Capital Investment Club

Transfer Remediation and Review Plan

Actionable closure plan for transfer fact confirmation, contracts, approvals, supplementary safeguards, monitoring, and reassessment.

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: Privacy program owner - confirmation required
Approver: Executive owner and privacy counsel - pending

Document control	Value
Document ID	CIC-PIA-TIA-008
Version	0.9
Superseded version	None - initial publication
Status	Draft for external legal and privacy review
Publication classification	Public
Owner	Privacy program owner - confirmation required
Approver	Executive owner and privacy counsel - pending
Effective date	Pending approval
Last reviewed	12 August 2026
Next review	12 November 2026 or earlier after a material change

Delivery objective

The objective is to convert the public working assessment into an approved, evidence-backed transfer program without representing documentation exercises as completed operational drills. Work is sequenced by risk and dependency rather than by long calendar phases. Independent owners may execute compatible actions in parallel.

Completion gates

The package can move from Draft to Approved only when:

- CIC legal entities, establishments, controller/processor roles, and accountable owners are named;
- every active provider, product, subprocessor, destination, and workforce-access country is reconciled;
- every material transfer has a lawful mechanism and completed supporting particulars;
- High risks are remediated, avoided, or explicitly time-limited and accepted where legally permissible;
- controlled evidence supports locations, contracts, security, retention, deletion, access, incidents, and monitoring;
- privacy, security, business, executive risk, and qualified counsel approvals are recorded;
- the public package passes disclosure, accessibility, link, rendering, and consistency review.

Action plan

Action ID	Action and evidence required	Accountable role	Priority and dependency	Exit condition
A-01	Confirm CIC legal entity or entities, establishments, registrations, exporter/importer roles, and relevant privacy representatives. Retain signed owner attestation and legal analysis.	Executive owner and counsel	Critical; first dependency	Controlled entity matrix approved.
A-02	Name privacy, security, vendor-risk, infrastructure, finance, communications, people, records, incident, and executive risk owners.	Executive owner	Critical; parallel with A-01	Governance register contains named owners and delegates.
A-03	Reconcile the source-derived provider list against contracts, invoices, production consoles, feature flags, network or audit evidence, and product owners.	Privacy program and infrastructure owners	Critical; after owners named	Every inventory row is Active, Inactive, Planned, or Retired with evidence date.
A-04	Export storage, processing, backup, support, remote-access, and subprocessor locations for each active provider. Keep account identifiers and topology in restricted evidence.	Infrastructure and vendor-risk owners	Critical; after A-03	Every active transfer has location evidence and retrieval date.
A-05	Confirm database provider, cluster and backup regions, encryption, keys, privileged access, support, DPA, transfer terms, deletion, continuity, and subprocessors.	Infrastructure and security owners	Critical	TR-02 is remediated or transfer redesigned.

Action ID	Action and evidence required	Accountable role	Priority and dependency	Exit condition
A-06	Complete Google Cloud hosting and storage evidence: entity, services, regions, backups, support, DPA, transfer terms, subprocessors, access, logging, deletion, and continuity.	Cloud owner	Critical	T-01, T-02, and T-15 have approved controlled records.
A-07	Assess each active financial and identity product independently, including fields, consent or legal basis, recipient roles, locations, contracts, retention, deletion, incidents, and transfer mechanism.	Finance, product, privacy, and counsel	Critical; after A-03	Every enabled rail has a signed decision; others are disabled or remain non-production.
A-08	Confirm real-time communication and recording state, routing, storage, consent, access, retention, deletion, provider terms, and mechanism.	Product, security, and privacy owners	Critical if recording active	Recording is approved with evidence or remains disabled.
A-09	Inventory employee, contractor, reviewer, approver, support, and incident-responder access countries; reconcile role, contract, training, device, access, and review records.	People and security owners	Critical	T-16 destination and safeguard record approved.
A-10	Execute correct EU SCC modules, UK IDTA/Addendum, Nigerian safeguards, Canadian protections, or approved adequacy/certification route for each flow. Complete annexes and verify certification scope.	Privacy owner and counsel	Critical; after A-01, A-03, A-04	Each active flow has a mechanism identifier, effective date, and approval.
A-11	Complete provider-specific government-access analysis using destination law, actual data, technical architecture, request policy/history, challenge commitments, and redress.	Counsel, privacy, and security	High; after A-04	Jurisdiction addendum approved per High-risk provider.
A-12	Validate field-level encryption coverage, key sources, access, rotation, recovery, and provider plaintext needs. Document where encryption cannot be an effective supplementary measure.	Security and engineering owners	High	Key/field matrix approved and gaps remediated.

