AI Regulatory Compliance Checklist

For Credit Unions Implementing AI Technologies

Regulatory Landscape Overview

As noted by NCUA (July 2025 Board Briefing): *"Regulators encourage use of technology when done in a safe and sound manner. Compliance with existing regulations, adherence to prudent risk management practices, and conducting third-party due diligence [remain essential]."*

Source: NCUA Board Briefing on Artificial Intelligence, July 24, 2025

NCUA Expectations for AI Use

Requirement	Status
AI governance policies and procedures documented	☐ Yes ☐ No ☐ N/A
Board/senior management oversight of AI initiatives	☐ Yes ☐ No ☐ N/A
Risk assessment conducted for AI implementations	☐ Yes ☐ No ☐ N/A
Third-party AI vendor due diligence completed	☐ Yes ☐ No ☐ N/A
Model risk management program addresses AI models	☐ Yes ☐ No ☐ N/A
Employee AI usage policies and training in place	☐ Yes ☐ No ☐ N/A
Incident response plan covers AI-related events	☐ Yes ☐ No ☐ N/A

> **GAO Finding (May 2025):** GAO Report #25-107197 indicates that lack of model risk management guidance may lead to inadequate oversight of credit unions' AI model use. GAO recommended NCUA update its model risk management guidance to encompass a broader variety of models.

GLBA & Privacy Requirements

Requirement	Status
Member data used in AI systems is properly classified	☐ Yes ☐ No ☐ N/A
Privacy notices disclose AI usage where applicable	☐ Yes ☐ No ☐ N/A
Member consent obtained for AI processing (where required)	☐ Yes ☐ No ☐ N/A
Data minimization principles applied to AI inputs	☐ Yes ☐ No ☐ N/A
AI vendor contracts include GLBA safeguards requirements	☐ Yes ☐ No ☐ N/A
No member NPI shared with consumer AI tools (ChatGPT, etc.)	☐ Yes ☐ No ☐ N/A

Third-Party AI Vendor Management

Per NCUA guidance and GAO findings, credit unions face distinct challenges managing AI service providers. Current regulatory limitations prevent NCUA from examining technology service providers directly.

Due Diligence Requirement	Status
AI vendor security assessment (SOC 2, penetration testing)	☐ Yes ☐ No ☐ N/A
Data handling practices reviewed (encryption, retention)	☐ Yes ☐ No ☐ N/A
Contract includes right to audit AI provider	☐ Yes ☐ No ☐ N/A
Business continuity/disaster recovery provisions documented	☐ Yes ☐ No ☐ N/A
Exit strategy and data portability provisions in place	☐ Yes ☐ No ☐ N/A
AI model documentation and explainability provided	☐ Yes ☐ No ☐ N/A
Ongoing monitoring process for vendor performance/security	☐ Yes ☐ No ☐ N/A

Fair Lending & ECOA Considerations

Requirement	Status
AI credit decisions tested for disparate impact	☐ Yes ☐ No ☐ N/A
Adverse action reasons can be provided for AI decisions	☐ Yes ☐ No ☐ N/A
AI model inputs reviewed for proxy discrimination	☐ Yes ☐ No ☐ N/A
Human review process for AI-assisted credit decisions	☐ Yes ☐ No ☐ N/A

Documentation & Audit Trail Requirements

- Maintain records of all AI systems in use (sanctioned and discovered)
- Document risk assessments and approval decisions for AI implementations
- Retain AI model validation and testing results
- Log AI-assisted decisions affecting members (credit, fraud alerts, etc.)
- Track employee AI training completion and policy acknowledgments
- Document incidents involving AI systems and remediation actions

Sources: NCUA AI Resource Center (ncua.gov/ai), NCUA Board Briefing July 2025, GAO Report #25-107197 (May 2025)