OPERATING GUIDE

Managing Vendors in a Modular Credit Union Technology Stack

Accountability, selection, review and AI-vendor oversight for credit unions that buy and partner rather than build

Roger Estrada · Process Excellence and PMO Executive · October 2026

---

1. Position

A credit union with a modular technology stack delivers member outcomes through vendors it does not control. Regulators, members and the board hold the credit union accountable for those outcomes anyway. Vendor management is the operating system that closes that gap: it decides who gets in, on what terms, who is accountable once they are in, and when they leave.

This guide sets out one operating model for that system. It converts a three-step sourcing process (RFI, RFP, RFQ) into a seven-stage lifecycle with named owners and control gates, scales oversight to vendor criticality, and extends the model to AI and automation vendors, where model behavior, data use and change control add risk that traditional vendor reviews do not cover.

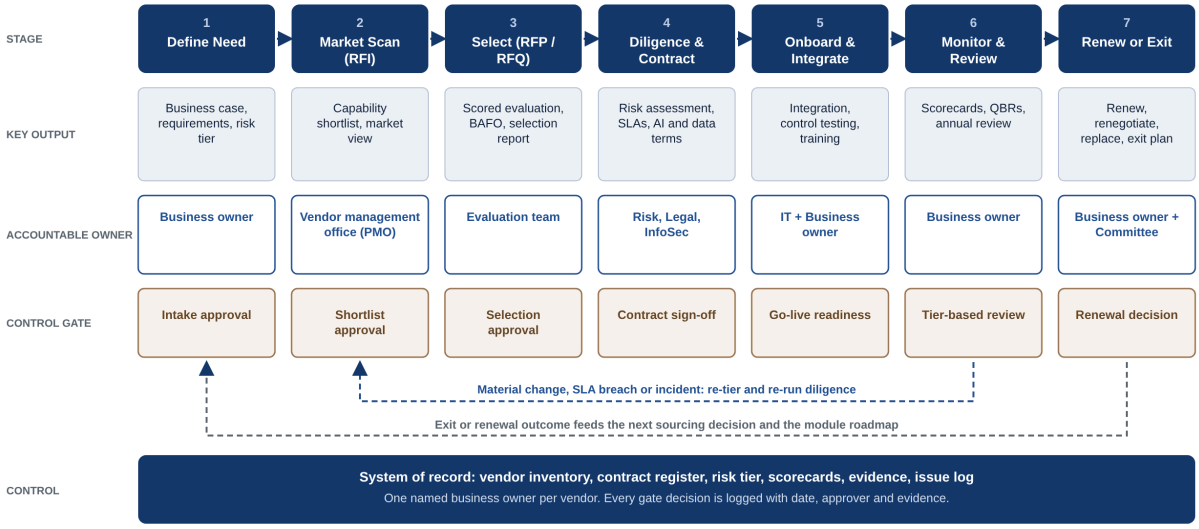
Operating principles

- **The vendor delivers; the credit union owns the outcome.** Every vendor has one named business owner accountable for results, spend and risk.
- **Tier drives oversight, not the buy decision.** Due diligence depth and review frequency follow criticality, data sensitivity and member impact.
- **Modules are replaceable by design.** Open interfaces, data portability and tested exit plans are contract requirements, not afterthoughts.
- **Independent challenge is built in.** Risk, compliance, legal and information security approve at defined gates; they do not rubber-stamp after the fact.
- **One system of record.** Inventory, contracts, tiers, scorecards, evidence and issues live in one place. No gate decision exists unless it is logged.

2. The Vendor Lifecycle

Figure 1 shows the seven stages. Each stage has a required output, one accountable owner and a gate that must be passed before the next stage starts. Two feedback loops keep the model live: material change or incident triggers re-tiering and renewed diligence, and every renewal or exit decision feeds the next sourcing decision.

Figure 1. Vendor lifecycle with accountable owners and control gates



Selecting the right sourcing path (Stages 2 and 3)

Instrument	Use when	Output
RFI	The market is unknown or the need is not fully defined. Used to learn what exists and who serves credit unions.	Capability shortlist and a go or no-go on proceeding to RFP
RFP	The need is defined and several vendors must be compared on solution, regulatory fit, technical alignment, risk and price.	Scored evaluation, reference checks, financial diligence, best-and-final offer, selection report
RFQ	The need and vendor are known: pricing for a defined scope, or an add-on to an existing agreement.	Itemized price and terms against fixed specifications

