

AI Governance for Credit Unions: Internal Compliance and Third- Party Oversight



Mid-Sized Credit Union CEO Roundtable
October 8th, 2026



Logan Hayward, ABCP/CC
IT Compliance Consulting Team Lead
logan.hayward@cuanswers.com



NIST NATIONAL INSTITUTE OF
STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE



<https://www.nist.gov/cybersecurity-awareness-month>

Introduction and Agenda

- 1 AI Uses for Credit Unions
- 2 Risks associated with AI use
- 3 Mitigating AI Risks
- 4 AI Compliance
- 5 Closing Thoughts



Logan Hayward,
IT Compliance Consulting
Team Lead
logan.hayward@cuanwers.com



AI Uses for Credit Unions

1 Member service

- Chatbots and virtual assistants
- Drafting responses to member inquiries
- Call summarization and service-quality reviews

2 Fraud and identity

- Identifying unusual account activity
- Detecting potential fraud patterns
- Prioritizing alerts for staff review

3 Lending

- Summarizing applicant information for loan officers
- Supporting underwriting decisions
- Reviewing loan packages



AI Uses for Credit Unions

1

Member service

The logo for posh, featuring the word "posh" in a dark blue, lowercase, rounded sans-serif font.

2

Fraud and identity

3

Lending

The logo for SCIENaPTIC, featuring the word "SCIENaPTIC" in a bold, black, sans-serif font, with the letter "a" in orange.

The logo for ZEST AI, featuring the word "ZEST" in a bold, dark blue, sans-serif font, followed by "AI" in a bold, orange, sans-serif font, with a small orange circle above the "I".



AI Use Risks

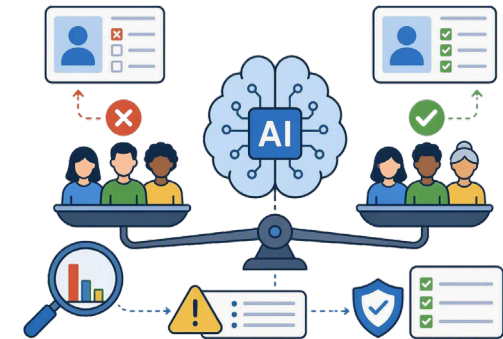
Data Security



Hallucinations



Bias



AI Use Risks

Data Security

AI tools can expose, retain, reuse, or improperly transmit personally identifiable information (PII) such as:

- Member names
- Account numbers
- Social Security numbers
- Loan files
- Call transcripts



AI Use Risks

Hallucinations

Generative AI can produce inaccurate, misleading, or fabricated information that appears credible.

Examples

- Incorrect member service responses
- Inaccurate policy guidance
- Denial of a loan based on non-existent/imagined requirements

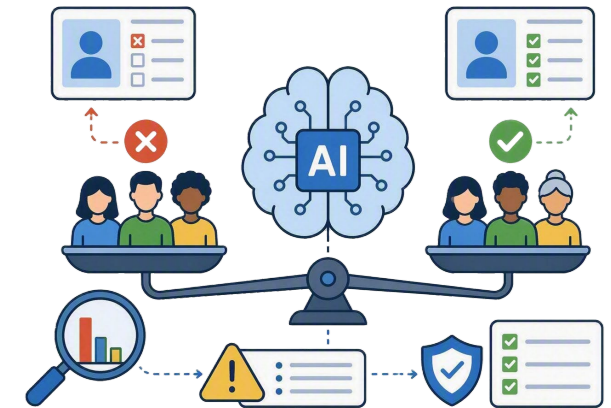


AI Use Risks

Bias

AI-driven lending, underwriting, collections, and marketing can create disparate or unfair outcomes.

The NCUA specifically identifies fair lending compliance and algorithmic decision-making as key risk areas requiring oversight.



Mitigating AI Risks – Data Security

1. Start With Data Classification

- Purview, BigID, Netwrix

2. Adopt a “Minimum Necessary Data” Standard

- AI systems should receive only the information required to complete the task.

