WELCOME TO

How to Write an AI Policy

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

Tandem

DISCLAIMER

- **This presentation is for information only.**
  Evaluate risks before acting on ideas from this session.

- **This presentation contains opinions of the presenters.**
  Opinions may not reflect the opinions of Tandem.

- **This presentation is proprietary.**
  Unauthorized release of this information is prohibited.
  Original material is copyright © 2025 Tandem.

Tandem

SESSION INFO

AUDIO/VIDEO

If you cannot hear sound or see the presentation now, adjust or change your settings.

SURVEY

At the end, fill out the survey for a chance to win an Amazon gift card.

RESOURCES

The slides, a recording, and certificate of attendance will be sent via email.

QUESTIONS

Use the “Questions” panel to chat with the presenters and Tandem team.

Tandem

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

Tandem™

A CoNetrix company

POLL QUESTION

What type of organization do you currently work for?

Tandem

POLL QUESTION

What is your organization’s asset size?

Tandem

Session Topics

- What Makes a Good AI Policy?
- Defining the Scope
- Core AI Policy Elements
- Tandem Policies Demo
- Wrap Up & Resources

Tandem

What Makes a Good AI Policy?

Tandem

AI isn’t just a trend.
It’s becoming a core part of how businesses operate.

Tandem

WHAT MAKES A GOOD AI POLICY?

Scope	+	Use Cases
Governance	+	Accountability
Vendor Management	+	Security Practices
Acceptable Use	+	Training

A clear policy sets boundaries, builds trust, and supports safe innovation.

Tandem

POLL QUESTION

Does your organization currently have an AI policy in place?

Tandem

Defining the Scope

Tandem

DEFINING THE SCOPE

- ? In-House or Outsourced
- ? Operationally Critical or Significant
- ? Restricted, Private, or Public Data
- ? Departments and Use Cases

Tandem

POLL QUESTION

How is AI currently being used in your organization?

Tandem

Governance & Accountability

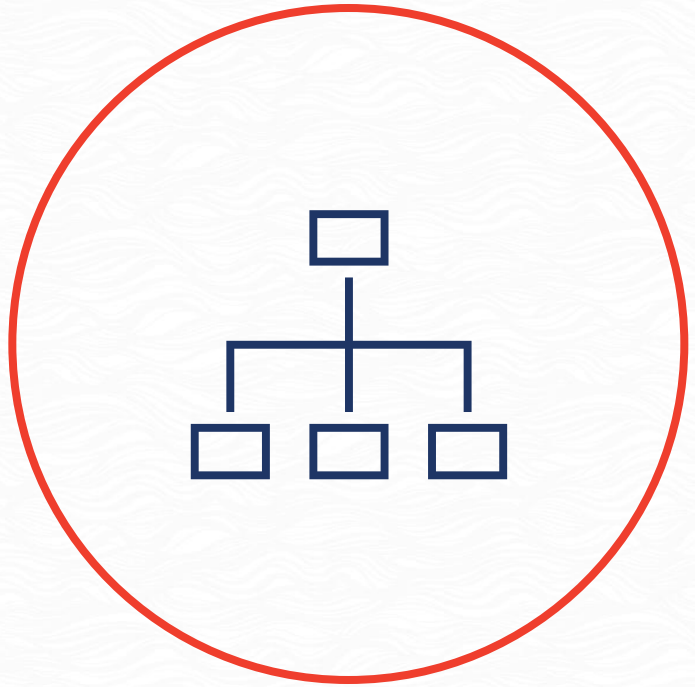
Tandem

POLL QUESTION

Who currently oversees AI use at your organization?

