Capital Investment Club

Evidence Calendar

Monthly, quarterly, annual, and per-event evidence collection schedule.

Last updated: 01/15/2024

Purpose

This calendar defines recurring evidence CIC should collect to prove policies and controls are operationalized.

Monthly Evidence

Evidence	Owner	Notes
Evidence calendar review	Governance admin	Confirm missing or overdue evidence.
Open high and critical risk review	Security owner	Confirm treatment status.
Open incident and remediation review	Security owner	Confirm closure progress.
Vulnerability remediation review	Engineering owner	Confirm aging and priority.
Production deployment sample review	Engineering owner	Confirm PR, tests, and deployment traceability.
Financial exception review	Finance owner	Review duplicate, missing, stale, or failed financial postings.
Support verification sample review	Support owner	Confirm sensitive support actions were verified.
Public profile report review	Operations owner	Confirm profile reports, visibility complaints, and content issues were dispositioned.
Support queue aging review	Support owner	Confirm old tickets, escalations, and user feedback are being handled.
PFS journal and metadata sample review	Finance owner	Confirm posted journals, metadata creation, and report extraction are complete and traceable.

Quarterly Evidence

Evidence	Owner	Notes
Privileged access review	Governance admin	Review cloud, repos, production, admin tools, support tools.

Evidence	Owner	Notes
Financial operations access review	Finance owner	Review wallet, ledger, transaction, and admin permissions.
Security risk register review	Security owner	Update ratings, owners, and treatment plans.
Exception register review	Governance admin	Expire, renew, or close exceptions.
Critical vendor watch review	Vendor owner	Check material changes, incidents, and renewals.
Public profile and content report review	Operations owner	Confirm profile/content reports are dispositioned.

Annual Evidence

Evidence	Owner	Notes
Policy review	Governance admin	Review all approved policies.
Enterprise risk assessment	Executive owner	Business, operations, security, vendor, financial, compliance.
Security risk assessment	Security owner	Product, infrastructure, data, access, vendor, SDLC.
Vendor reassessment	Vendor owner	Critical vendors.
Incident response tabletop	Security owner	Include security and customer support scenarios.
Disaster recovery test	Operations owner	Validate recovery for critical systems.
Standard access review	Governance admin	Non-privileged access.
Internal control assessment	Governance admin	Evaluate design and operation of core controls.
Security awareness acknowledgement	People or Operations owner	Personnel with system access.
Cookie and tracking technology review	Privacy owner	Confirm cookie register and public policy remain accurate.
Public policy review	Privacy or Legal owner	Review Privacy Policy, Terms, Cookie Policy, and DPA summary.
Business impact analysis refresh	Operations owner	Confirm critical workflows, RTO, RPO, and workarounds remain accurate.
Personnel policy acknowledgement	People or Operations owner	Confirm personnel with access have acknowledged current policies.
Support call-back and screen-share control review	Support owner	Validate code exchange, consent, file request, and rating controls.

Per-Event Evidence

Event	Evidence
New vendor	Vendor security review, contract review, risk tier.
New policy	Intake, draft, review comments, approval, publication.
Policy exception	Risk assessment, approval, expiry date, compensating controls.
Security incident	Incident record, timeline, root cause, remediation, postmortem.
Production release	PR, review, tests, deployment record.
Privileged access request	Request, approval, grant date, removal date if temporary.
User termination	Deprovisioning evidence.
Material architecture change	Risk review and security review.
Financial repair or migration	Approval, dry run where applicable, before and after counts, affected IDs, reconciliation result.
New public data field	Privacy review, classification, public display approval, retention mapping.
New support file request type	Purpose, data classification, retention, access limitation.
New AI or automation tool	Tool review, data classification boundary, approved use cases.
External audit or due diligence request	Request scope, evidence package, response owner, final submission record.
User data rights request	Verification, systems searched, action taken, response date.

Evidence Quality Standard

Evidence should identify:

- What control operated.
- Who performed it.
- When it was performed.
- What period it covered.
- What system or process was covered.
- What result was observed.
- What exceptions were found.
- What remediation was opened.

Evidence Storage Standard

Evidence should be stored in a controlled repository or system with clear naming, date, owner, control ID, and

review period. Evidence should not be casually stored in personal drives or chat threads unless copied into the official evidence location.

Evidence Naming Standard

Recommended evidence naming:

YYYY-MM-DD_CONTROLID_PERIOD_OWNER_SHORT-DESCRIPTION

Examples:

- 2026-06-30_CIC-AC-002_Q2_GOV_PRIVILEGED-ACCESS-REVIEW
- 2026-06-30_CIC-FIN-003_JUNE_FIN_WALLET-RECONCILIATION
- 2026-06-30_CIC-SUP-001_JUNE_SUPPORT_VERIFICATION-SAMPLE

Evidence Acceptance Criteria

Evidence should be rejected or returned for correction when:

- It does not show the control period.
- It does not identify the reviewer or performer.
- It only states that a control happened without showing support.
- It is a screenshot with no context, owner, or date.
- It omits exceptions or remediation.
- It includes sensitive data that should have been redacted.

Evidence Repository Index

CIC should maintain an index that maps evidence to control ID, period, owner, storage location, reviewer, exceptions, and remediation record. The index should be reviewed monthly during program build-out.