Capital Investment Club

Security Assurance, Audit, and Assessment Program

Internal assessments, independent reviews, evidence packages, findings, and remediation.

Last updated: 03/07/2025

Purpose

This program defines how CIC gains assurance that its security and control program is designed effectively and operating as intended.

Scope

This applies to CIC policies, controls, products, production systems, vendor relationships, access controls, security risks, financial controls, support workflows, and operational evidence.

Assurance Activities

CIC should perform:

- Internal control assessments.
- Security risk assessments.
- Access reviews.
- Vendor reviews.
- Incident response tabletop exercises.
- Disaster recovery tests.
- Vulnerability reviews.
- Independent audits or external assessments when business needs require them.

Internal Assessment Cadence

- Security program assessment: at least annually.
- Access control assessment: quarterly for privileged access.
- Vendor assessment: annually for critical vendors.
- Incident response assessment: annually.
- Disaster recovery assessment: annually.
- Policy compliance assessment: annually.

Annual Assurance Plan

CIC should maintain an annual assurance plan that identifies:

- Assessments scheduled for the year.
- Scope and systems covered.
- Control families included.
- Evidence owners.
- Expected testing method.
- Target completion date.
- External reviewer or internal reviewer.
- Prior-year findings that require follow-up.

The plan should prioritize high-risk areas such as access control, wallet and ledger integrity, financial workflow changes, security risk management, incident response, support verification, vendor dependencies, and public privacy commitments.

Independent Review

CIC should consider independent review when:

- A major customer, partner, or API provider requires it.
- CIC prepares for SOC 2, ISO 27001, or similar assurance.
- A major incident occurs.
- Leadership wants independent validation of high-risk controls.

External Audit Readiness

When preparing for an external audit or partner due diligence review, CIC should prepare:

- Current policy library and policy register.
- Current control register.
- Evidence calendar and evidence repository index.
- Risk register and most recent risk assessment.
- Incident register and postmortems.
- Vendor register and critical vendor reviews.
- Access review records.
- Change management samples.
- Financial reconciliation samples where in scope.
- Management assertion describing scope and exclusions.

Assessment Method

Assessments should evaluate:

- Policy coverage

- Control design
- Control operation
- Evidence quality
- Owner accountability
- Exception handling
- Remediation tracking
- Risk treatment effectiveness

Control Testing Methods

Assessments may use:

- Inquiry.
- Observation.
- Inspection of evidence.
- Reperformance.
- Sample testing.
- Browser workflow validation.
- API or log review.
- Configuration review.

High-risk controls should not rely only on inquiry.

Sample Selection

Where sample testing is used, the reviewer should document population, sample period, sample size, selection method, exceptions found, and conclusion. Samples should include failed, edge-case, or high-risk transactions where practical, not only clean examples.

Browser and Workflow Validation

For user-facing controls, assessments should include rendered workflow testing where practical. Examples include public profile visibility, organization context switching, grant applications, support verification, file uploads, wallet-related screens, and permission-sensitive pages.

Testing should confirm:

- The visible UI matches the policy and intended control behavior.
- Unauthorized actions are blocked.
- Disabled controls explain why the user cannot act.
- Sensitive information is not exposed in the wrong context.
- Actions produce clear confirmation or error feedback.

Findings

Findings must include:

- Finding ID
- Description
- Severity
- Affected system or process
- Root cause
- Owner
- Remediation plan
- Target date
- Status
- Closure evidence

Finding Severity

- Critical: likely material security, privacy, financial, legal, or availability impact.
- High: significant control failure or high-risk gap requiring near-term remediation.
- Medium: meaningful weakness with compensating controls or limited scope.
- Low: improvement opportunity or documentation gap.

Management Response

Each finding should include management response, remediation owner, remediation due date, interim risk treatment, and closure evidence.

Finding Lifecycle

Finding statuses should be:

- Open: finding accepted and awaiting remediation.
- In progress: owner is actively implementing remediation.
- Risk accepted: leadership approved a time-bound or permanent acceptance.
- Remediated pending validation: owner says complete and reviewer must validate.
- Closed: validation evidence confirms remediation.

Critical and high findings should be reviewed at least monthly until closed.

Closure Validation

Closure evidence should demonstrate the root cause was addressed. Acceptable closure evidence may include code changes, configuration screenshots, test results, access removal evidence, updated procedures, training records, reconciliation evidence, or user-facing browser validation.

Evidence Package

An evidence package should include:

- Approved policies

- Control register
- Evidence calendar
- Access review records
- Risk assessment records
- Vendor review records
- Incident records
- Change review samples
- Vulnerability remediation records
- Training or acknowledgement records
- Remediation tracker

Reporting

Assessment reports should summarize:

- Scope
- Method
- Controls reviewed
- Evidence reviewed
- Findings
- Remediation status
- Residual risk
- Management response

Review

This program must be reviewed at least annually.