AI Governance Checklist for Credit Unions

A high-level checklist aligned to the NIST AI Risk Management Framework

Roger Estrada · AI Governance · AI Strategy · 2026

NCUA treats its rules as technology-neutral and applies them to AI, and examiners benchmark AI programs against frameworks such as NIST. Organize the work under the four NIST functions, then complete the credit-union-specific items. Mark each line Done, Partial or Not started, and keep evidence for every Done.

1. GOVERN: Accountability, Policy and Culture

Done	Action	Lead
☐	Appoint an executive sponsor and charter an AI governance council (compliance, risk, legal or privacy, IT and security, operations, HR, business lead)	CEO
☐	Brief the board and supervisory committee in plain language; set an AI risk appetite	CEO / Board
☐	Adopt an AI governance policy and an acceptable-use standard covering ChatGPT, Claude, Gemini and similar tools	Sponsor
☐	Add AI addenda to existing policies: information security, vendor management, data classification, records retention, incident response, fair lending	Policy owners
☐	Name business purpose, control design, technical environment and re-review owners for every material system	Sponsor
☐	Set decision rights: who approves each tier, grants exceptions and can stop a system	Council
☐	Launch role-based training and a no-blame route for reporting AI concerns	HR / Compliance
☐	Assign an owner to track regulatory and examiner expectations, including state rules for state charters	Compliance

2. MAP: Know and Classify Your AI

Done	Action	Lead
☐	Build an AI inventory: internal builds, vendor-embedded features (core, digital banking, lending, fraud, contact center), CUSOs, employee-adopted tools, automations and bots	IT / AI lead
☐	Assign a risk tier and an authority level (inform, recommend, prepare, execute with approval, execute within limits) to each system	Risk
☐	Use one intake and assessment form for every request; document purpose, member benefit, data, systems touched and where a person reviews	AI lead
☐	Fix the workflow before automating it; define decision rules and human checkpoints	Business owner

Done	Action	Lead
☐	Assess impact on members and employees, including fair lending and complaint exposure	Compliance
☐	Map data sources and permitted purposes; classify data allowed in each tool type	Data governance
☐	Map dependencies on models, vendors and subprocessors for each material system	IT / Vendor mgmt

3. MEASURE: Test and Monitor

Done	Action	Lead
☐	Define metrics before launch: accuracy, bias, security, adoption, member outcomes, value	AI lead / Risk
☐	Test high-tier systems for validity, security, privacy, explainability and disparate impact	Risk / Compliance
☐	Confirm specific adverse-action reasons can be produced for any system touching credit decisions	Compliance
☐	Red-team high-risk systems for prompt injection, data leakage and excess permissions	Security
☐	Monitor overrides, exceptions, permission changes, vendor changes and drift; compare production to the approved record	System owners
☐	Sample human review quality to confirm review is substantive	Risk
☐	Have the supervisory committee or internal audit test whether AI controls operate as described	Audit

4. MANAGE: Treat Risk and Respond

Done	Action	Lead
☐	Keep one AI risk register with a named risk acceptor for each residual risk	Risk
☐	Set re-approval triggers: new model or vendor release, expanded data or permissions, move to a higher authority level, unapproved new use	Council
☐	Apply least privilege, transaction limits and a tested stop procedure to any AI that acts	Security
☐	Define an AI incident plan: containment, member and regulator notification, recovery, post-incident review; run an exercise yearly	Security / Risk
☐	Document and test a manual fallback for each material system	Operations
☐	Review realized value per use case and stop funding what does not deliver	Sponsor
☐	Report to the board each quarter: inventory, tiers, incidents, trigger events, value	Sponsor

5. Credit Union Essentials

Done	Action	Lead
☐	Member value. Require a member-benefit statement for each use case; keep an easy route to a person	CEO / Business
☐	Vendors and CUSOs. Request AI feature, model and subprocessor lists from every core, digital, lending, fraud and contact-center vendor; add AI terms at renewal	Vendor mgmt
☐	Technology service providers. Perform and record your own due diligence, since NCUA cannot examine them; collect SOC reports and AI disclosures	Vendor mgmt / Security
☐	Fair and responsible lending. Test outcomes by group, keep human override in thin-file, small-dollar and small-business underwriting	Lending / Compliance
☐	Member data. Keep the information security program current (NCUA Part 748), enforce GLBA privacy, block member or loan data from consumer AI accounts	Security / Privacy
☐	LLM assistants. Approve enterprise tenants only; publish a data-class matrix; disable connectors by default; require review before member-facing use	CIO / CISO
☐	BSA/AML. Keep human determination on suspicious activity; keep SAR and restricted material out of AI tools	BSA Officer
☐	Board and supervisory committee. Put AI in the committee's audit scope; use outside assurance where internal skill is thin	Supervisory committee
☐	Shared resources. Use leagues, CUSOs and peers for templates, assessments and shared vendor reviews	AI lead
☐	Mergers. Add AI and data-flow inventory to integration due diligence	Integration lead

First 90 Days

1. Appoint the sponsor, charter the council and brief the board.
2. Start the inventory and publish interim LLM assistant rules.
3. Tier every material system and name its owners.
4. Adopt the governance policy and acceptable-use standard.
5. Add AI questions to vendor reviews and contracts, starting with core and lending vendors.
6. Set permission limits, re-approval triggers and the incident route.

Beyond 90 Days

Months 4-6: make it examination-ready

Done	Action	Lead
☐	Complete the NIST AI RMF gap assessment and build an evidence index organized the way examiners benchmark AI (NIST, COSO, CISA, Treasury and FinCEN materials)	AI lead / Compliance
☐	Finish AI feature, model and subprocessor lists for every core, digital, lending, fraud and contact-center vendor and CUSO; record your own due-diligence conclusion on each	Vendor mgmt

Done	Action	Lead
☐	Test AI used in underwriting, pricing and marketing for fair lending; confirm adverse-action reasons; keep human override for thin-file, small-dollar and small-business credit	Compliance / Lending
☐	Brief the board and supervisory committee on first results; agree AI scope in the supervisory committee's audit plan	Sponsor
☐	Train member-facing staff on AI disclosure and routing to a person; publish member-facing AI language	Member services / HR

Months 7-12: prove it to the board and the supervisory committee

Done	Action	Lead
☐	Have the supervisory committee or outside auditor test AI controls; report results to the board	Supervisory committee
☐	Run an AI incident exercise that includes member and regulator notification and the involvement of core vendors and CUSOs	Security / Risk
☐	Review member impact for each member-facing system: complaints, service recovery, access to a person, outcomes by group	Business owners / Compliance
☐	Measure value in member terms (resolution time, access to credit, financial health) as well as cost	Sponsor
☐	Confirm the information security program (Part 748) and GLBA privacy cover AI data flows; test LLM assistant rules, including consumer-account blocks and connector approvals	CISO / Privacy

Each year

Done	Action	Lead
☐	Refresh the evidence index, policy approvals and inventory before each examination; track NCUA AI resources and state regulator expectations	Compliance
☐	Reassess core, digital and lending vendors and CUSOs on material AI releases; add AI terms at renewal	Vendor mgmt
☐	Re-approve high-tier and critical systems; retire those that no longer serve members or meet criteria	Council
☐	Share assessments and templates with peers through the league and CUSOs; adopt what works	AI lead
☐	Add AI and data-flow review to any merger or core conversion; refresh board and supervisory committee education	Integration lead / Sponsor

Governance is set up properly when every trigger event produces a recorded re-review decision, the board sees AI reporting every quarter, and the supervisory committee or an outside auditor tests the controls at least yearly.