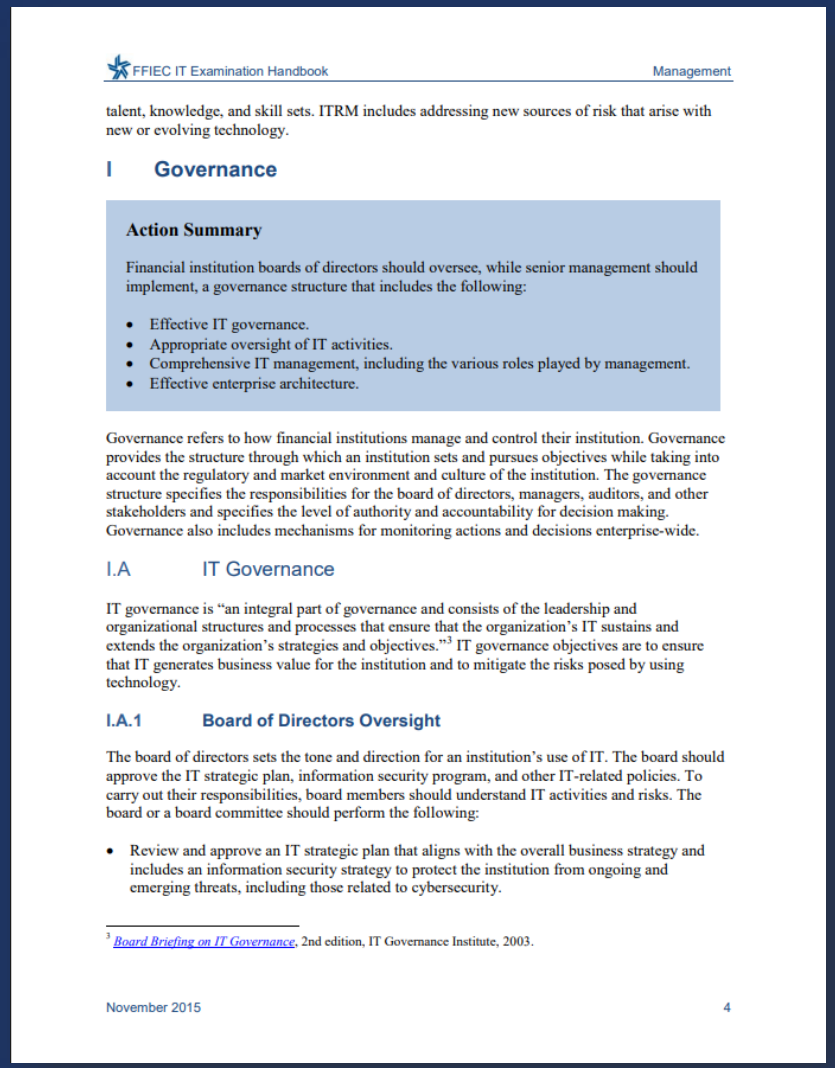
Tandem

Governance



Accountability

GOVERNANCE & ACCOUNTABILITY



talent, knowledge, and skill sets. ITRM includes addressing new sources of risk that arise with new or evolving technology.

I Governance

Action Summary

Financial institution boards of directors should oversee, while senior management should implement, a governance structure that includes the following:

- Effective IT governance.
- Appropriate oversight of IT activities.
- Comprehensive IT management, including the various roles played by management.
- Effective enterprise architecture.

Governance refers to how financial institutions manage and control their institution. Governance provides the structure through which an institution sets and pursues objectives while taking into account the regulatory and market environment and culture of the institution. The governance structure specifies the responsibilities for the board of directors, managers, auditors, and other stakeholders and specifies the level of authority and accountability for decision making. Governance also includes mechanisms for monitoring actions and decisions enterprise-wide.

I.A IT Governance

IT governance is "an integral part of governance and consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives."[3] IT governance objectives are to ensure that IT generates business value for the institution and to mitigate the risks posed by using technology.

I.A.1 Board of Directors Oversight

The board of directors sets the tone and direction for an institution's use of IT. The board should approve the IT strategic plan, information security program, and other IT-related policies. To carry out their responsibilities, board members should understand IT activities and risks. The board or a board committee should perform the following:

- Review and approve an IT strategic plan that aligns with the overall business strategy and includes an information security strategy to protect the institution from ongoing and emerging threats, including those related to cybersecurity.

[3] *Board Briefing on IT Governance*, 2nd edition, IT Governance Institute, 2003.

