AI Governance Readiness Checklist

Self-Assessment for Community Financial Institutions

For Bank & Credit Union Leadership Teams
PentEdge LLC — AI with Guardrails™
Confidential — 2026

How to Use This Checklist

Work through each section with your compliance, operations, and IT teams. Check items your institution can answer with confidence. Gaps represent areas where AIMS™ — or a focused remediation effort — can close the exposure before your next examination.

This checklist maps directly to the AI oversight expectations regulators are beginning to articulate. It is not a substitute for legal or compliance counsel, but it gives your leadership team a practical starting point.

SECTION 1

AI Inventory & Visibility

Before you can govern AI, you need to know what's in use. Most institutions are surprised by what they find.

Complete AI inventory exists	You have a documented list of every AI tool in use across all departments — approved and unapproved.
Shadow AI identified	You have assessed whether employees are using AI tools not sanctioned by IT or compliance.
Tool ownership assigned	Each AI tool in use has an assigned business owner responsible for governance.
Use cases documented	You can describe what each AI tool is used for, by whom, and in what business process.
Customer-facing tools flagged	Tools that directly influence customer interactions or decisions are separately identified and tracked.
Vendor identity confirmed	For each AI tool, you know the vendor, the underlying model, and whether a third party is involved in data processing.

SECTION 2

Risk Assessment

Regulators expect you to know not just what AI tools exist, but what risks they carry and how those risks are controlled.

Risk framework defined	You have a documented framework for assessing AI tool risk — not just cybersecurity risk, but model risk, fair lending risk, and regulatory exposure.
Inherent risk scored	Each AI tool has a baseline risk score that reflects its potential impact before controls are applied.
Controls assessed	You have evaluated the effectiveness of controls in place for each tool: policies, human oversight, monitoring, vendor due diligence, training, and audit.
Residual risk documented	A final risk rating (Low / Medium / High / Critical) exists for each active tool after controls are factored in.
High-risk tools escalated	Tools rated High or Critical have been reviewed at the appropriate leadership level and have a documented remediation or acceptance decision.
Review cadence set	High-risk tools are reviewed at least quarterly. Medium-risk semi-annually. Low-risk annually.

SECTION 3

Vendor & Third-Party Management

AI tools from third-party vendors carry the same third-party risk management obligations as any other vendor relationship.

Vendor contracts reviewed	You have reviewed vendor agreements for data handling provisions, model change notification requirements, and liability.
DHA executed	A Data Handling Agreement is in place for each AI vendor that processes or accesses your data.
NDA in place	Non-Disclosure Agreements are executed with all AI vendors with access to non-public information.
VDD completed	Vendor due diligence documentation is on file and current for each active AI vendor.
Model change tracking	You have a process to receive and respond to vendor notifications about model updates or changes to AI behavior.
Concentration risk assessed	You have considered what happens if a key AI vendor becomes unavailable or changes their terms.

SECTION 4

Documentation & Audit Readiness

When examiners ask about your AI governance posture, documentation is the proof. Can you produce it on demand?

Governance policy exists	Your institution has a written AI governance or acceptable use policy approved by the board or senior leadership.
Board awareness documented	The board has been briefed on AI tool usage and risks. That briefing is documented.
Decision audit trail exists	For every governance decision made about an AI tool, there is a record of who decided, when, and why.
Examiner-ready reports available	You can produce a complete AI inventory with risk scores, compliance status, and governance history within 24 hours of a request.
Incident response defined	You have a process for responding to AI-related incidents: data exfiltration, biased output, model failure, or unauthorized use.
Historical record retained	Governance records are retained in accordance with your document retention policy and regulatory requirements.

SECTION 5

Fair Lending & Consumer Protection

AI tools used in or near credit decisioning carry heightened regulatory exposure. These items deserve particular attention.

Credit-related tools identified	You have identified every AI tool that touches credit decisioning, underwriting, pricing, or collections.
Fair lending risk assessed	Each credit-related AI tool has been assessed for disparate impact and fair lending exposure.
Model validation in progress	Credit-related AI tools are subject to model validation consistent with SR 11-7 expectations.

☐	**ECOA / FHA compliance reviewed**	Legal counsel has reviewed AI-assisted credit tools for compliance with Equal Credit Opportunity Act and Fair Housing Act requirements.
☐	**Adverse action process reviewed**	If AI tools influence adverse action decisions, your adverse action notice process has been reviewed for compliance.

SECTION 6

Team Readiness & Training

Governance frameworks only work if the people responsible for them understand what's expected.

☐	**Governance ownership assigned**	A named individual or team owns AI governance at your institution — and has the authority and resources to act.
☐	**Staff training completed**	Employees who use AI tools have received training on acceptable use, data handling, and escalation procedures.
☐	**IT team briefed**	Your IT team understands the approved AI tools, the data sources they access, and the monitoring obligations.
☐	**Compliance team engaged**	Your compliance team has reviewed AI governance processes and has a role in ongoing oversight.
☐	**Escalation path clear**	Everyone who works with AI tools knows how to escalate a concern or report an issue.

Interpreting Your Results

Checked Items	What It Means	Recommended Next Step
28–32	Strong foundation. Governance is documented and active.	Focus on continuous monitoring and examiner-readiness automation.
18–27	Partial governance. Some key areas covered, gaps remain.	Prioritize the unchecked items. Consider AIMS™ to close gaps systematically.
10–17	Emerging governance. Significant exposure in multiple areas.	Schedule a risk assessment with PentEdge before your next examination cycle.

Under 10	Limited governance. Examination risk is elevated.	Contact PentEdge. AIMS™ implementation can establish governance in 90 days.

Ready to close the gaps?

AIMS™ addresses every section of this checklist systematically — inventory, risk scoring, vendor tracking, audit trail, and examiner-ready documentation — in a single platform built for community financial institutions.

Schedule a demo: lisa@thepentedge.com • thepentedge.com