Capital Investment Club

Vulnerability Management Program

Vulnerability identification, prioritization, remediation, validation, evidence, and reporting.

Last updated: 12/14/2025

Purpose

This program defines how CIC identifies, prioritizes, remediates, validates, and reports vulnerabilities affecting applications, APIs, infrastructure, endpoints, third-party dependencies, and production integrations.

Scope

This program applies to:

- CIC web applications, APIs, notification services, landing pages, and administrative portals.
- Production infrastructure and cloud configuration.
- Open-source dependencies and third-party libraries.
- Container, runtime, operating system, and package dependencies where applicable.
- Endpoints and corporate devices.
- Financial, identity, support, messaging, monitoring, and email integrations.

Vulnerability Sources

CIC may identify vulnerabilities through:

- Dependency scanning.
- Code review.
- Static analysis.
- Dynamic testing.
- Cloud configuration review.
- Penetration testing.
- Independent audits.
- Vendor notifications.
- Security advisories.
- User or researcher reports.
- Incident investigations.

Severity Ratings

Vulnerabilities must be prioritized based on severity and exploitability.

Severity factors include:

- CVSS or provider severity.
- Exposure to the internet.
- Authentication required.
- Data sensitivity.
- Financial or transaction impact.
- Availability impact.
- Known exploitation.
- Ease of remediation.
- Compensating controls.

Remediation Targets

Target remediation timelines should be risk based.

Severity	Target
Critical	As soon as practical, with emergency handling where needed
High	Prioritized remediation in the next planned release or sooner
Medium	Scheduled remediation based on risk and exposure
Low	Remediate through routine maintenance

When remediation cannot be completed within target, CIC must document the reason, owner, compensating control, and revised date.

Dependency Management

CIC must monitor dependencies for known vulnerabilities.

Requirements:

- Keep lockfiles current.
- Review security advisories.
- Test dependency updates before deployment.
- Avoid unsupported runtime versions.
- Prioritize dependencies affecting authentication, authorization, data processing, payments, financial APIs, file upload, and admin functionality.

Validation

Remediation must be validated through:

- Re-scan.
- Test evidence.

- Code review.
- Configuration review.
- Penetration retest where applicable.
- Deployment verification for production-impacting fixes.

Evidence

CIC should retain:

- Vulnerability reports.
- Dependency scan output.
- Finding tracker.
- Risk acceptance records.
- Remediation PRs or tickets.
- Validation evidence.
- Exception approvals.

Metrics

CIC should monitor:

- Open vulnerabilities by severity.
- Aging critical and high vulnerabilities.
- Remediation time.
- Reopened findings.
- Vulnerabilities by system owner.
- Exceptions and accepted risks.

Review

This program must be reviewed at least annually and after material incidents or audit findings.