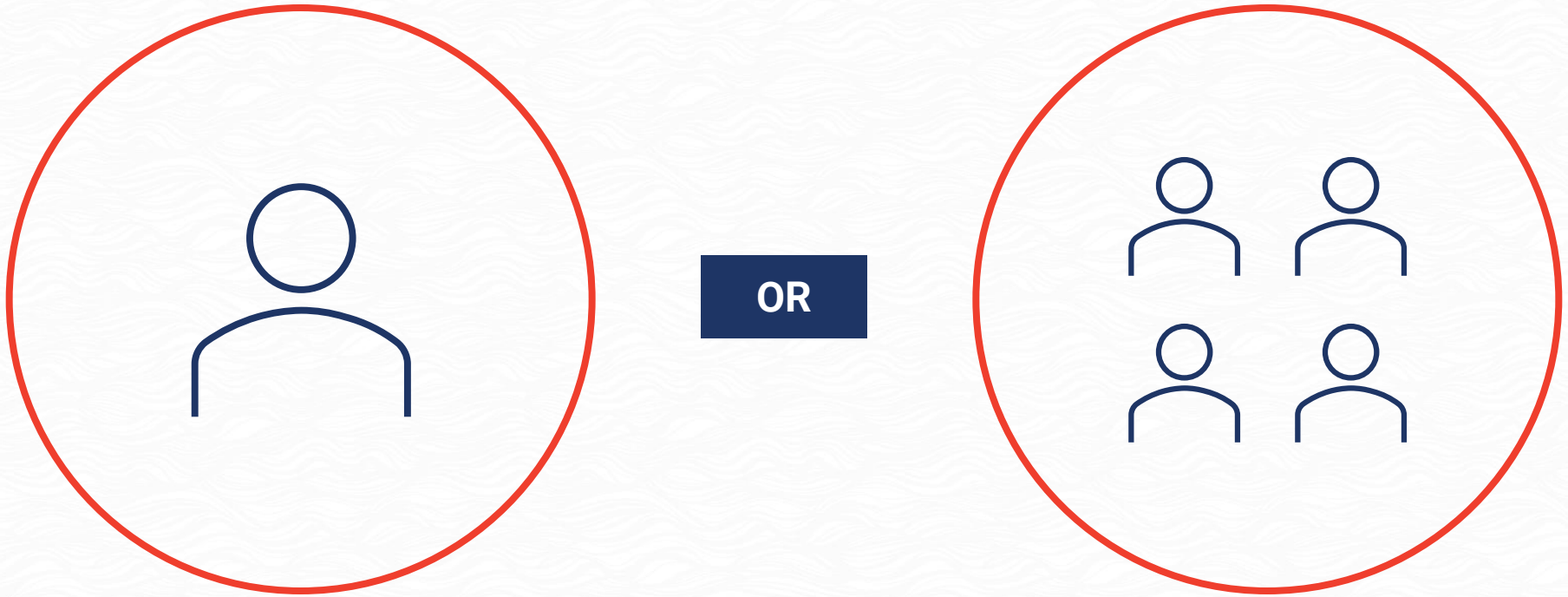
https://ithandbook.ffiec.gov/it-booklets/management/i-governance/

"IT governance is "an integral part of governance and consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives." IT governance objectives are to ensure that IT generates business value for the institution and to mitigate the risks posed by using technology."

FFIEC Management Booklet

Tandem

GOVERNANCE & ACCOUNTABILITY | OWNERSHIP



Tandem

RESPONSIBILITIES & FUNCTIONS

? Who approves the use of new AI tools?

? Who ensures vendor assessments are completed?

? Who is responsible for monitoring ethical and legal concerns?

Tandem

Vendor Management

Tandem™

WHAT DO YOU MEAN "VENDOR MANAGEMENT?"

Outsourced

In-House

Tandem

POLL QUESTION

Do you include outsourced AI systems in your vendor management program?

Tandem

OUTSOURCED AI SYSTEMS

- ☑ Microsoft CoPilot
- ☑ OpenAI ChatGPT
- ☑ Anthropic Claude
- ☑ Perplexity
- ☑ X Grok
- ☑ MetaAI
- ☑ Google Gemini, Duet, or AI Mode
- ☑ Apple Intelligence
- ☑ DeepSeek
- ☑ Other Integrated AI Systems

Tandem

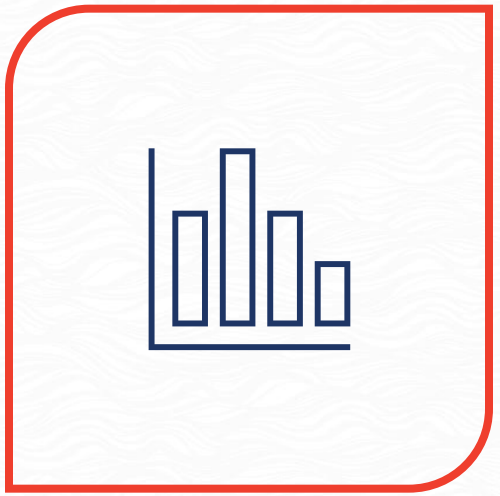
POLL QUESTION

How many of these AI systems does your organization use?

