The Best Intern You Never Hired

A Practical AI Playbook for Community Bankers

Future Ops 2026 | Nebraska Community Bankers Conference

Brandon Gettert

CEO / CISO | Curated Cyber

CURATED CYBER
A vCISO FIRM

ABOUT CURATED CYBER

Who We Are

Our Focus

- vCISO / Advisory Service
- Specialists in community banking security
- Also serve legal, software, and FinTech clients

What We Do

- Virtual CISO services (vCISO)
- Vendor Lifecycle Assurance (VLA)
- vAIO — Virtual AI Officer

TODAY'S TALK

Part pep talk. Part playbook.
Entirely practical.

AI is moving fast, and if you're still trying to figure out what to do about it, you're in good company. This session cuts through the noise and gives you a practical, no-nonsense look at what AI actually looks like inside a bank today.

From SAR narratives to board reports to vendor management, we'll walk through what your peers are already doing — and how to build the governance structure that keeps it from going sideways.

You'll leave with a clear picture of how to stand up an AI committee, run your first AI risk assessment, ask the right questions of your vendors, and build a culture where your team uses AI confidently and responsibly.

Whether you're already knee-deep in AI or just trying to figure out where to start — this one's for you.

ChatGPT | Copilot | Claude

TODAY'S TALK

What We're Covering Today

01

The Wake-Up Call

Why AI is no longer optional for community banks

02

What Your Peers Are Doing

Real use cases already running at banks like yours

03

Your Governance Playbook

AI Committee, risk assessment, policy, and vendor questions

04

Prompt Library

The gap between a bad AI user and a great one

LET'S BE REAL

I Know What Your Bank Actually Looks Like

"Some of you are the CISO, the compliance officer, and the person who fixes the printer."

Lean IT teams — One or two people covering everything from network security to end-user support. AI isn't a threat to your headcount — it's how you keep up.

Ag lending complexity — Seasonal cash flow, commodity price cycles, multi-generational operations. AI can help you draft, summarize, and research — the judgment stays with you.

Small towns, real relationships — Your customers know your name. AI handles the paperwork so you can spend more time on the relationship.

You don't need a data science team — You need a plan and a handful of enterprise licenses. The tools are built for people who run banks, not people who run algorithms.

THE WAKE-UP CALL

Not Using AI Would Be Like Not Using the Internet

In 1999, some banks said 'Our customers don't need online banking.' How'd that work out?

~2 hrs

avg time saved
per week per user
(St. Louis Fed, 2025)

50%

of GenAI users
save 5+ hrs/week
(13k-worker global survey)

75%

of knowledge workers
are already using AI
(Microsoft/LinkedIn, 2024)

47%

use AI without
telling their employer
(shadow AI is real)

Sources: St. Louis Fed (2025), LSE/Protiviti global survey (2025), Microsoft & LinkedIn Work Trend Index (2024)

THE WAKE-UP CALL

Shadow AI: It's Already in Your Building

100+

GenAI apps in Microsoft Defender's catalog.
How many are in yours?

Source: Microsoft Defender for Cloud Apps catalog

Your staff are using AI tools right now — whether IT knows it or not.

Microsoft Defender for Cloud Apps includes an AI App Discovery dashboard that surfaces every AI application running in your Microsoft environment. Most banks run this scan and find hundreds of unauthorized AI tools — apps employees downloaded, browser extensions with AI, and more.

"You don't have an AI problem. You have an unmanaged AI problem."

One Shadow AI audit = full visibility into what's already running | Takes ~30 min with Microsoft Defender

SECTION 1

What Your Peers Are Already Doing

Tools in use at community banks today: ChatGPT, Copilot, Claude

Compliance & BSA

SAR narrative drafts, CTR summaries, regulatory research, exam prep

Emails & Communications

Board reports, status updates, customer responses, policy summaries

Policy & Procedures

Policy drafting, procedure documentation, handbook modernization

IT & Troubleshooting

Ticket triage, runbook drafting, error message research, vendor change summaries

Lending & Credit

Credit memo drafts, financial summaries, loan package preparation

Marketing

Social media calendars, newsletter content, press releases, staff bios

SECTION 2

Your Governance Playbook

How to manage your intern so they don't burn down the bank.

