



2026 Annual Conference & Expo

Navigating AI Risk in Fintech Innovation

An internal audit perspective for credit unions

JUNE 18, 2026

PRESENTED BY

Joseph A. Zito, CPA, MBA – Principal, Financial Institutions Group

Lindsey Becker, CRCM – Senior Manager Internal Audit, Financial Institutions Group



"Doeren Mayhew" is the brand name under which Doeren Mayhew Assurance and Doeren Mayhew Advisors, LLC and its subsidiary entities provide professional services. Doeren Mayhew Assurance and Doeren Mayhew Advisors, LLC (and its subsidiary entities) practice as an alternative practice structure in accordance with the AICPA Code of Professional Conduct and applicable law, regulations and professional standards. Doeren Mayhew Assurance is a licensed independent CPA firm that provides attest services to its clients, and Doeren Mayhew Advisors, LLC and its subsidiary entities provide tax and business consulting services to their clients. Doeren Mayhew Advisors, LLC and its subsidiary entities are not licensed CPA firms.



Learning Objectives

- Define artificial intelligence (AI) and inform on various fintech companies and products in the industry
- AI and data analytics presents a transformative potential for credit unions and their internal audit departments. Benefits and risks will be outlined whether they have the use or not of fintech companies.
- Risks and controls for managing AI will be discussed utilizing the recently released COSO practical roadmap and guidance



Artificial Intelligence: What is it?

AI Defined

“The capability of computer systems or algorithms to imitate intelligent human behavior”.

- Merriam-Webster Dictionary

It's been around since the '50s

- Developing more and more over time – digital disruptors
- Some recent AI related products we use regularly
 - Siri
 - Teams
 - Alexa
 - Email spam filters
 - Chat boxes
 - Online shopping recommendations/feeds



Types of AI

Machine Learning (ML)

- 🖥️ Uses algorithms to more accurately predict outcomes.
- 🖥️ Models are locked based on a large dataset input and do not learn on their own.
- 🖥️ Decisions are transparent and consistent.
- 🖥️ Can be used in fraud detection and credit underwriting decisions.

Large Language Models (LLM)

- 🖥️ Sophisticated type of AI model that excels at understanding and generating natural language, or human-like, text.
- 🖥️ Models are "large" due to the vast amount of data they are trained on and their complex neural network structure.