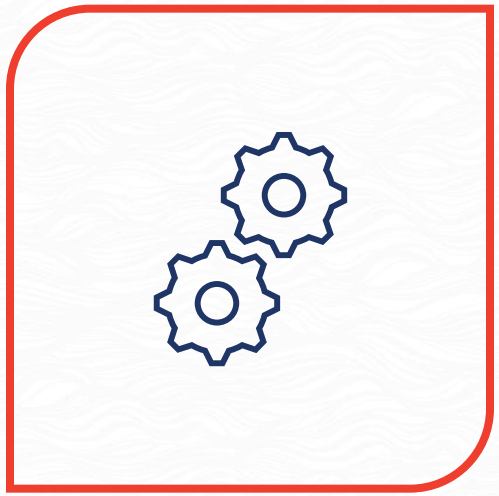
Tandem

DETERMINING AI TOOL CRITICALITY

License Type



Data Type



Function Type

Tandem

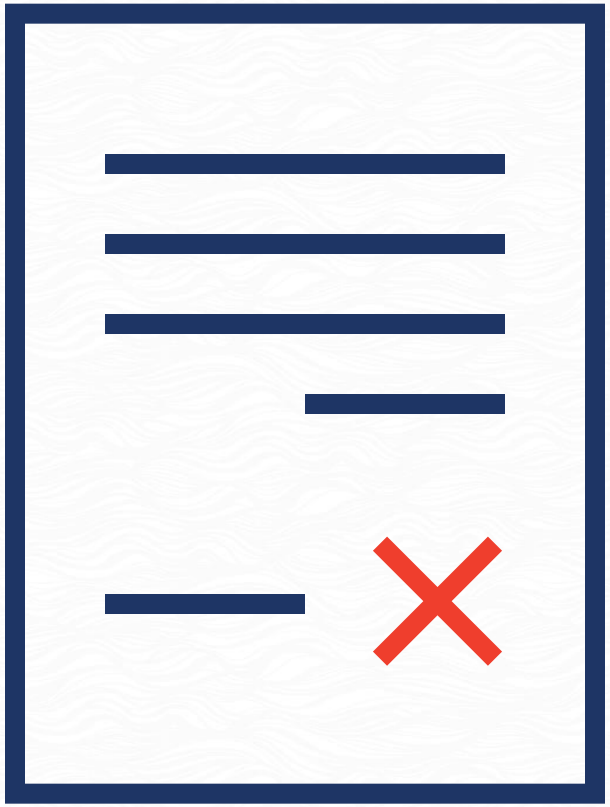
EVALUATION & ONGOING MONITORING

"Determine how the vendor accesses, processes, and secures input data."

"Evaluate how the AI model is trained, validated, and maintained."

"Monitor the AI vendor's activity, performance, uptime, and security."

Tandem



- Transparency
- Bias and Fairness
- Model Lifecycle
- Liability

Leverage Existing Security Policies

Tandem

ACCESS CONTROL POLICY

1. Not everyone should have equal access to AI systems.
2. AI systems may introduce new or existing access risks.
3. Clear access roles create accountability.

Tandem

IT ASSET MANAGEMENT POLICY

1. How AI tools are identified, inventoried, and approved for use
2. If personal or unvetted tools are allowed for business purposes
3. How AI system integrations are tracked and controlled

Tandem

DATA PROTECTION POLICY

1. Define what data is appropriate for AI tools.
2. Address encryption and anonymization.
3. Clarify what happens to data after it’s processed.

Tandem

MONITORING & LOGGING POLICY

1. Track who is using AI tools and how they're being used.
2. Monitor what data is being entered.
3. Watch for anomalies or risky behavior.
4. Review AI output before acting on it.

Tandem

INCIDENT MANAGEMENT POLICY

1. AI-related incidents should be reported.
2. Teams need guidance on how to respond to AI-related issues.
3. Post-incident reviews should evaluate AI use.

Tandem

Writing an AI policy doesn’t mean starting from scratch. It’s about reinforcing what’s already working and connecting the dots.

Use what makes sense for your environment.

Tandem

SUBMIT YOUR QUESTIONS!

