Capital Investment Club

Transfer Risk Register

Traceable register of transfer risks, existing safeguards, treatments, residual ratings, owners, approval requirements, and reassessment triggers.

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 and enterprise risk owners - confirmation required
Approver: Executive risk owner and privacy counsel - pending

Document control	Value
Document ID	CIC-PIA-TIA-007
Version	0.9
Superseded version	None - initial publication
Status	Draft for external legal and privacy review
Publication classification	Public
Owner	Privacy and enterprise risk owners - confirmation required
Approver	Executive risk 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

Rating method

Likelihood and impact are rated Low, Medium, or High. Residual risk reflects the current evidence state after evidenced safeguards, not the safeguards CIC intends to add. A missing transfer mechanism, unknown importer, unknown destination, or ineffective safeguard prevents an Approved decision for Restricted data.

Treatment decisions are:

- Mitigate: implement additional contractual, technical, or organizational controls.
- Avoid: stop or redesign the transfer.
- Transfer: allocate defined obligations contractually without treating the contract as complete risk removal.

- Accept: named executive risk owner accepts a time-limited residual risk after privacy, security, and legal review.

Active register

Risk ID	Risk and affected transfers	Current safeguards	Residual risk	Required treatment and owner	Decision state
TR-01	Actual production providers and optional integrations are not fully reconciled, causing incomplete transfer mapping. Affects T-01 to T-15.	Repository inventory and public processing register.	High	Privacy program owner must reconcile contracts, invoices, consoles, logs, and features.	Open; no blanket approval.
TR-02	Database provider, cluster, backup, and support locations are unconfirmed while broad Confidential and Restricted data may be stored. Affects T-03.	Connection security, application access controls, selected field encryption and masking.	High	Infrastructure owner must export provider, regions, encryption, access, backup, DPA, mechanism, and subprocessor evidence.	Suspend expansion of Restricted data if closure evidence cannot be produced.
TR-03	Cloud hosting/storage legal entity, exact region commitments, backups, support, and transfer terms are incomplete. Affects T-01, T-02, T-15.	Confirmed deployment architecture, transport security, access controls, governance policies.	Medium-High; High for identity files	Cloud owner must complete controlled evidence pack and counsel review.	Open with conditions; approval pending.
TR-04	Financial and identity providers can receive highly sensitive data without product-by-product transfer decisions. Affects T-06 to T-10.	Data minimization rules, webhook controls in selected paths, role restrictions, reconciliation controls.	High	Finance and privacy owners must approve each active rail, field map, provider entity, location, contract, mechanism, retention, deletion, and incident terms.	New unassessed products not approved.
TR-05	Voice, video, screen, and recording routing/storage locations and consent controls are unconfirmed. Affects T-12.	Role-based session access and recording workflow capability.	High	Product, security, and privacy owners must verify production state, routing, storage, consent, retention, deletion, provider terms, and mechanism.	Recording remains unapproved where evidence is absent.
TR-06	Email and notification content may expose sensitive information through an unconfirmed active provider or routing chain. Affects T-05.	Preference separation, templates, suppression handling, security notification design.	Medium-High	Communications owner must map provider by channel, minimize templates, confirm terms, locations, subprocessors, retention, and deletion.	Open.
TR-07	CIC workforce and contractor access countries are not inventoried, so remote access transfers may be omitted. Affects T-16.	Role-based access, admin separation, audit design, personnel governance.	High	People, security, and privacy owners must maintain location, role, access, contract, training, and review records.	New Restricted-data access from unassessed countries not approved.

Risk ID	Risk and affected transfers	Current safeguards	Residual risk	Required treatment and owner	Decision state
TR-08	Provider subprocessors or support locations may change without timely review. Affects all vendor transfers.	Vendor governance process and review triggers.	Medium-High	Vendor-risk owner must subscribe to notices, record deadlines, assess material changes, and document acceptance or objection.	Open.
TR-09	Executed SCCs, UK terms, Nigerian safeguards, Canadian comparable-protection evidence, or DPF scope may not match each actual flow.	Public legal framework and mechanism decision rules.	High	Privacy owner and counsel must select, complete, and approve a mechanism per transfer.	No legal approval inferred.
TR-10	Provider or public-authority access to plaintext may defeat encryption as a supplementary measure.	Transport encryption, provider encryption, selected field-level encryption, masking, minimization.	Medium-High to High	Security owner must document key control and plaintext necessity; redesign or suspend where effective protection cannot be achieved.	Transfer-specific decision required.
TR-11	Retention and deletion may differ across CIC and provider systems, extending cross-border exposure.	Retention analysis, deletion policy, dry-run capability, account-closure workflows.	Medium-High	Data owner must approve schedules and verify provider deletion, backups, legal holds, and completed runs.	Open.
TR-12	Government requests may be overbroad, secret, or difficult for affected people to challenge.	Documented request procedure, contract diligence requirements, minimization and audit.	Medium-High	Legal and privacy owners must confirm provider commitments and request history; apply case procedure and reassess after a request.	Documented, not yet exercised for this assessment.
TR-13	Evidence publication could expose credentials, private endpoints, architecture, personal data, or contract-confidential information.	Public/restricted evidence separation, redaction rules, source review.	Medium	Governance and security owners must run disclosure validation and manual review before every publication.	Mitigation implemented in publication workflow; recurring review required.
TR-14	CIC cannot promptly stop one provider flow if a mechanism or safeguard fails.	Policy suspension rule and environment-configured integrations.	Medium-High	Product and infrastructure owners must document kill switches, fallback behavior, preservation requirements, and owner escalation per active provider.	Technical coverage requires confirmation.
TR-15	A destination law, adequacy decision, certification, or provider practice may change between scheduled reviews.	Quarterly review schedule and material-change triggers.	Medium	Privacy owner must operate legal/provider monitoring and create immediate reassessment records for material changes.	Owner and evidence required.