1

AI Risk Assessment

Document tools in use, data flows, controls in place, and residual risk. This is what examiners are starting to ask for.

2

Stand Up an AI Committee

Ops, Compliance, IT, Lending, HR, and a C-Suite rep. Monthly meetings, standing agenda, use case pipeline.

3

Enterprise Licensing

Consumer-grade AI tools are not the enterprise version. Know your data agreement before your staff pastes a customer name.

4

Board Reporting

Your board needs to know where you stand. Build AI status into your regular reporting cadence.

5

AI Champions

Identify enthusiastic early adopters across departments. Let them lead use case pilots and train their peers.

THE INTERN ANALOGY

Meet Your New Best Friend

Knows everything. Seriously — has read virtually the entire internet.

Available 24/7. Never calls in sick. Never asks for a raise. Never complains.

Can draft a memo, summarize a 200-page exam report, write a formula, or explain a regulation — in seconds.

Speaks every language. Passed the bar. Writes like Hemingway.

But your best friend still gets things wrong sometimes. Always verify what they tell you.

You Own the Output.

Full Stop.

If an intern writes a memo and you sign it — you own it. AI is identical.

The obligation is on review and accountability — not on disclosure of the tool.

AI is a drafting and research assistant. You are the professional of record.

"You reviewed it. You own it."

THE AI COMMITTEE

Build an AI Committee — Not Just a Policy

AI governance isn't a document you file and forget. The AI Committee is a standing internal function.

Who Should Be On It

- **Operations**
- **Compliance**
- **IT / Security**
- **Lending**
- **Human Resources**
- **C-Suite Rep**

How It Runs

1. Monthly meetings with a standing agenda
2. Approve and maintain the AI tool inventory
3. Run the AI risk assessment and update it annually
4. Identify AI Champions
5. Manage AI incidents and define escalation paths
6. Report AI program status to the board

The AI Committee is the governance body — it sets policy, approves tools, owns risk, and reports to the board (IAPP, OneTrust, IIA best practice guidance)

YOUR AI POLICY

What a Bank AI Policy Actually Needs to Cover

Most banks either have no policy or have a generic one that doesn't fit the environment. Here is what a real one covers:

Permitted vs. Prohibited Uses

SAR drafts and board reports — permitted. Final credit decisions without human review — prohibited. Draw the line clearly.

Sanctioned Tool List

Only approved tools may be used. Consumer-grade and free-tier tools are explicitly prohibited. The list is maintained by leadership.

Data Handling Requirements

Customer PII and NPI stay out of AI tools. Employees use placeholder text.

Employee Accountability Standard

All AI output is validated before use or distribution. The employee who submits it owns it. No exceptions.

Regulatory Anchors

Policy aligns to GLBA, FFIEC guidance, FDIC, and OCC.

Vendor and Third-Party AI

All vendors using AI go through TPRM. Ask about model explainability, bias mitigation, data handling, and audit rights.

AI Committee Oversight

The committee approves new tools, reviews the policy annually, and owns the AI risk assessment and incident escalation path.

Ethics and Fairness

AI must not produce discriminatory outcomes. Validate for bias.

A good AI policy is Board-approved, annually reviewed, and accessible to every employee — not filed and forgotten.

VENDOR MANAGEMENT

What to Ask Your Vendors About AI

If you're a vendor:

Create an AI Use Statement for your clients.

- What AI tools do you use in service delivery?
- Is my data used to train any AI model?
- Do you have an enterprise agreement with your AI vendors?
- Do you have an AI policy and an AI Committee?
- Are audit logs in place for AI activity?

If you're a bank:

Ask your vendors for an AI Use Statement.

- Is my customer data in your AI training pipeline?
- Where is my data stored — US, offshore?
- What happens to prompts and outputs?
- Do you have an AI Risk Assessment on file?
- Have you run a vendor risk assessment on your own AI tools?

Your AI tool vendor is a third-party vendor. Run them through your TPRM process like everyone else.

