Tandem®

Artificial Intelligence Risk Management

A WORKBOOK FOR COMMUNITY FINANCIAL INSTITUTIONS

About the Authors

Alyssa Pugh, CISM, CRISC, Security+
GRC Content Manager
Tandem, LLC
LinkedIn.com/in/AlyssaPugh

Alyssa is an educator, expert, and content creator with a passion for helping people navigate the challenges of governance, risk management, and compliance (GRC). She has more than ten years of professional technical and information security experience. She currently serves as the GRC Content Manager for Tandem, where she supervises the Tandem Content team and oversees the development of cybersecurity compliance content and educational resources. In addition to her passion for technology, Alyssa is also a wife, graphic designer, and video game enthusiast.

Savannah Richardson, ITRF
GRC Content Analyst
Tandem, LLC
LinkedIn.com/in/Savannah-Lee-Richardson

Savannah finds joy in education - striving to make information more accessible for teaching and sharing resources. She has a B.A. in Business Administration, an M.S. in Finance, and has earned the IT Risk Fundamentals ISACA certificate. Currently, Savannah works as a GRC Content Analyst at Tandem. In her free time, Savannah collaborates with a dedicated group supporting small businesses through vendor markets, enjoys reading, and loves to travel.

Disclaimer
This resource is for information purposes only. Businesses may use this resource to assist with their AI risk management practices, but are encouraged to evaluate the risks and coordinate with appropriate legal counsel before acting on ideas from this document.

Contents

Why We Wrote This Workbook

AI is transforming how financial institutions operate, and with new capabilities come new risks. This workbook is designed to help institutions navigate those risks and use AI responsibly.

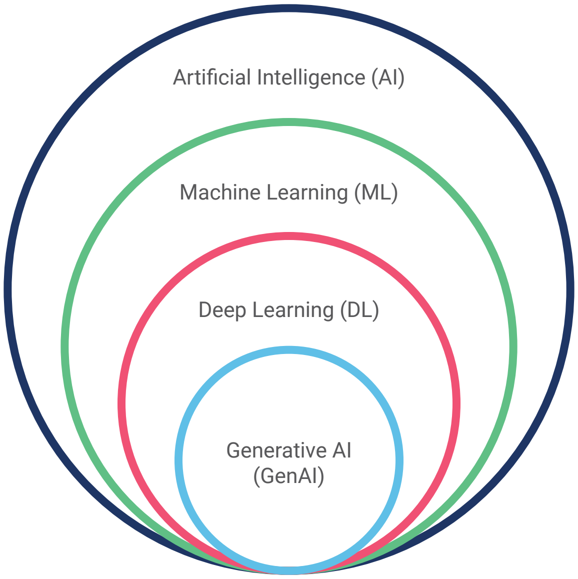
The concepts and tools in this workbook are even more effective when used in Tandem. See how Tandem can help you at Tandem.App/AI-Features-Demo.

What is Artificial Intelligence (AI)?

The term “artificial intelligence” (AI) has increased in popularity in recent years.

In 15 U.S.C. 9401(3), the United States government defines AI as:

> *“A machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. Artificial intelligence systems use machine and human-based inputs to (A) perceive real and virtual environments; (B) abstract such perceptions into models through analysis in an automated manner; and (C) use model inference to formulate options for information or action.”*



In short, AI is a system that uses human-set goals and inputs to understand its environment, create models, and make predictions or decisions.

Another way to look at AI is to describe it in subsets:
machine learning (ML), deep learning (DL), and generative AI (GenAI). Each one is basically a subset of the other, getting more specialized as you go along.

The term “AI” has come to be used primarily for GenAI, and that is what we mean when we refer to AI throughout this booklet.

AI Use Cases

There are numerous use cases for artificial intelligence. Several current popular use cases include:

Content Generation
(e.g., text, images, audio, video)

Data Analysis
(e.g., statistical analysis, anomaly detection)

Insight Generation
(e.g., predictive modeling, forecasting, AVMs)

Natural Language Processing
(e.g., summarization, translation, sentiment analysis)

Security Functions
(e.g., system monitoring, anti-malware, EDR / XDR)

Code Development
(e.g., code authoring, review, optimization, debugging)

Customer Support
(e.g., chatbots, ticket classification)

Business Automation
(e.g., robotic process automation, task automation, data entry)

AI Regulations and Guidance

When you search for regulatory writings about AI, you won't find much referring specifically to the term. What you will find though is that the federal banking regulators have released extensive guidance on security, third-party risk management, model risk management, and other areas that are directly applicable to AI.

Here's a summary of current regulations and guidance and how they apply to a financial institution's use of AI systems.

Gramm-Leach-Bliley Act (GLBA)

GLBA (15 U.S.C. 6801) and the resulting Interagency Guidelines Establishing Information Security Standards require financial institutions to protect nonpublic personal information by implementing administrative, technical, and physical controls. This regulation applies to all systems which access or store customer information, including AI systems. Learn more on our blog: GLBA Compliance: The Legislation, the Standards, and the Guidance.

FFIEC IT Examination Handbook

The FFIEC IT Examination Handbook is made up of several principles-based booklets designed to help examiners evaluate whether financial institution technology systems are secure, including AI systems. The booklets provide guidance on key security practices and controls, including access control, authentication, change management, data management, encryption, IT asset management, logging and monitoring, personnel security, training, and others which apply to AI.