Risk ID	Risk and affected transfers	Current safeguards	Residual risk	Required treatment and owner	Decision state
TR-16	Controller identity, establishment, and exporter role are not confirmed, creating uncertainty in applicable law and contract selection.	Governance documents identify role questions.	High	Executive and legal owners must confirm legal entities, establishments, registrations, and role per processing purpose.	Blocks final approval.
TR-17	Public draft may be misrepresented as legal approval, certification, or warranty.	Prominent draft status, limitations, evidence states, and no blanket approval.	Medium	Governance owner must preserve status metadata and obtain approval before changing to Approved.	Controlled by publication design.
TR-18	Historical evidence may include exposed credentials previously committed to source control.	Current deployment configuration removes runtime secrets from tracked descriptor and uses protected repository secrets.	High until rotation	Service owners must rotate every affected credential, review access and logs, validate deployment, and record completion without publishing secret values.	Open security remediation.

Risk ratings

Risk ID	Likelihood	Impact	Inherent risk	Residual risk	Treatment
TR-01	High	High	High	High	Mitigate through production reconciliation and owner approval.
TR-02	Medium	High	High	High	Mitigate urgently; avoid expansion if evidence cannot be produced.
TR-03	Medium	High	High	Medium-High to High	Mitigate through provider, region, contract, and safeguard evidence.
TR-04	Medium	High	High	High	Mitigate per product; avoid unapproved rails.
TR-05	Medium	High	High	High	Mitigate or keep recording disabled.
TR-06	Medium	Medium	Medium-High	Medium-High	Mitigate through channel mapping and content minimization.
TR-07	Medium	High	High	High	Mitigate through location inventory and least-privilege certification.
TR-08	Medium	High	High	Medium-High	Mitigate through notice monitoring and timely assessment.

Risk ID	Likelihood	Impact	Inherent risk	Residual risk	Treatment
TR-09	Medium	High	High	High	Mitigate through executed and approved mechanisms; avoid otherwise.
TR-10	Medium	High	High	Medium-High to High	Mitigate technically; avoid transfer where data cannot be protected.
TR-11	Medium	High	High	Medium-High	Mitigate through approved schedules and verified deletion.
TR-12	Low to Medium	High	High	Medium-High	Mitigate contractually and procedurally; reassess after any request.
TR-13	Medium	High	High	Medium	Mitigate through automated scanning and manual disclosure review.
TR-14	Medium	High	High	Medium-High	Mitigate through tested feasibility of provider-level suspension.
TR-15	Medium	High	High	Medium	Mitigate through quarterly monitoring and immediate triggers.
TR-16	High	High	High	High	Mitigate through entity and role confirmation before legal approval.
TR-17	Medium	Medium	Medium	Medium	Mitigate through immutable Draft metadata and approval governance.
TR-18	Medium	High	High	High until rotation	Mitigate through rotation, revocation, log review, and incident decision.

Risk acceptance requirements

A Medium-High or High transfer risk can be accepted only when the record includes:

- precise transfer scope and business necessity;
- reason mitigation or avoidance is not currently proportionate;
- applicable legal mechanism and counsel decision;
- compensating safeguards and evidence;
- affected data and people;
- monitoring and incident triggers;
- named privacy, security, business, and executive risk owners;
- start date, expiration date, and maximum review period;

- actions required before renewal.

High-risk acceptance must not be indefinite. It cannot override a legal prohibition or substitute for a missing required mechanism.

Priority order

The critical closure sequence is:

- confirm CIC legal entities and responsible owners;
- reconcile active providers and production destinations;
- close database and Restricted-file hosting evidence;
- close financial, identity, recording, and workforce-access flows;
- execute and approve applicable transfer mechanisms;
- rotate historically exposed credentials and verify access history;
- confirm technical suspension, deletion, and recurring monitoring controls;
- obtain executive and counsel approval.

Review triggers

Any material provider, product, data, purpose, destination, workforce, legal, certification, incident, government-request, architecture, encryption, retention, or subprocessor change requires review. Risks must also be reviewed at least quarterly while this report remains draft.

Limitation

This public register omits restricted technical and contractual evidence. It was prepared with AI assistance and requires named-owner confirmation and counsel review.