YOUR PLAYBOOK

Your First 30 Days — A Roadmap

Week 1	Week 2	Week 3	Week 4
Shadow AI Audit	**Stand Up Your AI Committee**	**Pick One Use Case & Pilot It**	**Define Your Review Workflow**
Run Microsoft Defender's AI discovery scan. Find out what's already running. No judgment — just visibility.	Even 4 people is enough to start. Ops, Compliance, IT, C-Suite. Set a recurring monthly meeting. Identify your Champions.	Choose something low-risk with measurable output — SAR drafts, procedure docs, or job descriptions. Run it 30 days.	Who reviews AI outputs before they go anywhere consequential? Document it. Make it a policy. Enforce it.

"Don't let perfect be the enemy of Good."

EXAMINER REALITY CHECK

What Regulators Are Already Asking About

FFIEC, OCC, and FDIC guidance on AI is maturing. Examiners are already asking these questions at community banks.

Do you have an AI policy?	Boards are expected to understand and oversee AI risk. A policy signals program maturity.
What AI tools are in use — sanctioned or otherwise?	Examiners want to see that you know what's running in your environment, including shadow AI.
How are you managing AI vendor risk?	Third-party AI tools fall squarely in your TPRM program. No carve-outs.
Is AI output reviewed before it reaches customers or regulators?	Human oversight of AI-generated content is a baseline expectation, not a best practice.
Has your board been briefed on AI risk?	AI is increasingly a board-level topic. If it's not in your reporting yet, it needs to be.

The policy-before-the-incident line: It is much easier to show examiners a governance program than to explain why you didn't have one.

AI RISK ASSESSMENT

What It Is — And How It Works

Built from GLBA, FFIEC Information Security Handbooks, NIST AI RMF 1.0, and U.S. Treasury AI guidance. Qualitative model. Examiner-ready.

THE THREAT	SCORING	CURRENT CONTROLS	RESIDUAL RISK	MGMT RESPONSE
Board has not established AI risk appetite or AI Committee	Likelihood: Medium Damage: Moderate Inherent: Medium	AI Committee established. AUP Board-approved. vCISO provides ongoing governance.	**Low / Medium** **Controls: Strong**	Formalize committee charter. Confirm AI risk in Board IS reporting cadence.
Staff using AI tools without enterprise agreement — data may leave the organization	Likelihood: High Damage: Moderate Inherent: Medium/High	Approved tool list defined. Consumer tools prohibited. AUP communicated and acknowledged.	**Medium** **Controls: Fair**	Block unsanctioned tools via content filter. Add AI disclosure question to TPRM process.
AI-enabled deepfakes and social engineering targeting staff and wire transfers	Likelihood: High Damage: Major Inherent: High	Phishing simulations, IS Awareness Training, out-of-band verification procedures in place.	**Low / Medium** **Controls: Strong**	Add deepfake scenarios to tabletop exercises. Require verbal verification for all wire requests.
AI output used in SAR narratives or board reports without human review	Likelihood: Medium Damage: Moderate Inherent: Medium	Ownership Standard: employee reviews and owns all AI-assisted output before submission.	**Low / Medium** **Controls: Strong**	Reinforce in training. Include in annual AUP acknowledgment. Document review workflow.

Each row = one risk area. Reviewed by the AI Committee. Updated annually or when your environment changes. Examiner-ready.

AVOID THESE

Common Pitfalls to Avoid

🚫 Deploying Without a Review Workflow

AI output going directly into a customer document or regulatory filing without anyone checking it. This is how you get burned — and how you explain it to an examiner.

🔓 Consumer Tools With Sensitive Bank Data

The free version of ChatGPT is not the enterprise version. If your staff is pasting customer names, account numbers, or SAR details into a consumer tool, you have a data problem right now.

🏢 Letting One Department Own It

If IT owns AI governance alone, Compliance gets nothing. If Compliance owns it, Operations gets nothing. This is cross-functional — it needs a committee.

📄 Treating AI Output as a Final Draft

First drafts. Always. Every single time. No exceptions. Review before anything goes out the door. The intern doesn't get to sign the memo.

🔍 Skipping Vendor Due Diligence on AI Tools

Your AI tool vendor is a third-party vendor. Run them through your TPRM process like every other vendor. Where does my data go? Is it used for training? Who has access?

