionate, but they must not be used to expose secret material. Access to Restricted evidence must be least privilege and audited.

Publication review checklist

Before publishing any revision:

- scan report content and deployment configuration for credentials, tokens, private keys, credential-bearing URIs, private endpoints, personal data, account identifiers, and restricted architecture;
- verify every internal governance link resolves;
- verify public external legal and provider sources resolve;

- verify document IDs, versions, statuses, dates, owners, and approval posture agree;
- verify browser and PDF rendering on desktop and mobile widths;
- verify no Integration evidenced statement became a production-use claim without controlled evidence;
- obtain security, privacy, governance, accessibility, and counsel review appropriate to the change.

Current evidence conclusion

The public and repository evidence supports publication of a transparent draft assessment. It does not support a final legal approval or certification. CTL-01 through CTL-21 define the evidence needed to close the remaining gaps.

Limitation

This index was prepared with AI assistance. Controlled evidence owners must confirm existence, integrity, access, retention, conclusions, and completion.