Third-Party Risk Management Guidance

The FDIC, FRB, and OCC's Interagency Guidance on Third-Party Relationships: Risk Management and the NCUA's guidance on Evaluating Third-Party Relationships provide details about managing the lifecycle of vendor relationships, including planning, due diligence and selection, contract negotiation, ongoing monitoring, and termination. This guidance should be applied to third-party relationships with AI service providers and service providers who integrate AI into their offerings.

Model Risk Management Guidance

The interagency Supervisory Guidance on Model Risk Management provides recommendations for managing model risk. AI systems depend heavily on models. As such, if you use AI systems to make certain types of decisions, the models should be managed in accordance with this and clarifying guidance. Learn more on our blog: Model Risk Management FAQs for Community Banks & Credit Unions.

Automated Valuation Models (AVM) Final Rule

The federal banking agencies published a final rule on Quality Control Standards for Automated Valuation Models. If you use AI to perform automated valuations, the requirements established in this rule would apply.

U.S. Treasury Department Guidance on AI

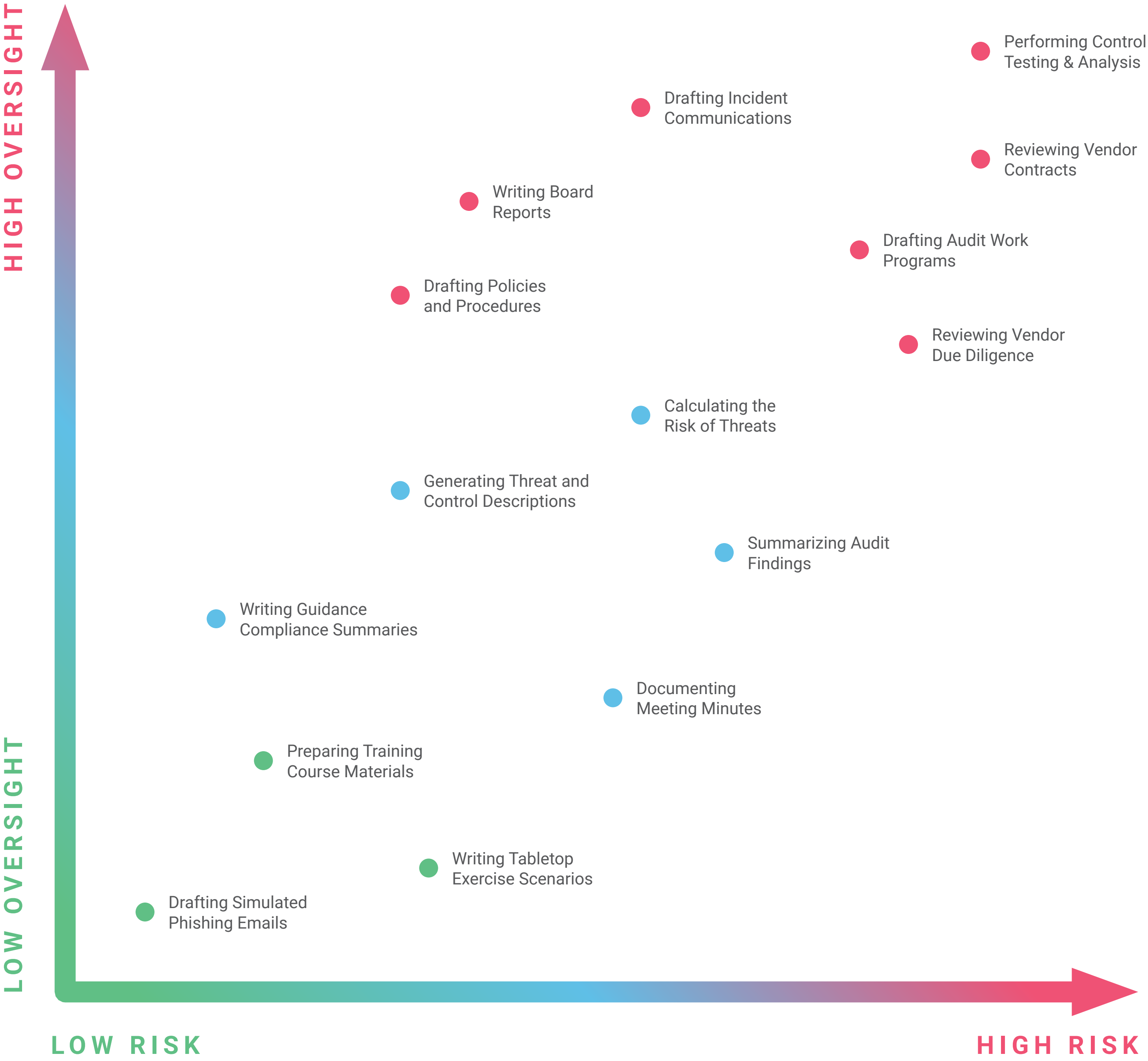
The U.S. Treasury Department has published two reports on AI, including a Report on the Uses, Opportunities, and Risks of Artificial Intelligence in Financial Services and a Report on Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Sector. Both documents provide insights and recommendations for secure implementation of AI.