Tandem

Acceptable Use & Training

Tandem

SETTING EXPECTATIONS FOR EVERYDAY AI USE

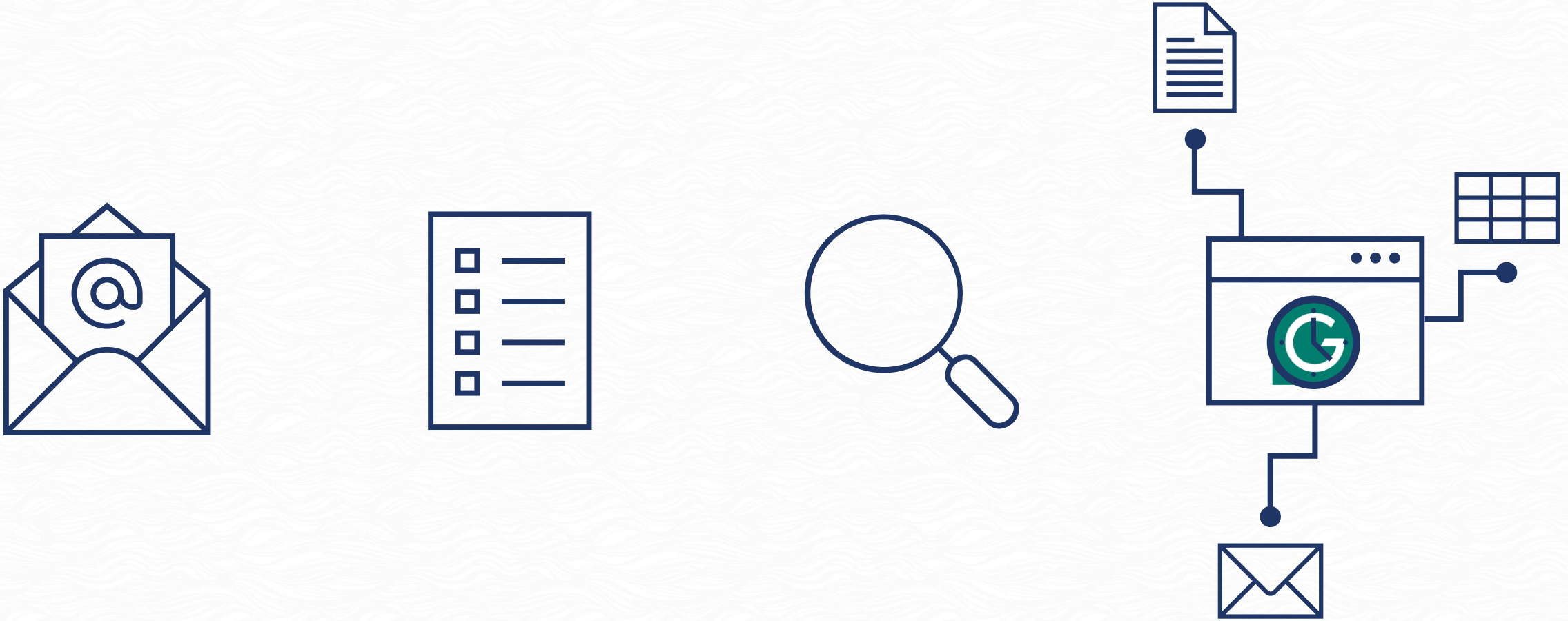
Define What Is and Is Not Allowed

Set Boundaries for High-Risk Use

Perform AI Security Awareness Training

Tandem

EXAMPLE: GRAMMARLY PRIVACY POLICY



Tandem

EXAMPLE: GRAMMARLY PRIVACY POLICY

When it comes to user content, by default, we process user content associated with your account to provide services to you (for example, writing suggestions, customization, and insights on how to use our features). For troubleshooting and product improvement, we typically retain user content for no longer than one year, after which we either delete or de-identify the content unless you choose to retain it in your account for longer or specifically ask us to delete it sooner, subject to any legal obligations requiring us to maintain the content for a longer period. We also pseudonymize, aggregate, and/or de-identify data and content when providing our services to you as described in our Technical Specifications. With the Grammarly Editor, we will store documents you create until you delete them or we close your account.

https://www.grammarly.com/privacy-policy

Tandem

POLL QUESTION

Does your Acceptable Use Policy address use of AI tools?

Tandem

POLL QUESTION

Does your security awareness training include AI topics?

Tandem

Keep It Simple & Straightforward

Tandem™

K . I . S . S .