ALWAYS VERIFY

The AI Hallucination Hall of Shame

⚖️ Mata v. Avianca (S.D.N.Y. 2023) — The Lawyer Who Cited Fake Cases

Attorney Steven Schwartz submitted a brief with six ChatGPT-invented cases that never existed. When caught, he asked ChatGPT to confirm they were real — it insisted they were. Judge Castel sanctioned the firm $5,000.

✈️ Moffatt v. Air Canada (BC Tribunal 2024) — The Chatbot That Invented Policy

Air Canada's chatbot told a customer he could apply for a bereavement fare retroactively. He booked, traveled, applied — denied. The tribunal ruled Air Canada liable. Their defense: 'the chatbot is a separate legal entity.' Rejected.

📊 Google Bard (Feb 2023) — $100 Billion Demo Error + The Book That Doesn't Exist

Demo #1: Bard claimed James Webb took the first-ever photos of exoplanets — wrong, that was VLT in 2004. Reuters caught it same day. Stock dropped ~9%, erasing $100B. Demo #2: On 60 Minutes, Bard described a book 'The Inflation Wars' by MIT economist Peter Temin. The book doesn't exist. Temin is real. The book isn't. That is almost impressive.

🎤 *STORY: Tell the Q2 Vendor Review story — what that process looked like before AI, and what it looks like now.*

SECTION 3

Prompt Literacy: Context Is Everything

The gap between a bad AI user and a great one is almost entirely how they prompt.

GENERIC PROMPT

"Write me a SAR narrative."

No role context. No institution size. No facts of the case.
AI fills in the blanks — usually wrong.

WELL-CRAFTED PROMPT

"I am the BSA Officer at a $400M community bank in Texas. State-chartered, FDIC regulated. Draft a SAR narrative for structuring activity: a cash-intensive business made three transactions under $10,000 in five days."

Well-prompted AI cuts drafting time by 60–80% vs. starting from scratch — context is the multiplier

PROMPT LIBRARY

Real Prompts Your Team Can Use Starting Today

A prompt library standardizes how your team uses AI — less variability, better output, easier to govern.

Calendar & Scheduling

What is my calendar for today? Format as start-end time (9:00am-10:00am). Meeting name only. No links, no organizer details, no bullets.

Grammar & Writing

Improve grammar and fix spelling in this email. Keep my voice and tone. Do not rewrite — just clean it up.

vCISO Meeting Notes

I am a vCISO for a community bank regulated by the FDIC. Take this transcript from today's vCISO call. Draft high-level meeting notes. Flag action items needing follow-up. Match the style of my previous vCISO summaries.

ITSC Meeting Notes

Take this transcript from today's ITSC meeting. Draft high-level meeting notes. Flag action items that need follow-up. Match the style of my previous ITSC summaries.

Policy Formatting

I want the output to match the client's Acceptable Use Policy. Extract its exact styling and formatting, then apply it to the content I provide.

monday.com Board Update

Board: [Bank Name]. From today's vCISO recap: post the full summary as an update on the Monthly vCISO Meeting item. Add action items. Update status and due date. Notes field 10 words max with date stamp only.

Build your own library. Store it somewhere every employee can find it. Review it when tools or workflows change.

WORKING WITH CURATED CYBER

The vAIO — Virtual AI Officer

If you want help standing up AI governance the right way — this is what working with us looks like.

AI Governance Framework

AI policy, acceptable use, and committee charter built for your institution size and regulatory profile.

AI Risk Assessment

Full assessment of your AI tool environment — inventoried, risk-rated, and examiner-ready.

Vendor AI Risk Review

We review your key vendors' AI posture so you can ask the right questions and document the answers.

AI Training and Enablement

Staff training, prompt literacy sessions, and AI Champion development across your organization.

Ongoing Advisory

Monthly AI Committee support, board reporting, and program maturity tracking as the landscape evolves.

Exam and Audit Support

We help you walk into your next exam with documentation that shows a managed, governed AI program.

brandon@curatedcyber.com | curatedcyber.com

AI won't replace Community Bankers.

But community bankers who use AI will replace those who don't.

Questions? We'd love to hear them.

Brandon Gettert | brandon@curatedcyber.com | linkedin.com/in/brandongettert/