For additional reading, see our blog: What are the Regulators Saying about Artificial Intelligence (AI)?

Using GenAI for GRC Functions

As a GRC company, we occasionally hear people ask, “Can I use AI for GRC tasks?” The short answer is, “it depends.” GenAI is powerful, but unpredictable. It produces unique outputs based on patterns in data, not verified facts, and often presents them confidently, whether correct or not. Because no two interactions are identical or reproducible, GenAI can create challenges when used for GRC. While AI promises convenience, the greater the risk of the task, the greater the need for human involvement, validation, and oversight.

The chart below illustrates GenAI risk across core GRC functions and how each relates to the level of human oversight necessary to ensure accurate results.



__Note:__ This chart is for illustrative purposes only. Risk levels and oversight needs will vary based on your organization’s environment and use cases.

AI Legal Considerations

But is it legal? While it may be convenient to use AI for certain GRC functions, approach with caution because it may not always be permissible. Here are three key considerations to evaluate before using AI for GRC.

CONFIDENTIALITY

Sharing documents covered by confidentiality agreements with an AI system can violate nondisclosure obligations with vendors, employees, or partners. This includes contracts, SOC reports, financial statements, etc.

RETENTION

AI systems retain input data. Even if the AI doesn't intentionally share or train on it, the organization's data is still transmitted and stored by a third party in a way that could violate retention and destruction policies.

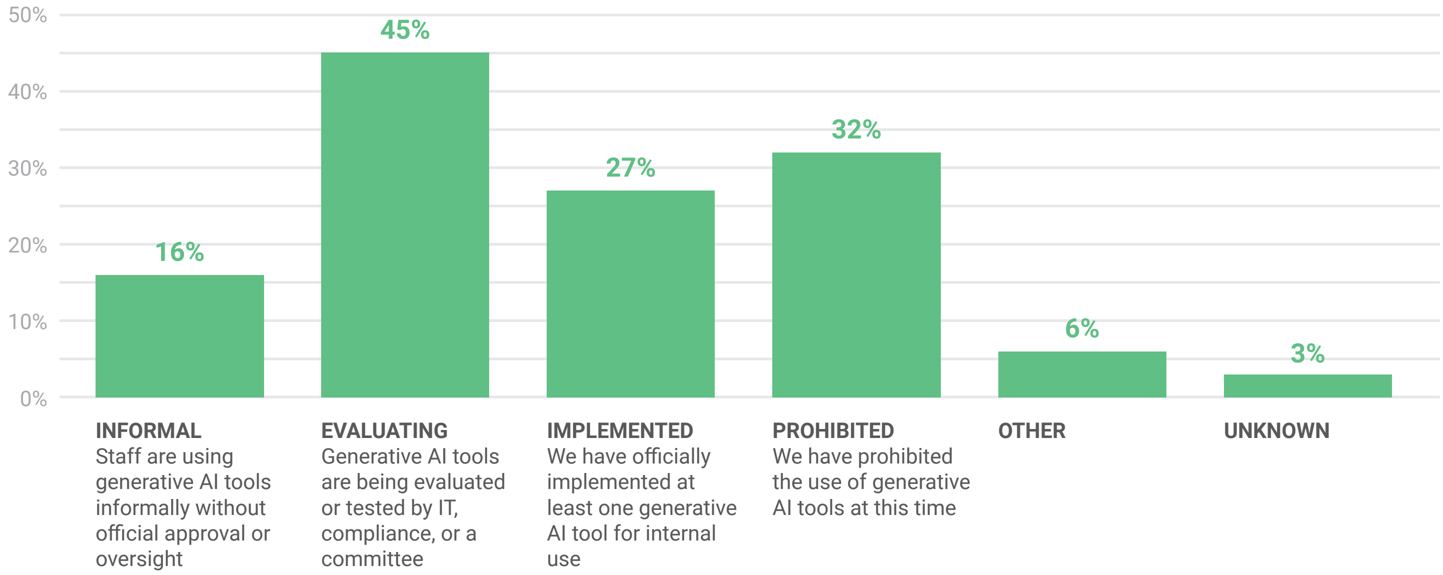
ACCOUNTABILITY

Even when using AI, your organization remains fully accountable for decisions and results. Misuse or overreliance may lead to compliance violations, operational issues, or other legal repercussions.

AI Adoption by Financial Institutions

Financial institutions continue to navigate implementing AI with caution. According to the 2025 Tandem State of Cybersecurity Report, nearly half of respondents are currently evaluating AI while one-third have fully prohibited its use. This suggests many community financial institutions are taking a careful, measured approach to AI adoption, with good reason.

AI USE IN FINANCIAL INSTITUTIONS



AI Risk Management Checklist

So, what does all this mean? How can financial institutions manage the risks of AI while taking advantage of the opportunities? Here are seven things you'll need to do, and we'll dive into each of these areas in the following sections.