3. Control access through identity and permissions

- Multifactor authentication
- Role-based access control
- Least-privilege permissions
- Periodic access reviews



Mitigating AI Risks - Hallucinations

1. Require Human Review

- Human oversight is the most important control

2. Document Significant Reviews

- Who performed the review
- What was reviewed
- What verification was completed

3. Require Evidence for Important Claims

- Disclaimer: *"No AI-generated factual statement may be accepted unless the reviewer can independently verify it through a trusted source."*
- This shifts reviewers from checking grammar to validating accuracy.



Mitigating AI Risks - Bias

1. Require Human Review

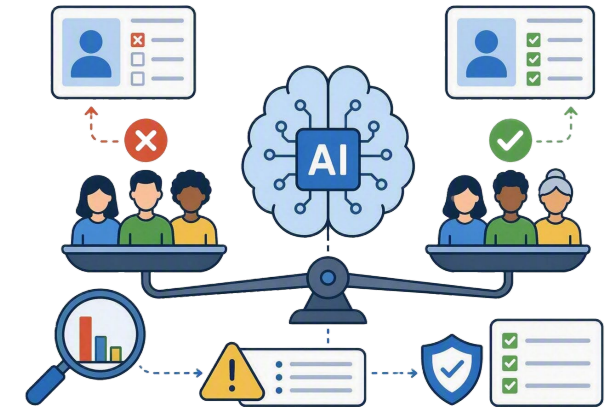
- Human oversight is the most important control

2. Document Significant Reviews

- Who performed the review
- What was reviewed
- What verification was completed

3. Require Evidence for Important Claims

- Disclaimer: *"No AI-generated factual statement may be accepted unless the reviewer can independently verify it through a trusted source."*
- This shifts reviewers from checking grammar to validating accuracy.



AI Compliance

“The NCUA supports the adoption of technology, including AI, when implemented in a safe, sound, and compliant manner.”

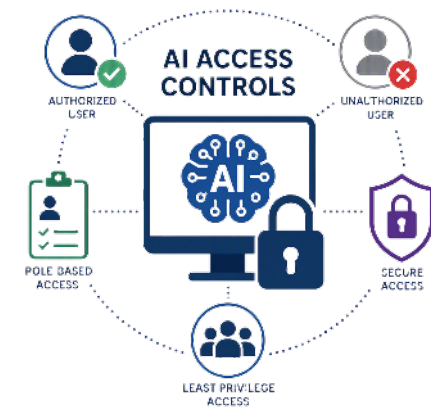
AI Policy



Risk Assessment



Access Controls



AI Policy

1. Purpose, Scope, and Acceptable Use

Define covered users and systems, approved tools, permitted uses, prohibited activities, and exceptions.

2. Governance and Accountability

Establish board and management oversight, risk appetite, ownership, AI inventory, risk assessments, and approval requirements.

3. Data Protection and Responsible AI Controls

Address member-data privacy, access controls, security, accuracy, fair lending, explainability, and required human review.

4. Third-Party Oversight and Ongoing Monitoring

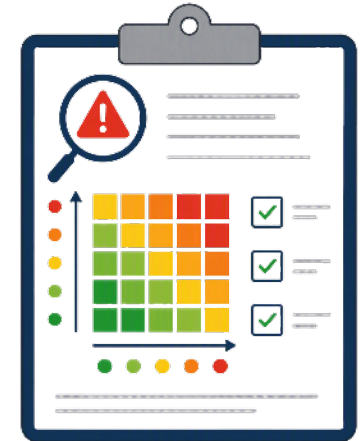
Cover vendor due diligence, contract protections, performance testing, incident response, employee training, reporting, and periodic reassessment.



