Capital Investment Club

Policy and Control Governance Program

Policy lifecycle, roles, registers, exceptions, metrics, and evidence administration.

Last updated: 08/30/2024

Purpose

This program defines how CIC creates, approves, publishes, administers, monitors, and improves policies, procedures, controls, evidence, risks, and exceptions.

Scope

This applies to all CIC personnel, contractors, administrators, privileged users, support users, production systems, source code repositories, cloud services, vendors, customer-facing platform services, and internal administrative tools.

Governance Objectives

- Maintain a current, approved policy library.
- Map policies to practical procedures and controls.
- Assign ownership for every control.
- Maintain evidence that controls operate as intended.
- Identify, mitigate, and monitor business, operational, financial, privacy, technology, and security risks.
- Support customer diligence, partner diligence, production API access, and audit readiness.

Required Policy Metadata

Every policy must include:

- Policy name and ID
- Version
- Status
- Executive owner
- Operational owner
- Control owners
- Reviewers and approvers
- Effective date
- Last review date
- Next review date

- Scope
- Related systems and processes
- Related controls
- Evidence requirements
- Exception process
- Training or attestation requirements
- Change history

Lifecycle

1. Intake

Policy requests may originate from a customer requirement, partner requirement, platform risk, incident, audit finding, product launch, vendor review, legal requirement, or operational gap.

Required intake fields:

- Requester
- Business driver
- Risk driver
- Affected systems and users
- Proposed owner
- Proposed deadline
- Required approval path

2. Drafting

Policies must be written clearly enough for teams to operate them. Requirements should avoid vague language unless the control owner can produce objective evidence.

Drafting requirements:

- Define policy rules.
- Define procedures or reference separate procedure documents.
- Identify controls and evidence.
- Identify exception paths.
- Define monitoring cadence.

3. Review

At minimum, policies should be reviewed by the operational owner and impacted control owners. Security, privacy, legal, finance, engineering, support, and executive reviewers must be included when the policy affects their domains.

4. Approval

Approval must be recorded before a policy is published. High-risk policies require executive approval.

Approval record:

- Approver name
- Role
- Approval date
- Version approved
- Effective date
- Conditions or exceptions

5. Publication

Published policies must be accessible to the people expected to follow them. Superseded versions must be retained for audit history.

6. Operation

Control owners must operate assigned controls, maintain evidence, escalate failures, and remediate gaps.

7. Monitoring

Governance administrators must maintain an evidence calendar and track overdue reviews, missing evidence, exceptions, audit findings, and remediation plans.

8. Refresh

Policies must be reviewed at least annually and sooner after:

- Security incident
- Privacy incident
- Major product release
- Architecture change
- Regulatory change
- Vendor change
- Customer diligence finding
- Audit finding

Roles

Executive Owner

Owns final accountability, approves material changes, and accepts residual risk.

Operational Owner

Maintains the policy, coordinates reviews, and ensures procedures are implemented.

Control Owner

Runs controls, preserves evidence, and remediates failures.

Governance Administrator

Maintains registers, review calendar, evidence calendar, approval records, and reporting.

Independent Reviewer

Performs internal assessment or independent review to confirm the governance program is operating effectively.

Governance RACI

Activity	Executive owner	Operational owner	Control owner	Governance admin	Independent reviewer
Approve high-risk policy	Accountable	Consulted	Consulted	Informed	Informed
Draft or update policy	Informed	Accountable	Consulted	Responsible	Informed
Operate control	Informed	Accountable	Responsible	Informed	Informed
Collect evidence	Informed	Accountable	Responsible	Consulted	Informed
Review evidence quality	Informed	Consulted	Consulted	Responsible	Consulted
Approve exception	Accountable for high risk	Responsible for normal risk	Consulted	Responsible for register	Informed
Perform internal assessment	Informed	Consulted	Consulted	Responsible	Accountable when assigned
Close remediation	Informed	Accountable	Responsible	Tracks	Validates when in scope

Registers

CIC must maintain:

- Policy register
- Procedure register
- Control register
- Evidence calendar
- Risk register
- Exception register
- Vendor register
- Incident register
- Access review register
- Audit and assessment tracker
- Remediation tracker

Exception Management

Exceptions must be documented, time-bound, risk-assessed, approved, and reviewed before expiration.

Required exception fields:

- Policy or control affected
- Requester
- Business justification
- Risk rating
- Compensating controls
- Approver
- Expiration date
- Review date
- Final disposition

Metrics

Governance should report:

- Policies reviewed on time
- Controls with current evidence
- Open high-risk exceptions
- Overdue access reviews
- Open audit findings
- Open critical vendor reviews
- Open high and critical security risks
- Incidents by severity
- Training and acknowledgement completion

Monthly Governance Reporting Pack

CIC should prepare a monthly governance summary during program build-out. The report should include:

- Policy review status.
- Evidence calendar completion.
- Open high and critical risks.
- Open exceptions and upcoming expirations.
- Open incidents and remediation status.
- Access review completion.
- Financial exception summary.
- Vendor review status.
- Support verification and support quality summary.
- Audit or assessment finding status.

The report should identify owner, due date, aging, risk level, and next action for every open high-risk item.

Governance Maturity Model

CIC may use the following maturity levels to track improvement:

Level	Description
1 - Documented	Policy or control is drafted and owner is identified.
2 - Implemented	Control exists in workflow, system configuration, or procedure.
3 - Evidenced	Operation is supported by dated evidence.
4 - Tested	Control has been independently tested or re-performed.
5 - Optimized	Metrics, automation, and recurring improvement are in place.

Critical controls should target at least Level 3 during program build-out and Level 4 once CIC prepares for formal external assurance.

Policy Approval Matrix

Policy type	Minimum approver
Security, access, incident, vendor, and SDLC policies	Executive owner plus Security or Engineering owner
Financial operations policies	Executive owner plus Finance owner
Privacy, terms, data processing, and public content policies	Executive owner plus Legal or designated privacy reviewer
Support and verification policies	Operations owner plus Security owner
Low-risk procedural updates	Operational owner

Governance Operating Calendar

CIC should maintain a calendar for policy reviews, access reviews, vendor reviews, evidence collection, risk assessments, incident exercises, recovery tests, and internal assessments.

Policy Quality Standard

Policies should be rejected for publication when they:

- Do not assign an owner.
- Do not define scope.
- Do not identify related evidence.
- Use vague obligations without a measurable control.
- Conflict with published public policies or product behavior.
- Are materially inconsistent with CIC's operating model.

- Do not define exception handling.

Control Quality Standard

Controls should be designed so a reviewer can determine whether they operated. A complete control should define trigger, owner, frequency, system, population, evidence, exceptions, and remediation path.

Document Control

Every approved policy should record version, approval date, approver, effective date, review owner, next review date, and material changes. Retired versions should be retained for audit history.

Evidence

Evidence must include control name, owner, period covered, date collected, reviewer, result, exceptions, and remediation links.

Enforcement

Policy violations may result in access removal, escalation to leadership, contract review, disciplinary action, vendor review, or other corrective actions.