1

Fit Your Organization

2

Cover the Essentials

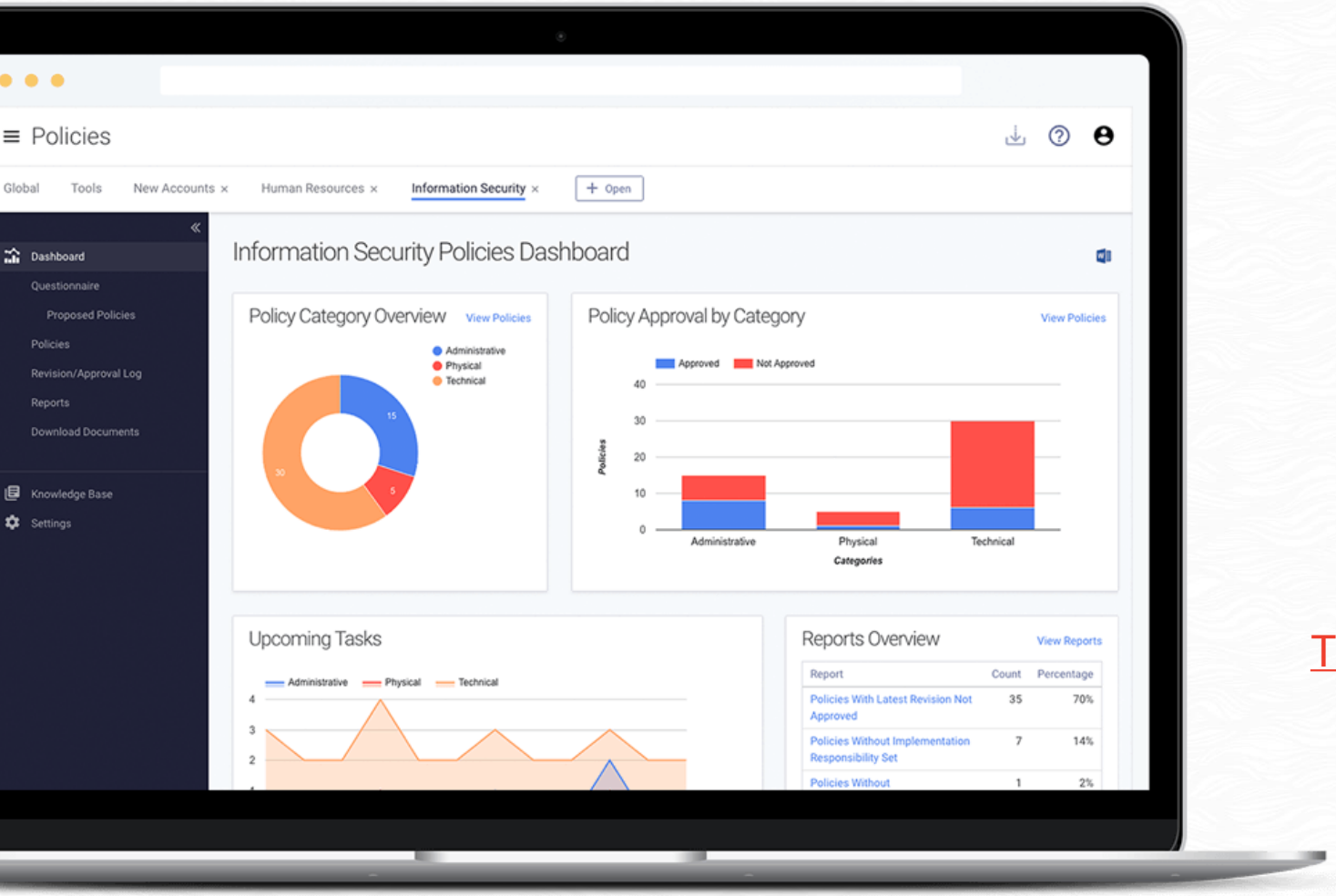
3

Build from Existing

4

Be Useful for People

Tandem



LEARN MORE

