Capital Investment Club

Transfer Impact Assessment Executive Summary

Decision-focused summary of CIC transfer scope, safeguards, material residual risks, approval dependencies, and publication posture.

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 compliance owner - confirmation required
Approver: Executive owner and privacy counsel - pending

Document control	Value
Document ID	CIC-PIA-TIA-002
Version	0.9
Superseded version	None - initial publication
Status	Draft for external legal and privacy review
Publication classification	Public
Owner	Privacy and compliance 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

Purpose

This summary explains CIC's current international transfer posture and the decisions required before the full Transfer Impact Assessment can be approved.

Overall conclusion

CIC operates a globally accessible platform using cloud infrastructure and integrations that can transfer or

remotely expose personal information across borders. The platform has meaningful privacy and security controls, but the reviewed source configuration does not prove every active provider, contract, storage region, support location, or transfer mechanism.

Overall posture: Medium-High, with High provider-specific risks pending confirmation.

This does not mean every transfer is unlawful or unsafe. It means CIC must not represent a transfer as approved until the responsible owner confirms the actual transfer circumstances and qualified counsel approves the mechanism where legal judgment is required.

What is confirmed

- CIC uses Google App Engine deployment and Google Cloud storage capabilities.
- CIC services use MongoDB-compatible database connectivity.
- CIC processes account, profile, KYC/KYB, identity, financial, wallet, marketplace, support, notification, security, audit, and careers information.
- CIC code contains provider paths for authentication, payments, banking, verification, email, notification, recordings, e-signature, and operational integrations.
- CIC has implemented masking and audited reveal for selected restricted information, application-level encryption for selected identifiers, correction and appeal workflows, notification preference controls, retention analysis, and compliance reporting.
- CIC has public governance policies for privacy, data classification, access, incident response, vendor risk, financial operations, support verification, and retention.

What requires confirmation

- CIC controller legal entity and relevant establishments.
- Which optional integrations are active in production.
- Contracting entity and executed DPA for each provider.
- Database provider and cluster region.
- Cloud service-specific storage, backup, support, and subprocessor locations.
- Transfer mechanism for each source-to-destination relationship.
- Current EU-US Data Privacy Framework participation where relied upon.
- Workforce and contractor remote-access countries.
- Production provider request history and transfer-impact evidence.

Highest-risk transfer families

Transfer	Why it matters	Required decision
Database hosting	Can contain nearly every CIC data category, including Restricted data.	Confirm provider, region, DPA, support access, onward transfers, encryption, and transfer mechanism.
KYC/KYB and financial verification	Identity documents and financial/national identifiers create severe misuse impact.	Confirm every external recipient, minimize fields, execute required terms, and approve supplementary safeguards.

Transfer	Why it matters	Required decision
Payments and banking	Providers may receive transaction, bank, identity, and compliance information.	Confirm active rails and provider-specific flows rather than approving all configured integrations.
Calls and recordings	Audio, video, screens, and support content may expose highly sensitive information.	Confirm production use, routing, recording location, consent, retention, access, and deletion.
Remote workforce access	Authorized personnel may access data from another jurisdiction without a storage change.	Inventory countries, limit privileges, certify access, and document transfer treatment.

Current safeguards

- Encrypted transport.
- Provider-managed encryption at rest where supported.
- Application-level encryption for selected restricted fields.
- Restricted-value masking and reason-gated audited reveal.
- Role-based admin, reviewer, approver, and support access.
- Data correction, appeal, and restricted-user recovery paths.
- Notification category and preference separation.
- Compliance audit events, dashboards, exports, and retention dry runs.
- Governance policies for vendors, access, incidents, classification, and financial integrity.

These controls reduce risk but do not replace an executed transfer mechanism or provider-specific location assessment.

Decision posture

Status	Meaning for CIC
Proceed	Facts, transfer mechanism, safeguards, residual risk, and approvals are complete.
Proceed with conditions	Time-limited owner approval exists with compensating controls and an expiration date.
Suspend new Restricted data	Critical facts or safeguards are missing. Existing records are preserved while the decision is resolved.
Stop	No lawful and effective mechanism or supplementary safeguard can address the transfer risk.

No blanket Proceed decision is issued by this draft.

Required approval actions

- Name the privacy/compliance owner and executive risk owner.
- Confirm the controller entity and relevant establishments.

- Export the active provider, account-region, subprocessor, and workforce-access inventory.
- Attach or attest to the current DPA and transfer mechanism for every active provider.
- Complete counsel review of the United States, Canada, UK, EEA, Nigeria, and any newly discovered destination.
- Accept or remediate remaining Medium-High and High risks.
- Approve the public report and restricted evidence index.

Publication position

This report package is suitable for transparent external review as a draft. It is not suitable to present as a completed legal approval, certification, or warranty until the approval actions are recorded.

Related material

- Full Transfer Impact Assessment (/governance/documents/transfer-impact-assessment)
- Transfer Processing Inventory (/governance/documents/transfer-processing-inventory)
- Transfer Risk Register (/governance/documents/transfer-risk-register)
- Transfer Remediation and Review Plan (/governance/documents/transfer-remediation-and-review-plan)

Limitation

This document was prepared with AI assistance and requires authorized factual confirmation and legal review. It does not itself approve a transfer.