Risk Assessment

Section 4: Software/Services

Artificial Intelligence										
Responsible Parties	Functional Description									
Credit Union	See Questionnaire: - What AI systems or tools are currently in use? - What business processes rely on AI technologies? - Are AI models hosted internally or through a third-party provider? - Do AI systems process Personally Identifiable Information (PII) or Protected Information for Financial Institutions (PIFI)?									
Classification: CN?, IU, SW	Overall Heat Chart:				5.6	4.1	4.9	3.3	4.	
Artificial Intelligence										
Threat	Controls					Risk Impact	Risk Probability	Inherent Risk	Control Effectiveness	Residual Risk
Non-secure Settings	- AI systems are subject to periodic security reviews (OWASP Top Ten). - Potential adversarial threats (e.g., data poisoning, model manipulation) have been evaluated. - Access is via encrypted channel. - Data is encrypted at rest.					9.0	4.0	6.5	3.0	4.
Outdated Systems	N/A									
Unauthorized Systems Access	- Access is restricted to authorized personnel. - Role-based access controls are in place. - AI system logs are reviewed for unauthorized access attempts.					7.0	5.0	6.0	3.0	4.
Unauthorized Physical Access	N/A									
Hardware Failure	N/A									
Software Failure	N/A									
Communications Failure	Communications are internet based and rely on the vendor and credit union internet connections.					5.0	4.0	4.5	3.0	3.
Network-Based Attack	Managed firewalls are configured to drop traffic for DoS/DDoS attacks.					5.0	5.0	5.0	4.0	4.
Software/Application-Based Attack	Managed firewalls are configured to drop traffic for DoS/DDoS attacks.					5.0	5.0	5.0	4.0	4.
Exposure of Sensitive Information	- Sensitive data used in AI models is encrypted in transit and at rest. - Strict data minimization practices are applied to AI training datasets.									



AI Access Controls



Web category + URL filtering

- Block known public AI and generative AI domains
- Maintain an exception list for approved enterprise AI services.



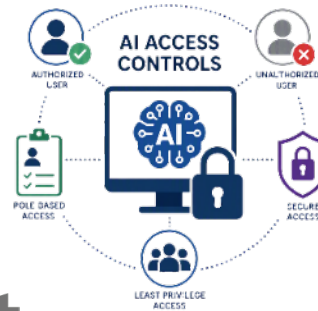
Endpoint controls

- Use endpoint management to block installation or execution of unauthorized AI software.
- Prevent users from installing browser extensions without administrator approval.
- Remove local administrator rights where they are not required.



Role-based access controls

- Create AI-specific roles such as approved user, developer, administrator, and auditor.
- Grant access only to employees with a validated business need.
- Conduct periodic access reviews and automatically remove access after role changes.



Closing Thoughts



“The NCUA supports the adoption of technology, including AI, when implemented in a safe, sound, and compliant manner.”

- AI compliance is not about eliminating every risk or slowing innovation.
- It's about knowing where AI is used, protecting member data, assigning clear ownership, and maintaining evidence that the technology is working as intended.
- Start with controlled, measurable uses, apply human oversight, and expand only when the value and the controls are clear.



AI Governance for Credit Unions

Internal Compliance and Third-Party Oversight

MID-SIZED CREDIT UNION CEO ROUNDTABLE • FALL 2026 • OCTOBER 8, 2026

PRESENTED BY

AJ Schalk, CUCO — AVP, AuditLink — aj.schalk@cuanswers.com

Introduction and Agenda

- 1 The 5-Stage Life Cycle
- 2 Identifying AI Use
- 3 Risk Assessment & Policy
- 4 Ongoing Monitoring
- 5 Contract Management
- 6 Regulatory Spotlight: Michigan DIFS Bulletin



AJ Schalk
AVP, AuditLink

The 5-Stage Life Cycle for AI

1

Planning

A strategy for identifying, selecting, and overseeing the third party.

Assess vendors' training data sources, model transparency, alignment with specific use case.

2

Due Diligence & Selection

Reviewing the third party's legal, financial, and operational ability to perform.

How do they handle data privacy? Will your data be used to train public models? Cybersecurity, etc.

3

Contract Negotiation

Defining rights, responsibilities, performance metrics, and accountability.

4

Ongoing Monitoring

Continuous oversight through control reviews, meetings, and reporting.

Includes tracking model drift, security vulnerabilities, and fairness metrics.

5

Termination

Planning an orderly transition, in-house move, or discontinuation of services.



Sound Familiar?

It should!

The 5-Stage Life Cycle

1

Planning

A strategy for identifying, selecting, and overseeing the third party.

2

Due Diligence & Selection

Reviewing the third party's legal, financial, and operational ability to perform.

3

Contract Negotiation

Defining rights, responsibilities, performance metrics, and accountability.

4

Ongoing Monitoring

Continuous oversight through control reviews, meetings, and reporting.

5

Termination

Planning an orderly transition, in-house move, or discontinuation of services.

Are We Using AI?