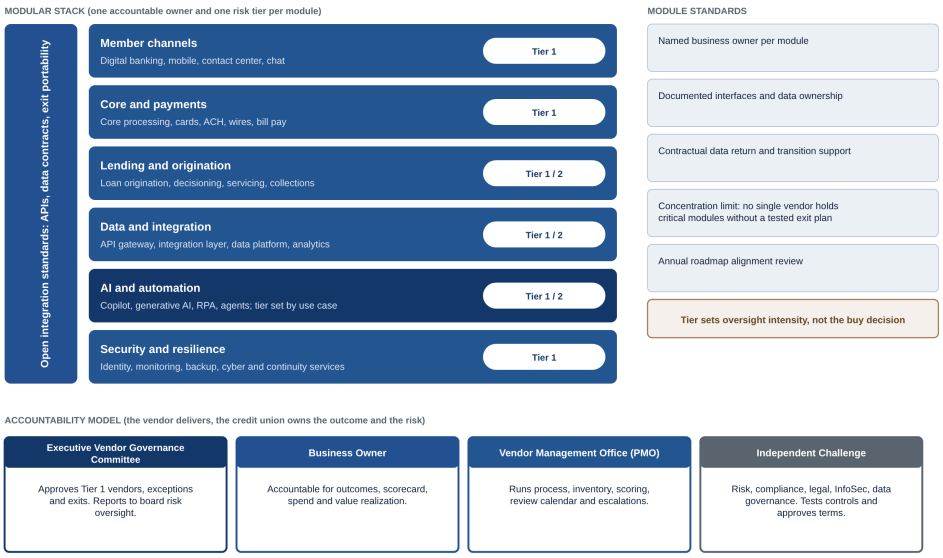
Selection standards

- **Sign an NDA before sharing any member, system or security information.**
- **Route all vendor questions through the vendor management office.** Log every question and answer, and distribute answers to all participating vendors at the same time.
- **Score every vendor against one pre-approved rubric,** with evaluators scoring independently before any consensus session.
- **Verify before you trust.** Complete reference checks, financial stability review, market reputation review and a roadmap viability assessment on every finalist.
- **Require evidence, not assertions.** Current SOC 2 Type II or equivalent, penetration test summary, business continuity test results, insurance certificates and regulatory exam history where available.
- **Document the decision.** A selection report with scoring, rationale, risk acceptance and approvals is the audit trail and the basis for contract negotiation.

3. Vendor Management in a Modular Stack

Credit unions that have moved away from single-vendor stacks assemble best-of-breed modules (channels, core and payments, lending, data and integration, AI and automation, security) around an open integration layer, often with partners and credit union service organizations (CUSOs) supplying parts of the stack. The benefits are speed, choice and leverage. The cost is more relationships, more interfaces and more places for accountability to blur. Figure 2 shows how the model keeps ownership clear.

Figure 2. Modular technology stack and vendor accountability model



Module rules

- **One owner per module.** A single business owner is accountable for each module's outcomes, even when several vendors contribute to it.
- **Own the interfaces.** Document APIs, data flows and data ownership. The credit union, not the vendor, holds the data dictionary and integration standards.
- **Contract for exit on day one.** Data return in usable formats, transition assistance, escrow where warranted, and a tested exit plan for every Tier 1 vendor.
- **Manage concentration.** Track how many critical functions depend on one vendor or one shared subcontractor, and set a limit that triggers a mitigation plan.
- **Review the roadmap annually.** Confirm each vendor's product direction still fits the credit union's strategy and the architecture target state.

Risk tiers

Tier	Criteria	Diligence at onboarding	Review cadence
Tier 1	Critical to member service or operations; handles sensitive member data; hard to replace; regulatory impact	Full: financial, security, compliance, resilience, subcontractors, on-site or virtual assessment, exit plan	Quarterly business review; annual full reassessment; continuous monitoring of incidents and SOC exceptions

Tier	Criteria	Diligence at onboarding	Review cadence
Tier 2	Important but substitutable; limited sensitive data	Standard: questionnaire, SOC report, references, contract review	Semi-annual performance review; annual risk refresh
Tier 3	Low impact; no member or sensitive data	Light: attestation and contract terms	Review at renewal

4. Accountability Model

Accountability is assigned by decision, not by department. The matrix below shows who is accountable (A), responsible (R), consulted (C) or informed (I) for each lifecycle activity. Each row has exactly one A.

Activity	Business owner	VMO (PMO)	AI and Auto.	IT and InfoSec	Risk and Legal	Committee
Define need and assign tier	A	R	C	C	C	I
Run RFI, RFP or RFQ	C	A	R	C	C	I
Due diligence and risk assessment	C	R	C	R	A	I
Contract, SLAs and data terms	C	R	C	C	A	I
Onboarding and integration	A	R	R	R	C	I
Performance scorecard	A	R	C	C	I	I
Periodic review and re-tiering	R	R	C	C	A	I
Renewal, remediation or exit	R	R	C	C	C	A

The AI and automation function acts as subject matter expert and governance partner on technology evaluation: it provides technical guidance, coordinates vendors and enforces AI standards, while the business owner remains accountable for the outcome the vendor delivers.

