Capital Investment Club

# Governance Registers and Templates

Operational registers and templates for policy approval, risk, exceptions, access review, incidents, vendors, evidence, and remediation.

Last updated: 05/08/2024

## Purpose

This document defines the operational registers and templates CIC should use to administer its policy, risk, control, security, support, vendor, access, financial, and audit programs.

## Scope

These templates apply to CIC governance administration, security operations, engineering reviews, support operations, finance operations, vendor management, incident response, and audit readiness.

## Required Registers

| Register | Purpose | Owner | Minimum cadence |
|---|---|---|---|
| Policy register | Track policy ownership, approval, publication, and review status. | Governance admin | Monthly during build-out, annual after stable |
| Control register | Track control owners, frequencies, evidence, and status. | Governance admin | Quarterly |
| Risk register | Track enterprise, security, privacy, financial, vendor, and operational risks. | Security or risk owner | Quarterly and after material events |
| Exception register | Track policy or control exceptions, approvals, compensating controls, and expiry. | Governance admin | Monthly |
| Evidence calendar | Track recurring and per-event control evidence. | Governance admin | Monthly |
| Access review tracker | Track access review populations, reviewer conclusions, and removal actions. | Governance admin | Quarterly for privileged access |
| Incident register | Track security, privacy, financial, vendor, and operational incidents. | Security owner | Per incident and monthly open-item review |
| Vendor register | Track vendors, risk tier, data processed, owners, contracts, reviews, and exit plans. | Vendor owner | Annual for critical vendors |

| | | | |
|---|---|---|---|
| Remediation tracker | Track findings, risks, incidents, audit gaps, and closure evidence. | Governance admin | Monthly |
| Support quality tracker | Track sensitive support actions, verification, file requests, screen share consent, and user ratings. | Support owner | Monthly |

## Template Library

| Template | Location | Use |
|---|---|---|
| Policy Register Template | templates/policy-register-template.md | Track policy lifecycle and review. |
| Policy Approval Record Template | templates/policy-approval-record-template.md | Record approval and publication for each policy version. |
| Risk Register Template | templates/risk-register-template.md | Record risk rating, controls, treatment, and review. |
| Exception Register Template | templates/exception-register-template.md | Record approved exceptions and expiry. |
| Control Evidence Template | templates/control-evidence-template.md | Record control operation evidence and review result. |
| Access Review Template | templates/access-review-template.md | Review privileged, financial, support, repository, cloud, and admin access. |
| Incident Register Template | templates/incident-register-template.md | Record incidents from intake through closure. |
| Vendor Register Template | templates/vendor-register-template.md | Track vendor risk, data, review, and exit requirements. |
| Remediation Tracker Template | templates/remediation-tracker-template.md | Track findings and corrective action through validation. |

## Administration Rules

- Registers must identify owner, review cadence, status, and evidence location.
- High-risk items must have owner, due date, and next action.
- Closed items must include closure evidence.
- Expired exceptions must be closed, renewed, or escalated.
- Evidence must be tied to control IDs where possible.
- Sensitive evidence must be redacted or access-restricted.
- Register exports used for third-party diligence must be reviewed before sharing.

## Minimum Monthly Governance Review

The monthly review should cover:

- Overdue policy reviews.
- Missing evidence.

- Open high and critical risks.
- Open critical incidents.
- Open financial exceptions.
- Overdue access removals.
- Vendor reviews due within 60 days.
- Exceptions expiring within 30 days.
- Open audit findings.
- Support verification or screen-share exceptions.

## Audit Preparation Use

Before responding to a customer, partner, bank, API provider, or auditor diligence request, CIC should assemble:

- Current policy register.
- Current control register.
- Evidence calendar completion summary.
- Latest risk assessment and risk register.
- Latest access review evidence.
- Latest vendor review evidence for critical vendors.
- Latest incident tabletop or incident response evidence.
- Latest disaster recovery test evidence.
- Open remediation tracker.

## Review

This document should be reviewed at least annually and whenever CIC adds a new governance process or assurance requirement.