Capital Investment Club

# Security Risk Management Policy

Security risk categories, register fields, ratings, treatment, acceptance, and reporting.

Last updated: 06/07/2026

## Purpose

This policy defines how CIC identifies, assesses, mitigates, accepts, monitors, and reports security risks.

## Scope

This applies to risks affecting CIC products, APIs, infrastructure, repositories, vendors, support workflows, financial workflows, user data, organization data, marketplace activity, grants, pitches, wallets, and administrative tools.

## Risk Categories

CIC tracks security risks across:

- Unauthorized access
- Data leakage or improper disclosure
- Fraud or account abuse
- Wallet, grant, pitch, or marketplace transaction integrity
- Service availability
- Third-party/vendor dependency
- Insecure software change
- Secrets exposure
- Logging or monitoring gaps
- Incident response readiness
- Privacy or retention failure
- Misconfiguration
- Insider risk

## Risk Register

Every material risk must be recorded with:

- Risk ID
- Description
- Risk category

- Impacted systems
- Data affected
- Likelihood
- Impact
- Inherent risk rating
- Existing controls
- Residual risk rating
- Risk owner
- Treatment plan
- Target date
- Status
- Evidence
- Review date

Risks must be written in a way that identifies the threat, affected asset or workflow, potential impact, and business consequence. Vague entries such as "security issue" or "data risk" are not sufficient.

## Risk Rating

Likelihood and impact should be scored from 1 to 5.

Risk rating:

- 1-5: Low
- 6-10: Medium
- 11-15: High
- 16-25: Critical

Critical and high risks require leadership visibility and a documented treatment plan.

## Security Impact Factors

Impact scoring should consider:

- Exposure of restricted or confidential data.
- Unauthorized access to user, organization, admin, wallet, support, or financial workflows.
- Incorrect financial, equity, grant, wallet, or ledger outcomes.
- Loss of service availability.
- Compromise of secrets, credentials, or service accounts.
- Public profile or private data leakage.
- Regulatory, contractual, customer, or API-provider impact.
- Loss of audit evidence or logging.
- Incident response difficulty.
- Reputational harm.

## Risk Treatment Options

- Mitigate through controls.
- Transfer through vendor contract or insurance where appropriate.
- Avoid by discontinuing the risky activity.
- Accept with executive approval and compensating controls.

## Security Risk Sources

Security risks should be identified from:

- Incidents and near misses.
- Vulnerability findings.
- Code review findings.
- Customer or partner diligence questions.
- Vendor assessments.
- Architecture reviews.
- Penetration tests or independent assessments.
- Access reviews.
- Support and fraud trends.
- Cloud, repository, and CI/CD alerts.
- Financial or transaction anomalies.

## Security Risk Assessment Triggers

CIC must perform security risk assessment:

- At least annually.
- Before launching major new product areas.
- Before integrating critical vendors or APIs.
- After material architecture changes.
- After significant incidents.
- After major regulatory or contractual changes.
- When customer or partner diligence identifies a material gap.

Assessment is also required before deploying new support access tooling, screen sharing, file upload capabilities, public profile visibility features, financial API integrations, PFS or ledger capabilities, organization context changes, or privileged admin workflows.

## Required Control Mapping

Each high or critical risk must map to:

- Preventive controls
- Detective controls
- Corrective controls

- Control owners
- Evidence source
- Monitoring cadence

Controls should be classified as preventive, detective, corrective, or compensating. If a risk has only detective controls and no prevention or correction path, the residual risk should generally remain elevated.

## Risk Acceptance

Risk acceptance requires:

- Business justification
- Residual risk description
- Compensating controls
- Expiration or review date
- Executive approval for high or critical risks

Accepted risks must have an expiration date. On expiration, the risk must be re-rated, closed with evidence, or re-approved. Permanent acceptance of high or critical risks is not allowed.

## Remediation Standards

Security risk remediation must include:

- Clear remediation tasks.
- Owner and target date.
- Test or validation plan.
- Evidence of completion.
- Residual risk reassessment.
- Closure approval.

Critical security risks require immediate containment or compensating controls while permanent remediation is in progress.

## Monitoring

Security risks must be reviewed at least quarterly. Critical risks should be reviewed monthly until reduced.

Monitoring should use available signals such as dependency alerts, CI/CD failures, cloud alerts, repository alerts, access review findings, support reports, incident reports, vulnerability scans, browser UAT findings, and production anomaly reports.

## Reporting

Security risk reporting should include:

- Open critical and high risks
- New risks

- Closed risks
- Overdue treatment plans
- Accepted risks
- Control failures
- Audit findings
- Incident trends

## Risk Governance Meeting

CIC should hold a recurring security risk review covering:

- Open high and critical risks.
- New risks and changed ratings.
- Overdue treatment plans.
- Accepted risks approaching expiration.
- Control failures.
- Incident trends.
- Vendor risk changes.
- Product or architecture changes requiring assessment.

## Risk Closure

A risk may be closed only when the treatment plan is complete, evidence is retained, residual risk is accepted or reduced, and the risk owner approves closure.

Closure evidence must be reviewed by someone other than the person who performed the remediation for high and critical risks where practical.

## Security Risk Exceptions

Exceptions to security risk treatment timelines or control requirements must include risk owner, business justification, compensating controls, expiration date, and approver. Exceptions involving restricted data, privileged access, wallet or transaction workflows, or production secrets must be visible to leadership.

## Evidence

Required evidence:

- Security risk register
- Risk assessment records
- Risk acceptance records
- Remediation plans
- Control evidence
- Risk review meeting notes
- Risk closure validation
- Exception approvals

- Security metrics and trend summaries

## Review

This policy must be reviewed at least annually.