Action ID	Action and evidence required	Accountable role	Priority and dependency	Exit condition
A-13	Validate role access, masking, audited reveal, service credential scopes, support access, and quarterly certification.	Security and application owners	High	Baseline access certification completed and exceptions closed.
A-14	Approve data and provider retention schedules; test dry run; execute authorized deletion; verify provider deletion and backup treatment.	Records and data owners	High	Schedule and first operating record approved.
A-15	Document kill switch, fallback, preservation, owner escalation, and user-impact behavior for every High-risk integration. This is a documented process requirement; a destructive production drill is not required for publication.	Product and infrastructure owners	High	Runbook reviewed and technically feasible controls confirmed.
A-16	Operate subprocessor notice subscriptions and record objection deadlines, assessment, decision, and register updates.	Vendor-risk owner	High	Every active provider has subscription or documented monitoring alternative.
A-17	Rotate credentials previously present in tracked deployment configuration; review relevant access/log history; validate deployment using protected secrets. Do not place values in evidence.	Service and security owners	Critical security action	Rotation attestations, deployment validation, and incident decision recorded.
A-18	Review privacy notices, provider disclosures, rights routing, and contact details against the reconciled inventory.	Privacy and communications owners	High; after A-03	Public notices accurately describe material transfers.
A-19	Review response procedures for government requests, provider failure, new subprocessors, transfer suspension, and incidents. Procedures may be marked Documented, not yet exercised.	Legal, privacy, security, and incident owners	High	Named owners approve usable runbooks and contact routes.
A-20	Complete public disclosure review, accessibility checks, route and PDF checks, legal-source checks, and restricted-information scan.	Governance, security, accessibility, and counsel	Final publication gate	All checks pass and exceptions are documented.

Action ID	Action and evidence required	Accountable role	Priority and dependency	Exit condition
A-21	Record privacy, security, business, executive risk, and counsel decisions for each residual Medium-High or High risk and for the complete package.	Executive risk owner	Final approval gate	Signed approval schedule complete.

Evidence handling

Public evidence includes the report package, policies, high-level control descriptions, and links to public legal or provider sources. Controlled evidence includes contracts, console exports, account and project identifiers, network/security architecture, key-management details, audit logs, government requests, personal data, incident records, and signed internal approvals.

Each controlled evidence item must have an ID, title, owner, classification, source, retrieval or test date, integrity reference where used, retention, access group, linked action/risk, and review date. The public evidence index may identify the record class and status but must not expose restricted content.

Review schedule

Review	Cadence	Required output
Open-remediation review	At least monthly until final approval	Updated actions, risks, blockers, evidence, and owner decisions.
Transfer register reconciliation	Quarterly and after material change	Active provider, location, mechanism, subprocessor, workforce, and risk updates.
High-risk provider review	At least annually and after material change	Diligence, contract, location, government-access, safeguard, incident, and continuation decision.
Certification or adequacy check	At approval and each scheduled review where relied upon	Current scope, entity, effective status, and alternative mechanism if unavailable.
Access certification	At least quarterly for privileged and Restricted-data access	Access list, reviewer, exceptions, removals, and evidence.
Public package review	At least annually and after material change	Updated reports, approval status, dates, links, PDFs, and publication check.

Immediate reassessment triggers

- new provider, product, subprocessor, destination, support region, or workforce country;
- new Restricted data, expanded purpose, or materially larger scale;
- controller, importer, or contractual-entity change;
- adequacy, DPF, SCC, IDTA, statutory, or regulator-guidance change;
- material security incident, unauthorized access, provider failure, or government request;
- encryption, key-control, identity, access, retention, recording, or architecture change;

- unresolved rights request or evidence that a safeguard is ineffective.

Escalation

An overdue critical action, unknown High-risk transfer, expired mechanism, failed safeguard, or unassessed Restricted-data destination must be escalated to the executive risk owner. New data transfers must be narrowed or suspended where required to prevent unapproved exposure. Business urgency does not silently override the decision rule.

Publication and approval record

Until the completion gates are met, all nine reports retain version 0.9 and Draft for external legal and privacy review status. Approval requires a new version, effective date, named owner and approver, signed decision record, and change summary. The historical draft remains available according to CIC governance retention requirements.

Limitation

This action plan was prepared with AI assistance. Named owners must confirm feasibility, evidence, legal conclusions, completion, and acceptance decisions.