Capital Investment Club

Risk Assessment Policy and Program

Annual and event-driven risk assessments across business, product, security, financial, and vendor domains.

Last updated: 06/07/2026

Purpose

This policy defines CIC's formal risk assessment program for identifying, evaluating, treating, and monitoring business, operational, technology, security, financial, vendor, and compliance risks.

Scope

This applies to CIC products, business processes, user data, organization data, grants, pitches, wallets, marketplace activity, support workflows, vendors, cloud infrastructure, code repositories, and internal tools.

Assessment Cadence

CIC must perform:

- Enterprise risk assessment at least annually.
- Security risk assessment at least annually.
- Vendor risk assessments before onboarding critical vendors and at least annually for critical vendors.
- Product risk assessments before launching material new platform capabilities.
- Off-cycle risk assessments after major incidents, major architecture changes, or material control failures.

Annual assessments should be scheduled, documented, approved, and retained even when no critical findings are identified. Off-cycle assessments should be linked to the triggering event, such as a production incident, security finding, new financial workflow, new vendor integration, or major data model change.

Risk Domains

Risk assessments should cover:

- Strategic risk
- Product risk
- Operational risk
- Security risk
- Privacy risk
- Financial and reconciliation risk
- Fraud risk

- Third-party risk
- Regulatory and contractual risk
- Business continuity risk
- People and access risk

Risk Assessment Method

For each risk:

1. Identify the risk. 2. Identify impacted systems, data, users, and processes. 3. Rate likelihood. 4. Rate impact. 5. Determine inherent risk. 6. Identify existing controls. 7. Determine residual risk. 8. Select treatment. 9. Assign owner. 10. Track remediation and evidence.

Risk Identification Sources

CIC should identify risks from:

- User complaints and support trends.
- Production incidents and near misses.
- Code reviews, security reviews, and UAT findings.
- Browser testing and workflow validation.
- Financial reconciliation exceptions.
- Wallet, grant, investment, assessment, and messaging defects.
- Organization context switching issues.
- Vendor security reviews.
- Vulnerability scans and dependency alerts.
- Penetration tests or independent assessments.
- Audit findings.
- Customer, partner, or API-provider diligence questions.
- Regulatory or contractual changes.

Likelihood Scale

- 1: Rare
- 2: Unlikely
- 3: Possible
- 4: Likely
- 5: Almost certain

Impact Scale

- 1: Minimal business impact
- 2: Limited operational impact
- 3: Moderate customer, financial, or operational impact
- 4: Significant customer, security, financial, or regulatory impact

- 5: Severe business, legal, customer trust, security, or financial impact

Risk Treatment

Options:

- Mitigate
- Transfer
- Avoid
- Accept

High and critical accepted risks require executive approval.

Treatment Time Objectives

Treatment timelines should be risk-based:

- Critical: immediate containment plan and target treatment within 30 days unless executive-approved exception exists.
- High: target treatment within 60 days.
- Medium: target treatment within 120 days.
- Low: monitor or address through planned improvement.

If a risk cannot be treated within the target window, the owner must document the reason, interim controls, revised date, and approval.

Residual Risk and Acceptance

Residual risk must be rated after controls are applied. Accepted high or critical residual risks require executive approval, business justification, compensating controls, expiration date, and re-review date. Accepted risk must not be used to avoid fixing defects that materially harm users, data integrity, financial integrity, privacy, or platform trust.

Required Outputs

- Risk register
- Risk assessment summary
- Risk heat map
- Treatment plan
- Accepted risk record
- Control mapping
- Remediation tracker
- Evidence links

Assessment Participants

Risk assessments should include representatives from leadership, engineering, security, product, support,

finance, operations, and any team that owns material platform workflows.

Required Assessments by Change Type

CIC should perform targeted risk review for:

- New wallet, funding, disbursement, equity, grant, or investment logic.
- New public profile, profile visibility, or user-generated content features.
- New support agent access, screen sharing, or identity verification flows.
- New organization context or permission model changes.
- New financial API, payment, banking, or KYC-adjacent provider.
- New file upload, document preview, or evidence storage feature.
- New admin tools or privileged workflows.
- New reporting, ledger, reconciliation, or PFS functionality.

Scenario Library

CIC risk assessments should consider scenarios such as:

- Unauthorized access to wallet or ledger administration.
- Incorrect equity or contribution calculations.
- Grant funding duplicated, missing, or released incorrectly.
- Organization context leakage.
- Public profile exposes incorrect or private information.
- Support agent accesses data without legitimate need.
- Vendor outage affects authentication, email, notifications, payments, or storage.
- Secrets exposed in repository or logs.
- Production deployment causes financial data inconsistency.
- KYC-adjacent workflow is bypassed or misrepresented.
- Critical user data cannot be recovered.

Control Gap Analysis

Each assessment should identify whether controls are missing, poorly designed, not operating, not evidenced, or no longer sufficient due to platform changes.

Control gaps should map to an owner, target date, and evidence requirement. Gaps that affect authorization, financial accuracy, data exposure, or production availability should be escalated even if no incident has occurred.

Reporting

Risk reports should include:

- Top risks
- Critical and high risks
- Overdue remediation

- Accepted risks
- New and closed risks
- Control gaps
- Residual risk trends

Reports should be reviewed by the executive owner or designated governance group at least quarterly. Critical risks should be reviewed until treatment is complete or formally accepted.

Risk Metrics

CIC should monitor:

- Open critical, high, medium, and low risks.
- Average age by severity.
- Overdue treatment plans.
- Accepted risks approaching expiration.
- Reopened risks.
- Risks linked to repeat incidents.
- Control gaps without evidence.
- Vendor risks pending review.
- Product launch risks not yet closed.

Quality Standard

A risk assessment is not complete unless it includes a clear risk statement, impact, likelihood, affected assets or workflows, existing controls, residual risk, owner, treatment decision, target date, and evidence location.

Evidence

Required evidence:

- Annual risk assessment
- Risk register
- Treatment plans
- Risk acceptance records
- Review meeting notes
- Remediation evidence
- Risk metrics dashboard or summary
- Off-cycle assessment records
- Control gap remediation evidence
- Executive approval for high or critical accepted risks

Review

This policy must be reviewed at least annually.