- ☐ Develop an AI system profile to outline use cases and responsibilities.
- ☐ Perform an AI risk assessment to identify reasonably foreseeable threats.
- ☐ Write an AI policy defining controls, expected behaviors, and prohibited activities.
- ☐ Manage vendors providing standalone or embedded AI systems.
- ☐ Provide training and awareness programs to address the human element in AI use.
- ☐ Ensure your incident response plan covers the outcomes of AI-related scenarios.
- ☐ Perform ongoing monitoring of AI systems and report results to the Board of Directors.

State of Cybersecurity Report

This document features several "By the Numbers" sections highlighting AI, third-party risk management, and cybersecurity trends in financial institutions. To learn more, you can download the full report at Tandem.App/Report.

Artificial Intelligence (AI)

Observation: Views on AI Adoption Vary A

Generative AI adoption among financial institutions is still emerging. Forty-fi evaluation, while 27% have officially implemented at least one tool for intern generative AI informally without official approval or oversight, and 32% have

AI USE IN FINANCIAL INSTITUTIONS

50%
40%
30%
20%
10%
0%
16%
45%
27%
32%
INFORMAL Staff are using generative AI tools informally without official approval or oversight
EVALUATING Generative AI tools are being evaluated or tested by IT, compliance, or a committee
IMPLEMENTED We have officially implemented at least one generative AI tool for internal use
PROHIBITED We have prol the use of ge AI tools at th

Observation: Microsoft Copilot Leads Ado

Microsoft Copilot stands out as the most widely adopted AI tool, with 68% o deep integration in financial institution technology environments. ChatGPT f low single digits, suggesting they have yet to gain meaningful traction in the

AI TOOL ADOPTION BY FINANCIAL INSTITUTIONS

24 2025 CYBERSECURITY REPORT FOR

Cybersecurity Frameworks & Tools

Observation: The FFIEC CAT is Slowly Bein

On August 29, 2024, the FFIEC announced the sunset of the Cybersecurity A 2025. Before this announcement, 90% of institutions were using the FFIEC C July, when this survey was conducted, 73% of institutions surveyed are usin beginning to gain popularity.

CYBERSECURITY FRAMEWORK USE

Diving Further

While the FFIEC CAT remains the dominant tool for now, most institutions ar term replacement framework. Below are some of the frameworks that saw t

CHANGE IN CYBERSECURITY FRAMEWORK USE

14 2025 CYBERSECURITY REPORT FOR

Staffing

Observation: Staff Sizes Remain Unchange

Most institutions (83%) have 10 or fewer full-time IT or information security As might be expected, the larger the institution, the more IT and security sta

NUMBER OF FULL-TIME IT AND SECURITY STAFF

NUMBER OF FULL-TIME IT AND SECURITY STAFF BY A

Culture Impact: Strong Culture Correlates

The data shows a clear connection between organizational culture and the size of the IT team. Institutions who prioritize a strong cybersecurity culture tend to build larger teams, reflecting a deeper investment in security beyond baseline requirements. In contrast, organizations who approach cybersecurity primarily as a compliance obligation tend to operate with smaller IT teams, which may limit their ability to proactively strengthen their overall security posture. This highlights how culture not only shapes strategy but also directly influences resource allocation.

CYBERSECU

8 2025 CYBERSECURITY REPORT FOR

2025

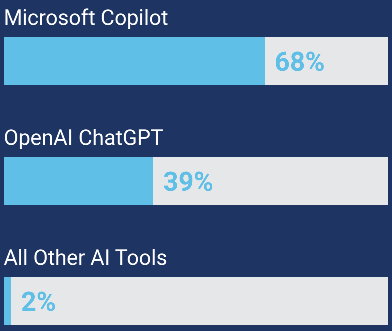
CYBER SECURITY REPORT

FOR THE FINANCIAL INSTITUTION INDUSTRY

Tandem

BY THE NUMBERS

Microsoft Copilot is the most widely adopted AI tool, followed by ChatGPT. All other tools have adoption rates of 2% or less.



SOURCE
2025 State of Cybersecurity Report

DEFINITION

"Embedded AI" refers to third-party software or systems which now include AI features as part of their offerings. Examples of vendors that have embedded AI into their solutions include Adobe, Grammarly, Salesforce, Slack, and Zoom.

DID YOU KNOW?

Some AI tools inherit access or permissions associated with the account they use. If that account has privileged access, the AI could reach much more data than you might expect.

TANDEM TIP

Use the **Information Assets** feature in the Tandem Risk Assessment product to document these details.

AI System Profile

The first step in managing the risk of AI is to clearly define what system you plan to use, how you plan to use it, and who is responsible for it.

Worksheet

01. Which AI system are you planning to use?

□ Microsoft Copilot
□ OpenAI ChatGPT
□ Embedded AI
□ Perplexity AI
□ Anthropic Claude
□ Other (explain) ______________________
□ Google Gemini
□ X Grok

02. What are you planning to use this AI system to accomplish?

03. What types of data will the AI system be able to access?

□ Confidential
□ Business
□ Other (explain) ______________________
□ Sensitive
□ Employee
□ Unclassified
□ Customer/Member

04. What type of account is needed to use this AI system?

□ Dedicated user account with unique credentials
□ Current network, domain, or user account with existing credentials
□ Other (explain) ______________________

05. What type of access permissions will the AI system inherit, if any?

06. Who is responsible for oversight of this AI system?

____

AI Risk Assessment

The next step is to assess the AI system's risks. For each threat below, think about how likely it is to happen and how serious the consequences could be, in light of your AI system and its use case. Then, select a corresponding risk level.