Tandem Policies Software

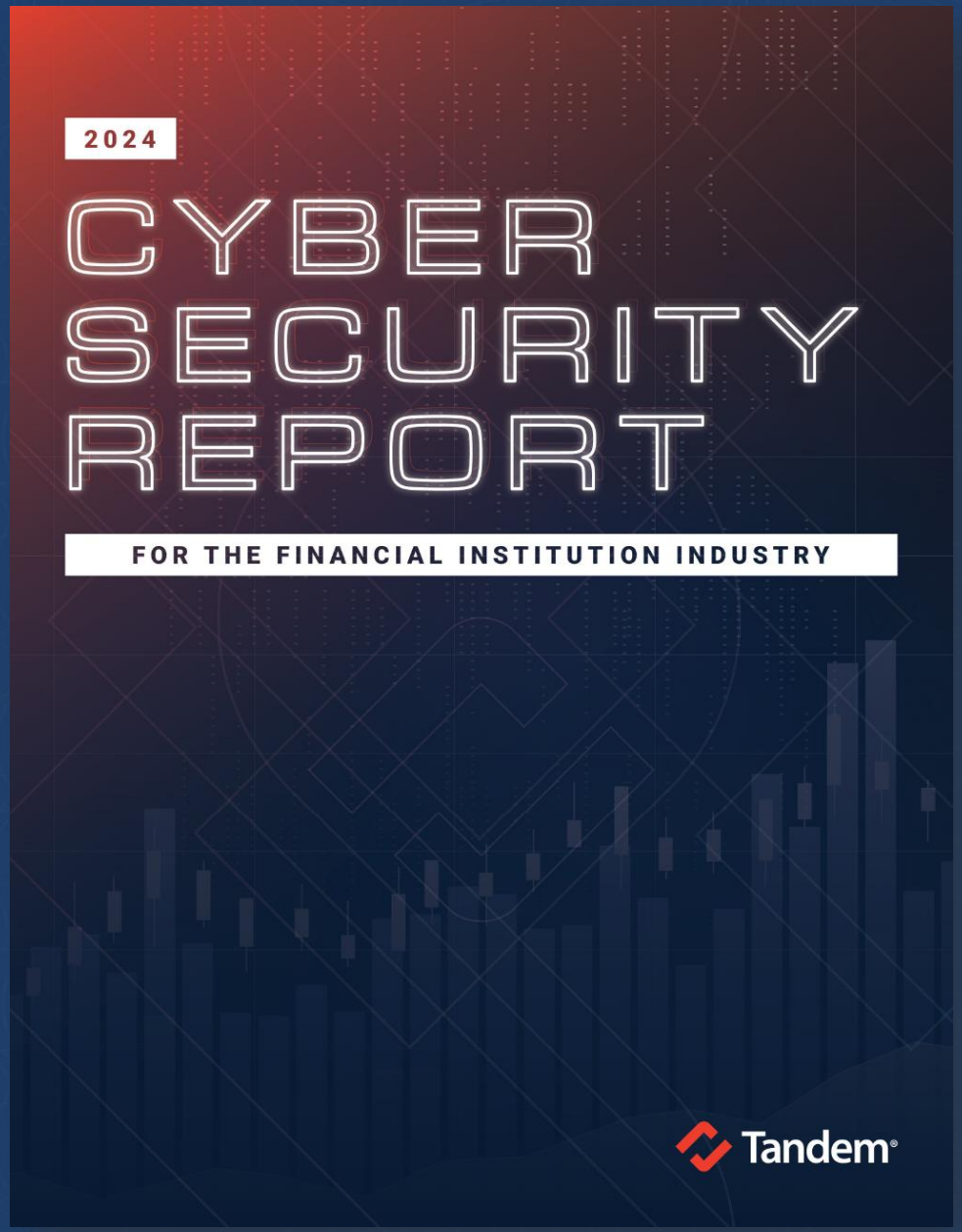
Tandem.App/Policies-Management-Software

SUBMIT YOUR QUESTIONS!

Tandem

Fill out the survey for a chance to win!

