Cybersecurity Governance for Pension Funds in the Age of AI

Webinar

October 18, 2023

NATIONAL INSTITUTE ON
Retirement Security
Reliable Research. Sensible Solutions.

Speakers

Tyler Bond

Research Director,
NIRS

Andrew Roth

Deputy Director
Teacher Retirement System of Texas

Peter Dewar

President
Linea Secure

Nate Haws

Associate Principal Consultant
Linea Solutions

Agenda

- Logistics and Introductions
- AI for Organizational Use
- Texas TRS AI Initiatives
- AI Cybersecurity Risk Landscape
- AI Organizational Governance Frameworks
- Use Case Demonstration
- Q&A

• AI for Organizational Use

- Generative AI is still a work in progress
- AI has the potential to decrease the **digital debt** and give us more time to be productive and creative
  - Workers spend 57% of workday communicating
  - 68% of people say they don’t have enough uninterrupted focus time during the workday
- **Using AI is a skill** just like learning to use a language
- Organizations can utilize it by **creating a Culture of AI**

Source: The 2023 Microsoft Work Trend Index

Creating a Culture of AI

Summary Steps

1. Assemble AI Team
2. Create Governance Charter
3. Create AI Use Policy
4. Understand Opportunities
5. Build Excitement
6. Refine Use Cases
7. Train
8. Iterate
9. Maintain

POLL QUESTION 1

Do you have an AI governance framework in place at your fund?

1. Yes
2. No

Texas TRS AI initiatives

Use Cases: Benefits

- Customer service: Call center, Chat
- Answer simple member inquiries

Use Cases: Investments

- Multi-Strategies Group
- Public Markets

Use Cases: Health

- Claims analysis (medical and pharmacy)
- Trend analysis

Artificial Intelligence at TRS: Risks

Risks:

- Unauthorized use or disclosure of sensitive or confidential information
- Fraud
- Bias
- Inaccurate information
- Violation of others' legal rights (to privacy, intellectual property, etc.
- Safety and Security
- Third-party risk

Artificial Intelligence at TRS: Governance

AI Policy

- Acknowledges potential value of AI to TRS; the need to use AI ethically and responsibly; and that AI use creates risk
- Covers use of both machine learning and generative AI tools
- Outlines a process for reviewing approving use of tools and systems with AI components
- Covers use of third-party tools and systems
- Envisions a cross-functional, multi-disciplinary AI Review Team; includes IT, IS, L&C, Records; and SMEs as appropriate

References

- NIST AI Management Framework and NIST Trustworthy and Responsible AI Resource Center
- HIPPAA
- TX Government Code
- US Copyright Act
- White House AI Bill of Rights

AI Cybersecurity Risk Landscape

- Shadow adoption
- Exposure of PII
- Reliability and provenance (models ‘hallucinate’ and can use sources without attribution)
- More advanced phishing

POLL QUESTION 2

Which AI cyber risk are you most concerned about?

1. Shadow adoption
2. Exposure of PII
3. Reliability and provenance
4. More advanced phishing
5. Other (write-in)

AI Cybersecurity Risk Landscape

Usage of AI technology may occur before a detailed risk analysis can occur

Ways to mitigate:

- Limit usage
- Awareness training for digital trust
- Improve verification
- Maintain a record of usage

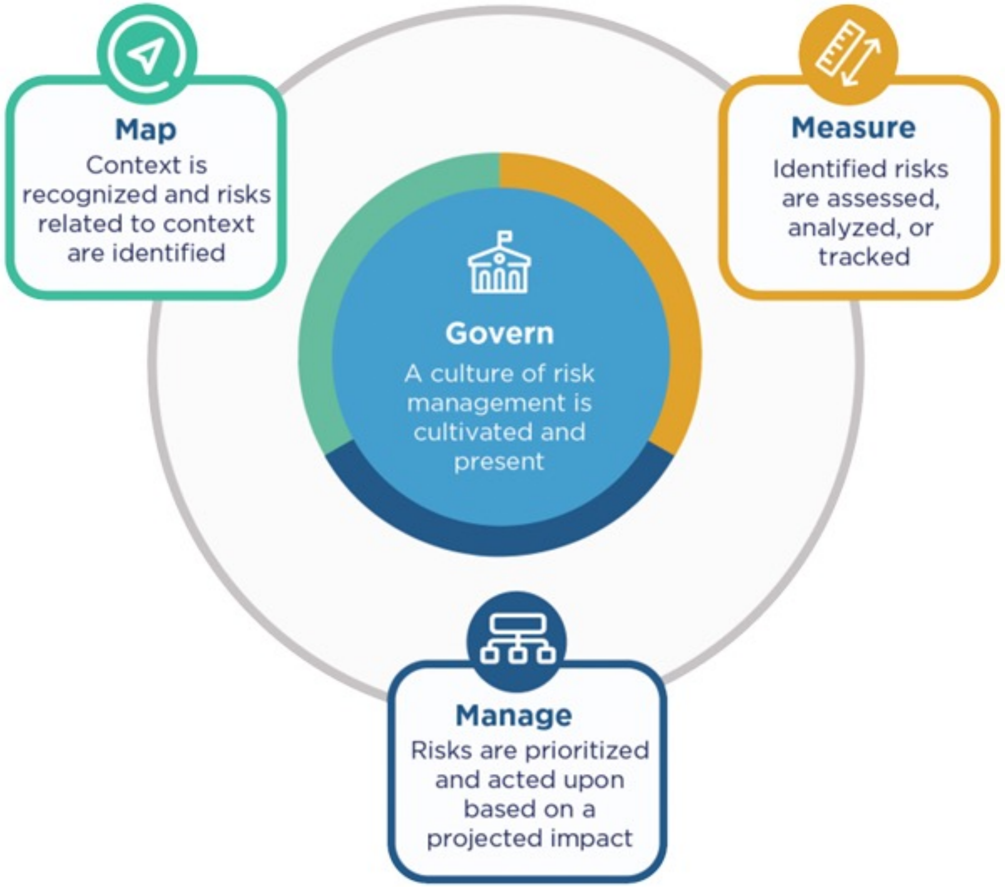
National Institute of Standards & Technology

- Founded 1901 – is one of the nation's oldest physical science laboratories
- **Created a Cyber Security Framework (CSF) for protecting privacy of information systems**
- CSF Issued in 2014 – helps organizations to better understand, manage, and reduce their cybersecurity risks
- **Identifies which activities are most important to focus on**
- Provides a common language to address cybersecurity risk management
- Especially helpful in communicating inside and outside the organization
- Can be used to identify opportunities for improving cybersecurity posture
- Allows for a maturity process
- The Framework balances comprehensive risk management with cost
- **Will help to prioritize investments and maximize the impact of each dollar spent on cybersecurity**

NIST AI Risk Management Framework (RMF)

- Organizations need to perform an **overall risk assessment** to understand how AI adoption would impact them
- Develop AI actors within the org with **test, evaluation, verification, and validation** (TEVV) expertise
- Use **trustworthy AI systems** only:
    - Valid and reliable, safe, secure and resilient, accountable and transparent, explainable and interpretable, privacy-enhanced, and fair with harmful bias managed
- Share knowledge with other organizations to **develop industry best practices**
- Follow the **AI RMF Core**

NIST AI RMF Core



Map
Context is recognized and risks related to context are identified

Measure
Identified risks are assessed, analyzed, or tracked

Govern
A culture of risk management is cultivated and present

Manage
Risks are prioritized and acted upon based on a projected impact

Use Case Demonstration

Questions