Capital Investment Club

Security Assessment and Penetration Testing Process

Internal assessments, independent audits, independent penetration tests, remediation, retesting, and assurance evidence.

Last updated: 01/17/2026

Purpose

This process defines how CIC performs internal assessments, independent audits, and independent penetration tests to gain assurance over the security program and validate that security controls operate effectively.

Scope

This process applies to:

- CIC platform applications and APIs.
- Production infrastructure and cloud configuration.
- Financial, identity, support, and notification integrations.
- Access control and administrative workflows.
- Wallet, grant, pitch, investment, withdrawal, ledger, and reconciliation workflows.
- Governance policies, controls, evidence, and remediation.

Assessment Types

CIC may use multiple assessment types:

- Internal control assessment.
- Security risk assessment.
- Architecture review.
- Secure code review.
- Vulnerability scan.
- Configuration review.
- Tabletop exercise.
- Independent penetration test.
- Independent audit or readiness assessment.

Annual Assessment Program

CIC should perform at least one formal security program assessment annually.

The assessment should review:

- Policy coverage.
- Control design and operating effectiveness.
- Access control.
- Logging and monitoring.
- Vulnerability management.
- Incident response.
- Vendor risk.
- Change management.
- Data privacy and retention.
- Business continuity.
- Evidence quality.

Penetration Testing

CIC should perform independent penetration testing for externally exposed, high-risk, or materially changed systems.

Penetration testing scope should include, where applicable:

- Authentication and session management.
- Authorization and role boundaries.
- Organization context switching.
- Public profile visibility and privacy behavior.
- File uploads and data exports.
- Wallet, grant, pitch, investment, withdrawal, and ledger workflows.
- APIs and webhooks.
- Administrative portals.
- Common web application vulnerabilities.

Remediation

Findings must be triaged by severity, assigned to owners, and tracked to closure.

Records should include:

- Finding title.
- Severity.
- Affected asset.
- Evidence.
- Owner.
- Target date.
- Remediation plan.
- Validation evidence.

- Closure date.

Evidence

CIC should retain:

- Assessment plan.
- Test scope.
- Assessor identity or vendor.
- Report.
- Finding tracker.
- Remediation evidence.
- Retest evidence.
- Management sign-off.

Review Cadence

- Internal security assessment: at least annually.
- Independent penetration test: at least annually for high-risk external systems or after material changes where practical.
- Findings review: monthly until closure.
- Process review: annually.

Review

This process must be reviewed at least annually.