Worksheet

THREAT OVERVIEW

		🔴 High	🟡 Medium	🟢 Low	⚪ N/A
Employee Risks	**Human Error** An employee accidentally misuses or misconfigures the AI system.	□	□	□	□
	Improper Data Destruction An employee fails to retain or delete data associated with the AI system.	□	□	□	□
	Insider Threat An employee deliberately misuses the AI system to harm the organization.	□	□	□	□
	Shadow IT An employee uses or integrates unapproved components with the AI system.	□	□	□	□
	Unauthorized Use An employee uses the AI system for purposes beyond what is allowed.	□	□	□	□
	Unintentional Disclosure (Human) An employee reveals sensitive data by entering it into the AI system.	□	□	□	□
System Risks	**Inaccurate / Unreliable AI Output** The system produces results that are misleading, biased, or fabricated.	□	□	□	□
	Software Problem / Failure The system experiences technical issues that disrupt operations.	□	□	□	□
	Unintentional Disclosure (System) The system reveals sensitive data through responses, logs, or other means.	□	□	□	□

TANDEM TIP

Check out the **Artificial Intelligence (AI) Risk Assessment Type** in the Tandem Risk Assessment product for more details.

THREAT OVERVIEW

		● High	● Medium	● Low	● N/A
Threat Actor Risks	**Compromised Credentials** A bad actor accesses the AI system using stolen identifiers.	□	□	□	□
	Cyber Attack A bad actor targets the AI system leading to outages or data breaches.	□	□	□	□
	Privilege Escalation A bad actor leverages the AI system to access other systems or data.	□	□	□	□
	Supply Chain Attack A bad actor introduces malicious features into the AI system.	□	□	□	□
Third-Party Risks	**Inadequate Logical Access Controls** A vendor fails to enforce strong access controls on the system.	□	□	□	□
	Inadequate Vendor Management A vendor is improperly managed leading to issues or noncompliance.	□	□	□	□
	Insecure Coding Practices A vendor creates a vulnerable system through insecure development activities.	□	□	□	□
	Lack of Independent Testing A vendor fails to independently validate the AI system's security.	□	□	□	□
	Vendor Compromise A vendor is compromised or fails to deliver expected services.	□	□	□	□
	OVERALL RISK	□	□	□	□

Tip: *Consider both the average and the highest risk levels when determining the overall risk.*

AI Policy

To manage the risks associated with AI, you need to have a policy that outlines required controls, expected behaviors, and prohibited activities.

Worksheet

01. Write a clear policy statement.

Example: *Ensure the secure implementation of all artificial intelligence (AI) systems to safeguard data confidentiality, integrity, and availability. Include vendors that integrate AI into their services or provide AI services in the vendor management program.*

02. Write implementation procedures to set clear expectations, such as:

- □ Implementing appropriate controls to secure the AI system
- □ Requiring approval before using new AI systems
- □ Prohibiting the use of unapproved AI systems
- □ Defining how the AI system can and cannot be used
- □ Training employees to use AI systems appropriately
- □ Including AI vendors in the vendor management program
- □ Considering AI-specific factors when determining vendor criticality
- □ Evaluating the vendor's security, as it pertains to AI functions

03. Update the acceptable use policy (AUP) to state:

- □ Employees must not use unapproved AI systems
- □ Employees must use approved AI systems in an appropriate manner *(e.g., not inputting customer data into the AI system)*

04. Approval Date

PRO TIP

Think twice before covering every security practice as part of your AI policy. Your organization's existing information security policies likely already set expectations that apply to AI systems. For example:

- Acceptable Use Policy
- Access Control
- Configuration Management
- Data Management
- IT Asset Management
- Network Monitoring
- Security Awareness Training
- User Authentication
- Vendor Management

Rather than reinventing the wheel, your AI policy should define AI-specific requirements.

GUIDANCE

The FFIEC Information Security Booklet defines an acceptable use policy (AUP) as:

"A document that establishes an agreement between users and the enterprise and defines for all parties the ranges of use that are approved before users can gain access to a network or the internet."

The booklet goes on to state:

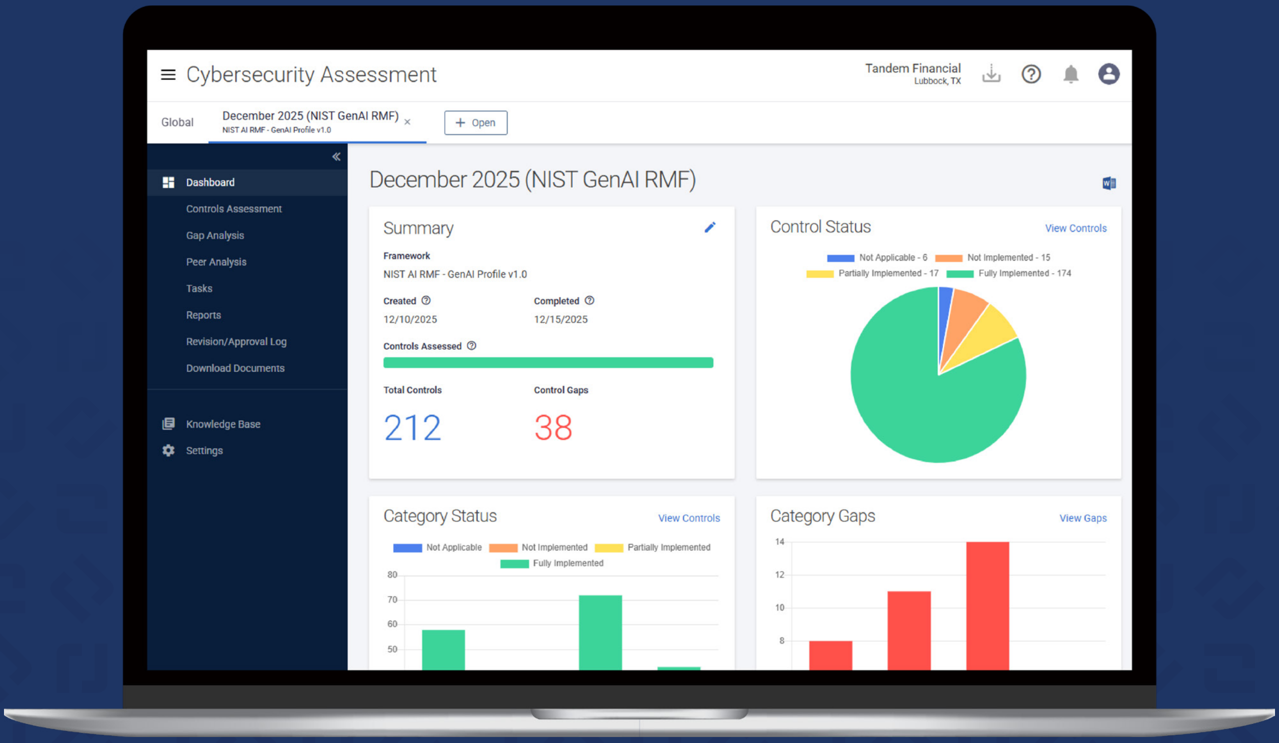
"The institution should collect signed acknowledgments of the employee acceptable use policy as part of the annual training program."

TANDEM TIP

For more details, check out the **Artificial Intelligence (AI)** customizable policy template in the Tandem Policies product.

Tandem Cybersecurity Assessment

Perform cybersecurity control self-assessments based on the NIST Artificial Intelligence Risk Management Frameworks (RMF).



December 2025 (NIST GenAI RMF)

Summary

Framework
NIST AI RMF - GenAI Profile v1.0

Created: 12/10/2025

Completed: 12/15/2025

Controls Assessed

Total Controls: 212

Control Gaps: 38

Control Status

Not Applicable - 6
Not Implemented - 15
Partially Implemented - 17
Fully Implemented - 174

Category Status

Category Gaps

If you are looking for guidance on which controls to implement, sign up for Tandem Cybersecurity Assessment to evaluate your controls against common frameworks, including the NIST AI RMF, NIST GenAI RMF, NIST Cybersecurity Framework, CIS Controls, CRI Profile, and more. Sign up for free to get started today.

TANDEM.APP/CYBERSECURITY

AI Vendor Management

To manage the risk of vendors who provide standalone or embedded AI systems, you must perform thorough due diligence. In addition to your existing vendor management procedures, consider the following AI-specific topics.

Worksheet

01. Which of the following best describes the vendor's AI model?

Knowing which model a vendor uses helps you understand whether they're running their own AI system or relying on a third-party solution, which in turn affects whether your data could be shared outside the vendor.

□ Internally-developed model

□ Third-party-developed model

□ Other (explain) ______________________________

□ Open-source model

□ Hybrid model

02. How is the vendor's AI model trained?

Knowing how a model is trained is important, as each approach carries different levels of risk. Understanding whether it's trained on your organization's data, other organizations' data, user inputs, or its own data helps determine how to interpret and rely on its outputs.

□ Large public datasets

□ Proprietary datasets owned by the vendor or its clients

□ Inputs provided by system users

□ Anonymized datasets

□ Self-supervised learning on the model's own outputs

□ Other (explain) ______________________________

03. Can the organization opt out of participating in model training?

□ Yes, fully □ Yes, partially □ No, not at all

04. How is the AI system and data hosted?

□ Locally ("on-premises")

□ Private cloud

□ Other (explain) ______________________________

□ Community cloud

□ Public cloud

PRO TIP

To answer these questions, you may need to review the vendor's publicly available documentation or consult with the vendor.

Understanding how a vendor's AI model is built and trained isn't just a formality. It's critical to keeping your data safe.

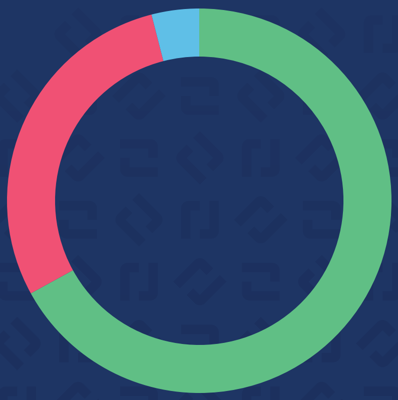
If the vendor cannot or will not provide the information you need, that's a warning signal. It doesn't necessarily mean you can't work with them, but it is something to monitor.