You may not be using AI internally (Copilot, ChatGPT, Claude, etc.) — but are your third parties?



Identifying AI Use

1 Identify AI embedded in all third-party services

Ask the question, document the answer — including existing relationships.

2 Can the vendor provide transparency?

How are they using AI? Will they share an AIS (AI Systems Policy)?

3 Will they notify you of material system changes?

If they begin using AI, will they tell you? If so, how?

4 Is it used to make decisions?

Risk Assessment and Policy

1 Develop an AIS (AI Systems Program)

Designed to mitigate risk of adverse consumer outcomes

2 AIS can be companion document to Vendor Management Policy

Ensure that AI risk is being addressed in your policy and risk assessment

3 Include verbiage on upfront due diligence performed

Asking the questions from identifying AI use. Mention the documentation of these inquiries

4 Specific carve outs for AI

Although many of these processes are the same, specify AI verbiage

Ongoing Monitoring

“Not so different from already established regulations, just AI specific.”

Assess Vendor Data Quality

Confirm the data suitability behind the vendor's AI before relying on its output.

Monitor the Vendor & Results

Ongoing review of AI performance and results — not just a one-time check.

Due Diligence Documentation

Keep the same records you already apply to other vendors.

Contract Management

1

Data Usage & Ownership

Who owns member data processed by AI, and how the vendor may reuse it.

2

Change Notification

The vendor's obligation to notify you of material AI or system changes.

3

Audit & Inspection Rights

Your ability to review vendor AI practices, outputs, and results.

Contract Management (cont.)

4

Liability & Indemnification

Accountability for errors or harm caused by AI-driven decisions.

5

Service-Level Commitments

Performance and accuracy standards for AI-supported services.

6

Termination & Data Return

A clear process for exiting the relationship and retrieving or deleting data.

Regulatory Spotlight: Michigan DIFS Bulletin

ISSUED JANUARY 14, 2026 — BULLETIN 2026-03-BT/CF/CU

● Who It Applies To

Depository institutions (including credit unions), mortgage lenders/servicers, money transmitters, licensed lenders, and other DIFS-regulated financial service providers in Michigan.

● The Core Ask

A written “AIS Program” — an AI Systems Program — for the responsible use of AI Systems that make or support decisions affecting consumers.

● The Standard Doesn't Change

AI-driven decisions still can't be inaccurate, arbitrary, capricious, or unfairly discriminatory — including under Michigan's Elliott-Larsen Civil Rights Act.

● No AI? Still a Requirement

Providers who don't formally use AI Systems should, at minimum, have a written employee acceptable-use policy.

What DIFS Expects in an AIS Program

1

Governance

Senior management ownership, board accountability, and clear committees spanning compliance, legal, and data science.

2

Risk Management & Internal Controls

Data quality and bias testing, model inventories, validation, and monitoring for Model Drift.

3

Third-Party AI Systems & Data

Due diligence on vendor AI, plus contract terms for audit rights, data security, and regulator cooperation.

4

Documentation

Policies, procedures, and records proportionate to the AI System's risk to consumers.

What Examiners Will Ask For

The Written AIS Program

Your policies, procedures, and governance documentation — and how it's tailored to your risk.

Model & Vendor Inventories

Descriptions of every Predictive Model or AI System in use, whether built in-house or by a vendor.

Due Diligence & Contracts

Vendor due diligence records, audit rights, and validation and Model Drift testing results.

Key Takeaway for Your Credit Union

- Sound familiar? It should — DIFS's expectations map directly onto the 5-stage life cycle and contract terms already on in place for vendors today.
- Most credit unions don't build their own AI — you rely on vendors who do, so the Third-Party AI Systems requirements apply directly to your vendor contracts.
- “We don't use AI” isn't an exemption — DIFS still expects a written acceptable-use policy at minimum.
- Using AI never relieves your anti-discrimination obligations.
- This is Michigan-specific guidance — if you operate in other states, check for similar bulletins from your home regulator.

Have Any Questions?

AJ Schalk, CU*CO — AVP, AuditLink

aj.schalk@cuanswers.com

AuditLink

CU*Answers Management Services

6000 28th Street SE

Grand Rapids, Michigan 49525

(800) 327-3478

info@auditlinksuite.com

auditlinksuite.com