Capital Investment Club

Control Register

Baseline controls, owners, frequency, evidence, status, and governance expectations.

Last updated: 06/01/2023

Purpose

This register defines baseline controls CIC should maintain to support security, risk, privacy, operational, and audit readiness.

Control Format

Each control should include:

- Control ID
- Control name
- Control objective
- Control owner
- Frequency
- Evidence
- Related policy
- Related risk
- Status

Baseline Controls

Control ID	Control	Owner	Frequency	Evidence
CIC-AC-001	Privileged access is approved before provisioning.	System owner	Per request	Access request and approval
CIC-AC-002	Privileged access is reviewed quarterly.	Governance admin	Quarterly	Access review record
CIC-AC-003	Terminated or transferred user access is removed promptly.	Operations owner	Per event	Deprovisioning record
CIC-AC-004	Service accounts have named owners and limited permissions.	Engineering owner	Annual	Service account inventory

CIC-AC-005	Organization context switching does not expose unauthorized data.	Product owner	Per release sample	Browser test evidence
CIC-AC-006	Break-glass access is approved, time-bound, and reviewed.	Governance admin	Per event	Break-glass record
CIC-SEC-001	Security risks are tracked in a risk register.	Security owner	Quarterly	Risk register
CIC-SEC-002	Critical and high security risks have treatment plans.	Security owner	Monthly for open items	Treatment plan
CIC-SEC-003	Security incidents are recorded and reviewed.	Security owner	Per incident	Incident register
CIC-SEC-004	Incident response tabletop exercise is performed.	Security owner	Annual	Tabletop record
CIC-SEC-005	Critical assets have owners and classifications.	Security owner	Annual	Asset inventory
CIC-SEC-006	Security monitoring signals are reviewed for critical workflows.	Security owner	Monthly	Alert or monitoring review
CIC-ENG-001	Material code changes are reviewed before merge.	Engineering owner	Per change	Pull request review
CIC-ENG-002	Security-sensitive changes receive heightened review.	Engineering owner	Per change	PR notes or approval record
CIC-ENG-003	Material changes include relevant tests.	Engineering owner	Per change	Test results
CIC-ENG-004	Secrets are not committed to source code.	Engineering owner	Continuous	Secret scan or review evidence
CIC-ENG-005	Database migrations and repair scripts are reviewed and tested.	Engineering owner	Per change	Migration review and test evidence
CIC-ENG-006	User-facing changes receive browser validation when practical.	Engineering owner	Per change	Screenshot or browser evidence
CIC-VUL-001	Vulnerabilities are triaged and tracked.	Security owner	Continuous	Vulnerability tracker
CIC-VEN-001	Critical vendors are reviewed before onboarding.	Vendor owner	Per onboarding	Vendor review
CIC-VEN-002	Critical vendors are reviewed annually.	Vendor owner	Annual	Annual vendor review
CIC-VEN-003	Subprocessors are documented for customer and privacy reference.	Vendor owner	Annual	Subprocessor register

CIC-VEN-004	Vendor incidents are tracked and assessed for CIC impact.	Vendor owner	Per incident	Vendor incident record
CIC-DATA-001	Sensitive data access is restricted by business need.	Data owner	Continuous	Role matrix and access review
CIC-DATA-002	Support access is limited to legitimate support purposes.	Support owner	Continuous	Support access logs or tickets
CIC-DATA-003	Data inventory and retention schedule are maintained.	Data owner	Annual	Data inventory and retention schedule
CIC-DATA-004	New public data fields receive privacy and display review.	Privacy owner	Per change	Privacy review record
CIC-BCP-001	Critical systems have recovery expectations.	Operations owner	Annual	Critical system inventory
CIC-BCP-002	Recovery capability is tested for critical systems.	Operations owner	Annual	Recovery test evidence
CIC-BCP-003	Business impact analysis is reviewed for critical workflows.	Operations owner	Annual	BIA record
CIC-GOV-001	Policies are reviewed at least annually.	Governance admin	Annual	Policy review records
CIC-GOV-002	Exceptions are documented, approved, and time-bound.	Governance admin	Per exception	Exception register
CIC-GOV-003	Evidence calendar is reviewed monthly.	Governance admin	Monthly	Evidence calendar review
CIC-GOV-004	Control evidence is indexed and tied to control IDs.	Governance admin	Monthly	Evidence repository index
CIC-GOV-005	Policy changes are approved before publication.	Governance admin	Per policy change	Policy approval record
CIC-FIN-001	Wallet and transaction-impacting changes are reviewed carefully.	Finance owner	Per change	Change review and test evidence
CIC-FIN-002	Financial workflow exceptions are tracked to resolution.	Finance owner	Per exception	Exception or remediation record
CIC-FIN-003	Wallet and ledger balances are reconciled.	Finance owner	Monthly	Reconciliation evidence
CIC-FIN-004	Financial repair and backfill scripts are approved and idempotent.	Finance and engineering owners	Per repair	Repair approval and before-after evidence

CIC-FIN-005	Equity and ownership calculations are tested for payment accuracy.	Finance and engineering owners	Per material change	Test evidence
CIC-FIN-006	Financial reports and PFS outputs use current dynamic data.	Finance owner	Per release sample	Report validation evidence
CIC-PRV-001	Privacy requests are logged, verified, and dispositioned.	Privacy owner	Per request	Data rights request record
CIC-PRV-002	Public profile visibility is enforced as configured.	Product owner	Continuous	Test evidence and profile setting records
CIC-PRV-003	Public policies are reviewed and updated for material product changes.	Privacy or legal owner	Annual and per material change	Policy review record
CIC-SUP-001	Sensitive support actions require user verification.	Support owner	Per event	Support verification record
CIC-SUP-002	Support file requests include purpose and retention handling.	Support owner	Per request	Support ticket and file request record
CIC-SUP-003	Screen sharing requires user consent and sensitive data safeguards.	Support owner	Per event	Screen share consent record
CIC-SUP-004	Support quality and satisfaction are reviewed.	Support owner	Monthly	Support quality review
CIC-LOG-001	Security-relevant logs are retained for critical workflows.	Security owner	Continuous	Log retention configuration or evidence
CIC-CFG-001	High-risk production configuration changes are reviewed.	Engineering owner	Per change	Change record
CIC-DR-001	Critical system recovery expectations are documented.	Operations owner	Annual	BIA and recovery target record
CIC-DPA-001	Critical subprocessors are documented and reviewed.	Vendor owner	Annual	Subprocessor register

Control Status

Suggested statuses:

- Designed
- Implemented
- Operating
- Needs remediation
- Retired

Review

This register should be reviewed at least quarterly during program build-out and at least annually once mature.

Control Testing Guidance

Each control should be tested using at least one method: inquiry, inspection, observation, reperformance, configuration review, log review, or workflow testing. High-risk controls should have evidence beyond inquiry.