LEARN MORE

Discover the foundations of third-party risk management at Tandem.App/Vendor-Workbook.

BY THE NUMBERS

Two-thirds of financial institutions evaluate AI use as part of their vendor management program.



● Yes (67%)

● No (29%)

● Unknown (4%)

SOURCE
2025 State of Cybersecurity Report

TANDEM TIP

Check out the **Artificial Intelligence (AI) Vendor Review** in the Tandem Vendor Management product for more details.

05. What controls has the vendor implemented to protect the model from biased, malicious, or unauthorized input?

AI models are susceptible to a variety of threats (e.g., scripting, prompt injection, training data manipulation, targeted poisoning, backdooring, etc.). As a result, the vendor needs to implement controls to protect the model, like the following.

- □ Data sanitization
- □ Input validation
- □ Anomaly detection
- □ Quality assurance
- □ Access controls
- □ Ongoing monitoring
- □ Human oversight
- □ Staff training
- □ Other (explain) ____________________

06. Which of the following methods are used to validate the AI model?

Model validation is a fancy way of saying "making sure the AI does its job correctly." Validation can be performed by the vendor, the organization, or both. Vendors often handle the more technical aspects and may provide certifications or evidence of testing, but the ultimate responsibility for the accuracy and reliability of AI outputs rests with the organization. The more critical the system, the more thoroughly the model needs to be validated.

- □ Professional review *(e.g., an expert assesses the results for accuracy)*
- □ Historical comparison *(e.g., comparing current results with previous results)*
- □ Model benchmarking *(e.g., comparing outputs from multiple models)*
- □ Confidence scores *(e.g., ensuring outputs fall into an approved confidence range)*
- □ Outlier detection *(e.g., alerting of outputs which fall outside an approved range)*
- □ Random sampling *(e.g., selecting a subset of data from a larger dataset to review)*
- □ Other (explain) ____________________

07. How often is model validation performed for the AI system?

○ Less than Annually ○ Annually ○ Semiannually ○ Quarterly ○ Monthly ○ Weekly ○ Daily ○ As Needed

08. What does the vendor's privacy policy say about how they will access, use, store, retain, and share your data?

09. Who are the vendor's business partners (a.k.a., fourth parties, subcontractors) who might access your data?

AI Training

People are often the biggest source of risk when it comes to AI. To manage this risk, training and awareness are key controls.

Worksheet

01. What types of training are provided to employees on use of AI?

- □ Initial / ongoing system training
- □ System instructions / manuals
- □ Acceptable use policy
- □ Nondisclosure agreements
- □ Security awareness training
- □ AI-specific awareness training
- □ Other (explain) ____________________

02. What topics are covered by your AI training materials?

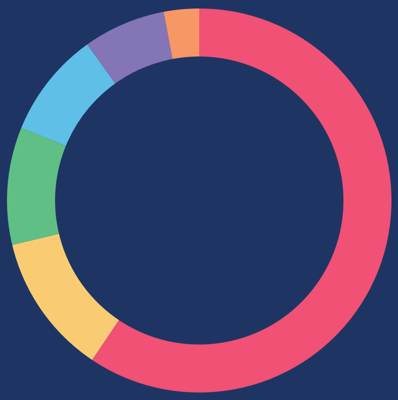
- □ AI capabilities and limitations
- □ AI security risks (e.g., data leakage, phishing, deepfakes)
- □ Approved and prohibited AI systems
- □ Approved and prohibited AI use cases
- □ How to request new AI systems or use cases
- □ How to keep personal AI systems separate from work systems
- □ How to verify and validate AI outputs
- □ How to detect and respond to AI incidents
- □ How to report AI concerns or issues
- □ Other (explain) ____________________

03. How often are employees trained on AI?

○ Weekly ○ Monthly ○ Quarterly ○ Semiannually ○ Annually ○ As Needed

BY THE NUMBERS

60% of financial institutions say data leakage is their biggest concern with using AI.



- ● Data Leakage (60%)
- ● Content Accuracy (12%)
- ● Lack of Governance (10%)
- ● Legal or Compliance (9%)
- ● Missed Opportunities (7%)
- ● Staff Overreliance (3%)

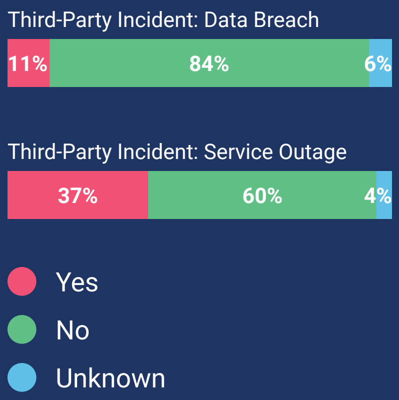
SOURCE
2025 State of Cybersecurity Report

TANDEM TIP

For more details, check out the **Artificial Intelligence (AI)** security awareness training course that comes with the Tandem Policies and Tandem Phishing products.

BY THE NUMBERS

Over the past year, one in ten financial institutions reported a third-party data breach and more than one-third reported a service outage caused by a third-party incident.