Tandem

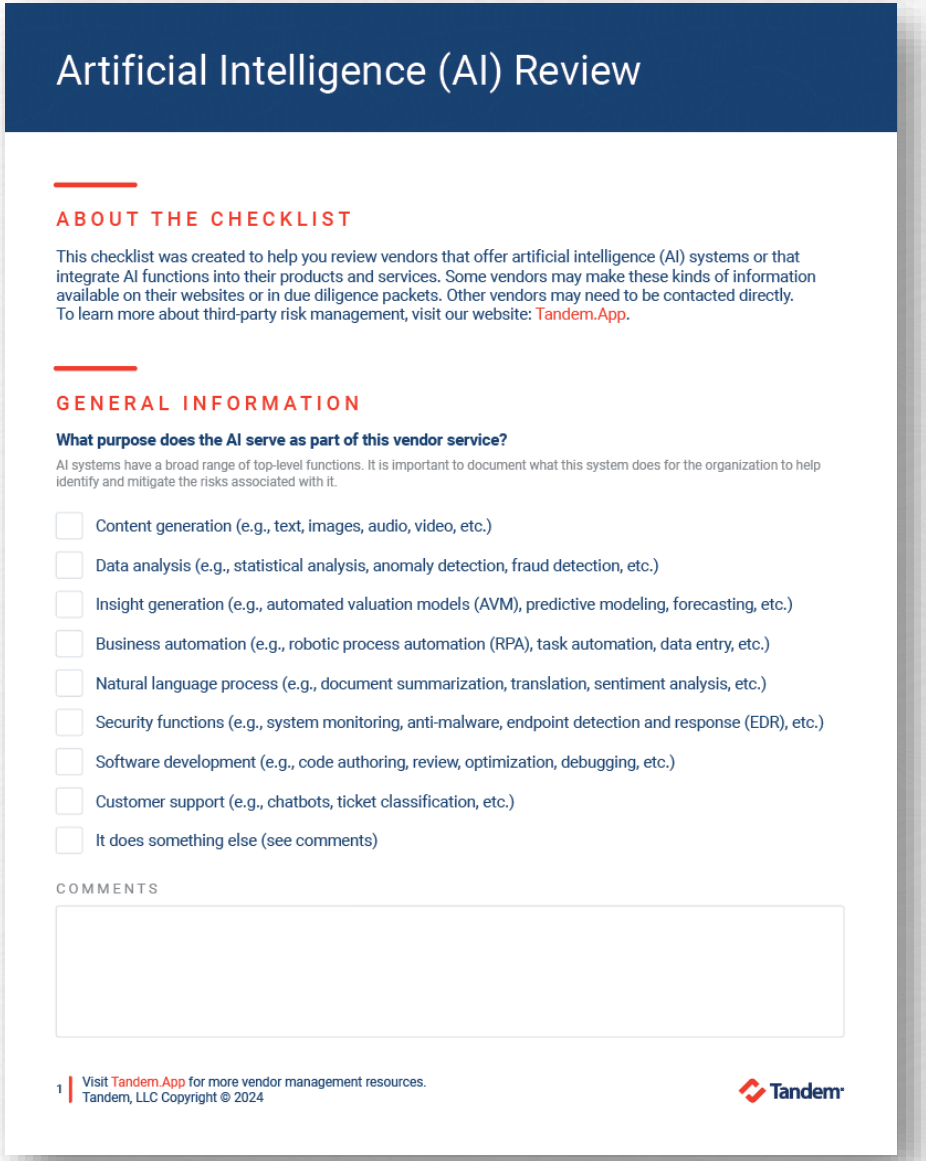


CYBER REPORT

Be Part of the 2025 State of Cybersecurity Survey

Tandem.App/Survey

Tandem



Artificial Intelligence (AI) Review

ABOUT THE CHECKLIST

This checklist was created to help you review vendors that offer artificial intelligence (AI) systems or that integrate AI functions into their products and services. Some vendors may make these kinds of information available on their websites or in due diligence packets. Other vendors may need to be contacted directly. To learn more about third-party risk management, visit our website: Tandem.App.

GENERAL INFORMATION

What purpose does the AI serve as part of this vendor service?

AI systems have a broad range of top-level functions. It is important to document what this system does for the organization to help identify and mitigate the risks associated with it.

- [ ] Content generation (e.g., text, images, audio, video, etc.)
- [ ] Data analysis (e.g., statistical analysis, anomaly detection, fraud detection, etc.)
- [ ] Insight generation (e.g., automated valuation models (AVM), predictive modeling, forecasting, etc.)
- [ ] Business automation (e.g., robotic process automation (RPA), task automation, data entry, etc.)
- [ ] Natural language process (e.g., document summarization, translation, sentiment analysis, etc.)
- [ ] Security functions (e.g., system monitoring, anti-malware, endpoint detection and response (EDR), etc.)
- [ ] Software development (e.g., code authoring, review, optimization, debugging, etc.)
- [ ] Customer support (e.g., chatbots, ticket classification, etc.)
- [ ] It does something else (see comments)

COMMENTS

Tandem, LLC Copyright © 2024

Tandem

FREE RESOURCE

Artificial Intelligence (AI) Vendor Review Checklist

Tandem.App/AI-Review-Checklist

Tandem

THANKS FOR JOINING

How to Write an AI Policy

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

Tandem