Capital Investment Club

Asset and Software Inventory Process

Corporate asset, production asset, software, repository, vendor software, and dependency inventory practices.

Last updated: 04/18/2026

Purpose

This process defines how CIC identifies, records, reviews, and maintains an inventory of corporate assets, production assets, cloud resources, vendor software, internally developed software, open-source dependencies, and third-party libraries.

Scope

This process applies to:

- Employee and contractor laptops.
- Cloud services, server instances, databases, storage buckets, queues, build systems, and CI/CD tooling.
- CIC repositories, deployed applications, APIs, background services, and administrative portals.
- Vendor-sourced software and SaaS tools.
- Open-source packages and third-party libraries.
- Security, support, monitoring, identity, financial, payment, and communication tools.

Process Owner

The Security/Technology owner is accountable for the inventory program. System owners, repository owners, vendor owners, and people operations must keep their assigned records current.

Asset Inventory Requirements

CIC must maintain an asset inventory for corporate and production assets connected to CIC networks or environments.

Each asset record should include:

- Asset name.
- Asset type.
- Owner.
- Environment.
- Business purpose.
- Data classification.

- Location or provider.
- Access method.
- Criticality.
- Status.
- Creation date.
- Last review date.
- Decommission date where applicable.

Production cloud resources should also include:

- Project/account/subscription.
- Region.
- Service name.
- Resource ID.
- Tags or labels.
- Public exposure status.
- Backup or recovery status.
- Monitoring coverage.

Software Inventory Requirements

CIC must maintain a software inventory covering:

- Internally developed applications and services.
- Repositories and primary maintainers.
- Runtime platforms and frameworks.
- Open-source dependencies.
- Third-party SaaS tools.
- Vendor software used for identity, payment, financial APIs, support, monitoring, and communication.
- Critical libraries that process consumer financial data or personal data.

Each software record should include:

- Software name.
- Version or package lock reference where applicable.
- Owner.
- Business purpose.
- Data processed.
- Vendor or source.
- License or contract status.
- Criticality.
- Security review status.
- Update cadence.
- Last review date.

Update Triggers

Inventory updates are required when:

- A new employee or contractor receives a device.
- A device is returned, lost, replaced, or retired.
- A new cloud resource is created.
- A production service is deployed.
- A repository is created or archived.
- A third-party vendor is onboarded or offboarded.
- A critical software dependency is added.
- A financial, identity, support, monitoring, or security integration changes.
- A material architecture change occurs.

Review Cadence

- Production asset review: quarterly.
- Corporate endpoint review: quarterly.
- Software and dependency review: quarterly.
- Vendor software review: annually, with critical vendors reviewed more frequently where required.
- Inventory process review: annually.

Evidence

CIC should retain:

- Asset inventory export or register.
- Software inventory export or register.
- Device assignment records.
- Cloud resource inventory.
- Repository inventory.
- Dependency lockfiles and vulnerability scan output.
- Vendor register.
- Review sign-off.
- Remediation records for stale, orphaned, or unauthorized assets.

Exceptions

Inventory gaps must be tracked as remediation items with an owner, target date, and compensating controls.

Review

This process must be reviewed at least annually.