5. Vendor Review and Performance

Reviews are scheduled by tier and triggered by events. Each review uses the same scorecard so vendors can be compared across modules and over time.

Scorecard dimension	Weight	Evidence
Service performance	30%	SLA attainment, ticket aging, availability, delivery against milestones

Scorecard dimension	Weight	Evidence
Risk and compliance	25%	Audit and SOC results, open findings, regulatory changes absorbed, incident handling
Security and data protection	15%	Control test results, access reviews, subcontractor changes, breach history
Financial health	15%	Financial statements, ownership changes, concentration of the vendor's own revenue
Strategic fit and roadmap	15%	Roadmap delivery, product direction, member experience impact, value realized against the business case

Weights are a starting point; adjust by module and record the change.

Review triggers and escalation

- **Event triggers:** security incident, SLA breach in two consecutive periods, adverse audit finding, vendor merger or acquisition, change of key subcontractor, material model or product change, regulatory change.
- **Escalation path:** business owner and vendor account lead, then vendor management office and independent challenge, then governance committee. Each step carries a time limit and a required remediation plan with dates.
- **Outcomes:** continue, continue with remediation, restrict scope, re-bid, or exit. The decision, owner and date are logged.

6. AI and Automation Vendors

AI vendors follow the same lifecycle with additional controls, because the product can change behavior without a software release, and member or team member data can flow into models. Two delivery models need different handling: buy (the credit union configures and operates a vendor product) and partner-deliver (the vendor builds, hosts or runs the capability for the credit union). Partner-deliver carries more risk transfer questions and needs stronger contract terms and monitoring.

Additional diligence and contract requirements

- **Data use.** No training on credit union or member data without written approval. Define retention, deletion, residency and subprocessor disclosure.
- **Transparency.** Documented model purpose, limitations, data sources and testing. Explainability sufficient for the decision it supports.
- **Testing and monitoring.** Pre-deployment testing for accuracy, bias and security (including prompt injection for generative AI), with agreed performance thresholds and ongoing monitoring.
- **Human oversight.** Defined points where a person reviews or can override output, especially for member-affecting decisions.

- **Change control.** Advance notice of material model, version or data changes, with the right to re-test before adoption.
- **Incident and exit.** Notification windows aligned to the credit union's incident response and regulatory reporting duties; documented model, data and prompt portability on exit.
- **Approved platform use.** Enterprise assistants and generative AI tools are used under enterprise terms only, with an approved-use policy and monitoring for unapproved tools.

Alignment to the NIST AI Risk Management Framework

Function	Vendor management control	Evidence
Govern	AI vendor policy, tiering, named owners, approval gates, committee oversight	Policy, inventory, gate log, committee minutes
Map	Use-case intake, data and impact mapping, vendor role defined (buy or partner-deliver)	Intake record, data flow map, risk tier
Measure	Testing for accuracy, bias, security and drift; scorecard metrics	Test reports, scorecards, monitoring dashboards
Manage	Change control, incident response, remediation, re-tiering, exit	Issue log, incident records, exit plans

7. Regulatory Anchors

Examiners expect a vendor management policy covering planning, due diligence and ongoing controls, applied in proportion to risk. Core references: NCUA Letters to Credit Unions 07-CU-13 (Evaluating Third Party Relationships), 08-CU-09 (Evaluating Third Party Relationships Questionnaire) and 01-CU-20 (Due Diligence Over Third Party Service Providers); NCUA 12 CFR Part 748 (security program and cyber incident reporting); GLBA safeguards requirements; the NIST AI Risk Management Framework and its generative AI profile; and model risk management principles for any vendor model used in decisioning. Confirm current guidance with compliance and legal before adopting this model.

8. Program KPIs

Measure	Target	Why it matters
Vendors with current tier and named owner	100%	Accountability exists for every relationship
Tier 1 and 2 reviews completed on schedule	95% or higher	Oversight is operating, not documented only
Open high-risk findings past due	0	Remediation discipline
Contracts renewed without prior review	0	No automatic renewals without a decision
Weighted SLA attainment, Tier 1	Per contract	Service delivered to members and staff
Spend versus contract and business case	Within 5%	Cost control and value realization
Tier 1 vendors with a tested exit plan	100%	Replaceability of modules

9. Standing the Program Up: First 90 Days

Window	Actions
Days 1-30	Build the vendor inventory; assign a business owner and provisional tier to every vendor; stand up the system of record; adopt the lifecycle gates and RACI; freeze auto-renewals on Tier 1 contracts pending review.
Days 31-60	Complete diligence refresh on Tier 1 vendors; publish the scorecard and review calendar; add AI and data terms to the contract template; run the first quarterly reviews; charter the governance committee.
Days 61-90	Test two Tier 1 exit plans; report first KPI set to executive leadership; close gaps found in diligence; embed AI-vendor intake into the use-case prioritization process; set the roadmap review for the next planning cycle.