Third-Party Incident: Data Breach

Third-Party Incident: Service Outage

SOURCE
2025 State of Cybersecurity Report

PRO TIP

To evaluate whether your incident response team is prepared to handle AI-related incidents, consider hosting a tabletop exercise using an AI-based scenario.

Discover how you can host a great tabletop exercise at Tandem.App/Tabletop-Webinar.

TANDEM TIP

For more details, check out our **Action Plans** and **Deepfake Tabletop Scenarios** in the Tandem Incident Management product.

AI Incidents

Things don't always go as expected. That's why having a clear incident response plan is essential. Here are common AI-related incident scenarios. Consider if any of these have occurred at your organization.

- An employee puts confidential data into an unapproved AI system
- An employee integrates an unapproved AI notetaking app
- An employee falls victim to a social engineering deepfake attack
- An employee accesses unauthorized resources via the AI system
- An employee uses inaccurate AI-generated content without review
- An AI system returns inaccurate or unexpected results
- An AI system inadvertently exposes confidential data
- An AI system experiences a service outage disrupting business
- An AI system misuses an employee's privileged access permissions

While it is impossible to plan for every potential incident, an incident response plan should address the underlying risks by outlining steps to prevent, detect, and respond to common types of incidents.

Worksheet

01. What types of incidents does your incident response plan address?

□ Data breaches
□ Social engineering
□ Other (explain) ____________________
□ System failures
□ Third-party incidents

02. Is the incident response team prepared to handle AI-related incidents?

□ Yes, fully □ Yes, partially □ No, not at all

03. Who should employees contact if they have an AI-related incident?

____

AI Monitoring and Reporting

Ongoing monitoring of AI is an evolving challenge, but that doesn't mean it should be ignored. Regular tracking and reporting are essential for managing risk and keeping leadership informed.

Worksheet

01. How do you plan to monitor for use of unapproved AI systems (a.k.a., "shadow IT" or "shadow AI")?

- □ Monitor network traffic
- □ Review software installations
- □ Review third-party app integrations
- □ Ask auditors to assess AI usage
- □ Ask about AI during vendor onboarding
- □ Ask about AI during business impact analysis (BIA)
- □ Conduct regular employee surveys
- □ Encourage self-reporting of AI use
- □ Other (explain) ____________________

02. How do you plan to monitor for unauthorized use of approved AI systems?

Directly monitoring every user input is generally not feasible, and the ability to monitor for unauthorized use depends on the AI system's configuration and deployment, whether it's an enterprise-approved standalone tool or an embedded AI feature within another application.

03. How often are AI system access permissions reviewed?

○ Annually ○ Semiannually ○ Quarterly ○ Monthly ○ As Needed ○ Never

04. Which of the following AI-related topics do you include in your report to the Board?

- □ Approved and prohibited AI systems
- □ Approved and prohibited AI use cases
- □ AI risk assessment results
- □ AI policy
- □ AI vendor management results
- □ AI training and awareness initiatives
- □ AI incidents
- □ AI monitoring results
- □ Other (explain) ____________________

WANT TO LEARN MORE?

Watch a video of Tandem's AI risk management features in action at Tandem.App/AI-Features-Demo.

About Tandem

WHO WE ARE

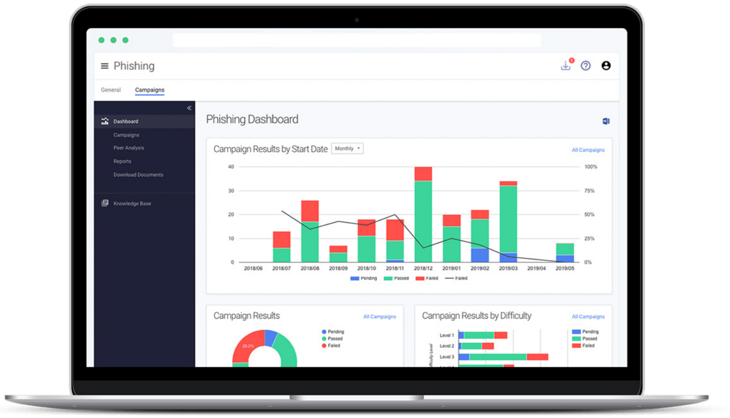
Financial institutions of all sizes struggle with the burden of information security compliance. Tandem grew out of the confidence that we can ease this burden.

First, we supported our clients by helping them maintain their documents, but it didn't take long to decide that a software solution could help more people, faster. In 2007, we began developing the do-it-yourself compliance application for information security, now known as Tandem.

We named our product Tandem because it works in partnership - in tandem - with you. You bring your knowledge of your organization and your needs. We bring software built by information security experts to help you create, organize, and manage your information security program.

We believe you have what it takes to manage information security and regulatory compliance. With the right tool, you can do it fast.

Learn more about how Tandem can help you at Tandem.App.



OUR PRODUCTS

- Audit Management
- Business Continuity Plan
- Compliance Management
- Cybersecurity Assessment
- Identity Theft Prevention
- Incident Management
- Internet Banking Security
- Phishing
- Policies
- Risk Assessment
- Vendor Management

Tandem®

info@tandem.app
844-698-9800