Capital Investment Club

Monitoring, Alerting, and Triage Process

Real-time detection, alert severity, triage, escalation, resolution, and evidence for production and security events.

Last updated: 02/21/2026

Purpose

This process defines how CIC detects, triages, escalates, investigates, and resolves events that may negatively impact the security, availability, privacy, financial integrity, or reliability of production assets.

Scope

This process applies to:

- Production applications and APIs.
- Infrastructure and cloud services.
- Authentication, authorization, support, identity, KYC-adjacent, and organization context workflows.
- Wallet, grant, pitch, investment, withdrawal, ledger, and reconciliation workflows.
- Vendor integrations and webhooks.
- CI/CD and deployment pipelines.
- Security alerts and suspicious behavior.

Monitoring Sources

CIC should use applicable monitoring sources, including:

- Application logs.
- API logs.
- Infrastructure metrics.
- Cloud provider events.
- CI/CD logs.
- Database and storage events.
- Authentication and access events.
- Vendor integration status.
- Security-tool alerts.
- User and support reports.

Alert Severity

Severity	Description	Example
Critical	Active or likely severe production, security, data, or financial impact	Unauthorized access, wallet imbalance, production outage
High	Material impact or likely escalation if not addressed quickly	Payment provider outage, repeated failed deployments
Medium	Degraded behavior or suspicious pattern requiring investigation	Increased API errors, unusual access-denied activity
Low	Informational or minor issue requiring review	Non-critical warning, low-volume retry failures

Triage Steps

For each material alert:

1. Confirm the alert source and time window. 2. Identify affected systems, users, organizations, data, and transactions. 3. Determine severity. 4. Assign an owner. 5. Preserve evidence. 6. Check recent deployments, configuration changes, vendor status, and related incidents. 7. Contain impact where needed. 8. Communicate internally and externally where required. 9. Resolve or mitigate the condition. 10. Document outcome and follow-up actions.

Escalation

Escalation is required when:

- Customer data may be exposed.
- Consumer financial data may be affected.
- Wallet, grant, pitch, investment, withdrawal, or ledger integrity may be affected.
- Authentication, authorization, or support access may be compromised.
- Critical production functionality is unavailable.
- Regulatory, contractual, or partner notification may be required.

Evidence

Each material alert should retain:

- Alert ID or source.
- Time detected.
- Triage owner.
- Severity.
- Impact assessment.
- Investigation notes.
- Evidence reviewed.
- Actions taken.
- Resolution time.
- Follow-up tasks.

Review Cadence

- Critical and high alerts: reviewed as they occur.
- Alert quality: quarterly.
- Monitoring coverage: quarterly.
- Triage process: annually.

Review

This process must be reviewed at least annually and after major incidents.