Capital Investment Club

Vendor Risk Management Policy

Vendor tiering, onboarding diligence, contract expectations, monitoring, access, and offboarding.

Last updated: 06/07/2026

Purpose

This policy defines how CIC evaluates, approves, monitors, and offboards vendors that support CIC products, operations, security, payments, customer support, cloud infrastructure, communications, analytics, identity, or data processing.

Scope

This applies to vendors, subprocessors, SaaS tools, contractors, cloud providers, API providers, payment providers, support tools, data processors, and security tools.

Vendor Risk Tiers

Critical

Vendor supports production operations, handles sensitive data, affects availability, affects financial operations, or is difficult to replace quickly.

Examples may include cloud hosting, authentication, payment or financial APIs, email and notification infrastructure, database or storage providers, support tooling with user data access, monitoring/logging platforms, and security tooling.

High

Vendor handles sensitive data or supports important business processes but has limited production impact.

Examples may include analytics providers, document processing tools, communications vendors, customer support tools, KYC-adjacent providers, and development tools with repository or production metadata access.

Medium

Vendor handles limited business data or supports non-critical operations.

Low

Vendor has no sensitive data access and minimal operational impact.

Inherent Risk Factors

Vendor risk tiering must consider:

- Type and sensitivity of data processed.
- Whether the vendor can access production systems.
- Whether the vendor supports financial, wallet, grant, pitch, marketplace, KYC-adjacent, messaging, support, or identity workflows.
- Availability impact if the vendor fails.
- Subprocessor complexity.
- Contractual leverage and termination rights.
- Data residency or cross-border transfer implications.
- Security assurance available.
- Concentration risk and replacement difficulty.
- Regulatory, audit, or customer diligence impact.

Onboarding Requirements

Before onboarding critical or high-risk vendors, CIC must review:

- Business purpose
- Data accessed or processed
- Security controls
- Privacy and data processing terms
- Availability and business continuity posture
- Breach notification terms
- Subprocessor posture where applicable
- Access model
- Contract owner
- Exit plan

The review must be completed before the vendor receives production data, production credentials, administrative access, or repository access. Exceptions require documented approval, compensating controls, and an expiration date.

Due Diligence Materials

Request where appropriate:

- SOC 2 report or equivalent assurance
- Information security policy summary
- Data protection documentation
- Penetration test summary or security assessment
- Business continuity documentation
- Incident response documentation

- Privacy policy and DPA
- Security questionnaire

If a vendor cannot provide standard assurance material, CIC should document alternate evidence such as public security documentation, architecture review, contractual commitments, limited data access, compensating controls, or a decision not to onboard the vendor.

Vendor Register Fields

The vendor register should track:

- Vendor name.
- Business owner.
- Service provided.
- Data processed.
- Risk tier.
- Contract status.
- DPA status.
- Security review status.
- Subprocessor status.
- Access granted.
- Renewal date.
- Last review date.
- Next review date.
- Exit plan.

Contract Requirements

Critical and high-risk vendor contracts should address:

- Confidentiality
- Data protection
- Security obligations
- Breach notification
- Subprocessors
- Audit rights where feasible
- Service levels where applicable
- Data return or deletion
- Termination rights

Critical vendor contracts should also address regulatory cooperation where applicable, audit or assurance support, incident cooperation, data location, encryption expectations, support response, service continuity, subcontractor controls, and clear ownership of customer data.

Approval Requirements

Vendor approval should follow this baseline:

- Low risk: business owner approval and register entry.
- Medium risk: business owner plus governance/security review.
- High risk: business owner, security/privacy review, and contract review.
- Critical risk: executive owner approval, security/privacy review, contract review, and documented exit or continuity plan.

Security, privacy, or legal review may require additional controls before approval.

Monitoring

Critical vendors must be reviewed at least annually. High-risk vendors should be reviewed annually or based on risk. Medium and low-risk vendors may be reviewed on a risk-based cadence.

Monitoring should include review of contract renewal dates, security reports, incident history, subprocessor changes, access granted to the vendor, product or integration changes, support performance, and whether the vendor remains necessary.

Vendor Incident Handling

Vendor incidents must be evaluated for data impact, service impact, customer impact, legal notification, contractual notification, and operational workaround. Critical vendor incidents should be tracked in the incident register when they materially affect CIC.

Vendor incident review should record:

- Date CIC became aware.
- Vendor notice and incident summary.
- Data or services affected.
- CIC users, organizations, or workflows affected.
- Immediate containment or workaround.
- Required customer, regulator, or partner notification.
- Corrective actions.
- Closure evidence.

Concentration and Exit Risk

CIC should evaluate whether it depends too heavily on a single vendor for authentication, hosting, payments, messaging, notifications, storage, or support. Critical vendors should have an exit or contingency plan appropriate to their risk.

Vendor Access

Vendor access must follow CIC access control requirements:

- Approved business need
- Least privilege

- Named owner
- Time-bound when possible
- Reviewed periodically
- Removed promptly when no longer needed

Offboarding

Vendor offboarding must include:

- Access removal
- Data return or deletion confirmation where applicable
- Contract closure
- Replacement or continuity plan
- Final evidence record

Restricted Vendor Uses

CIC must not use vendors for sensitive workflows unless the vendor is approved for that purpose. Restricted workflows include wallet or transaction processing, KYC-adjacent evidence, authentication, support identity verification, production database access, private messages, user uploads, public profile verification evidence, and administrative security logs.

Vendor Access Review

Vendor access must be reviewed at least quarterly for critical vendors and at least annually for high-risk vendors. Reviews should verify named accounts, API keys, service accounts, shared inboxes, support console access, repository access, and production configuration access.

Vendor Data Inventory

For each critical or high-risk vendor, CIC should document:

- Data elements processed.
- Data classification.
- Data source.
- Processing purpose.
- Retention period.
- Deletion or return mechanism.
- Whether data is encrypted in transit and at rest.
- Whether the vendor can access the data directly or only process it as a service.

Exceptions

Vendor policy exceptions require documented business justification, risk owner, compensating controls, approval, expiration date, and review cadence. Critical vendor exceptions must be visible to leadership.

Evidence

Required evidence:

- Vendor register
- Risk tier
- Security review
- Contract review
- Access approvals
- Annual review records
- Offboarding records
- Vendor access review evidence
- Vendor incident records
- Subprocessor review records
- Exception approvals
- Data deletion or return confirmations

Review

This policy must be reviewed at least annually.