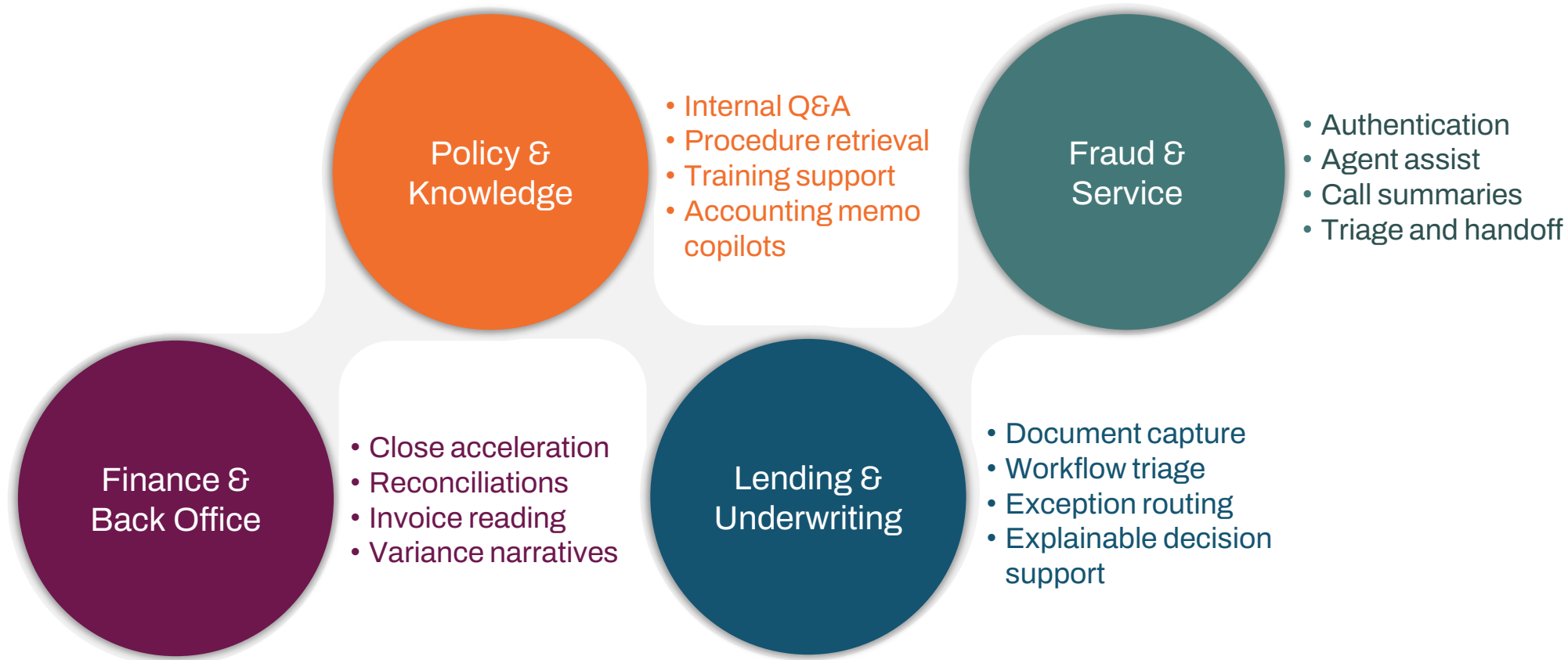
Types of AI

Generative AI (GenAI)

- 🖥️ Can create new content from various data sources (text, images, videos, audio), vs. prescribed outputs with ML, and can keep learning based on new inputs.
- 🖥️ Works by learning patterns from large datasets and then generating novel content that resembles the learned patterns.
- 🖥️ Used for chatbots and intelligence reporting.
- 🖥️ Can be used in fraud detection and credit underwriting decisions.
- 🖥️ Can create efficiencies but not created to make decisions on its own.
- 🖥️ Needs more human due diligence.

Where Value is Real Today

Credit Union and Fintech



Fiserv Collaboration with OpenAI & Amazon Web Services

- agentOS, an agentic AI operating system designed to help automate manual tasks directly within FiServ's platforms
- Key features
 - AI agent marketplace (build/deploy third-party AI agents)
 - Workflow automation (commercial loan onboarding, deposit intelligence and AML triage)
 - Enterprise-level security; operates on Amazon Bedrock and integrates with OpenAI
 - Ensures models meet strict banking security and governance standards
- Fiserv has co-developed AI agents with six of its partners and nine software companies have signed up to create AI agents for agentOS



COSO Practical Roadmap for AI

What is COSO?

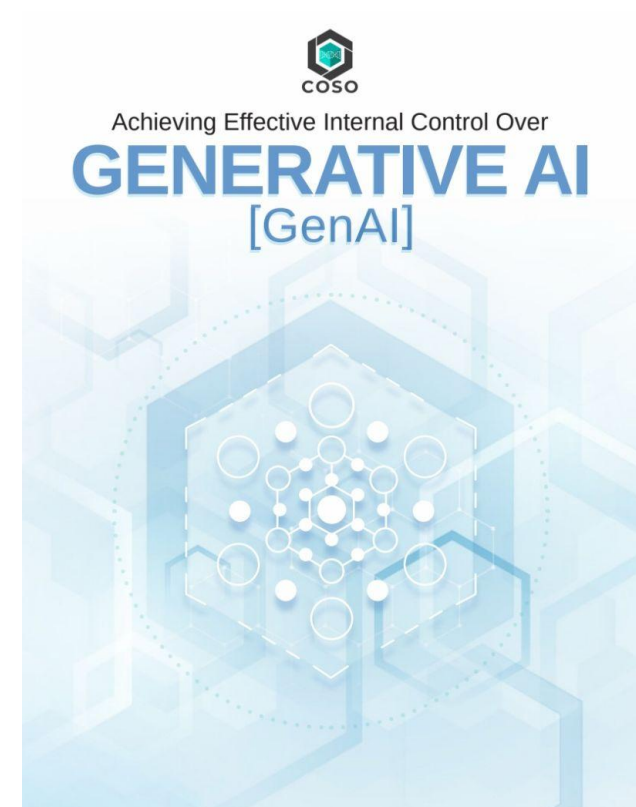
17 PRINCIPLES OF THE COSO FRAMEWORK



- Committee of Sponsoring Organizations of the Treadway Commission
- Globally recognized organization that developed a framework for:
 - Internal controls
 - Risk management
 - Governance
- Internal Audit uses COSO to evaluate the design and effectiveness of controls
- Five control components (Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring)
 - 17 Principles - provide addressment to AI

Purpose of COSO's AI Guidance

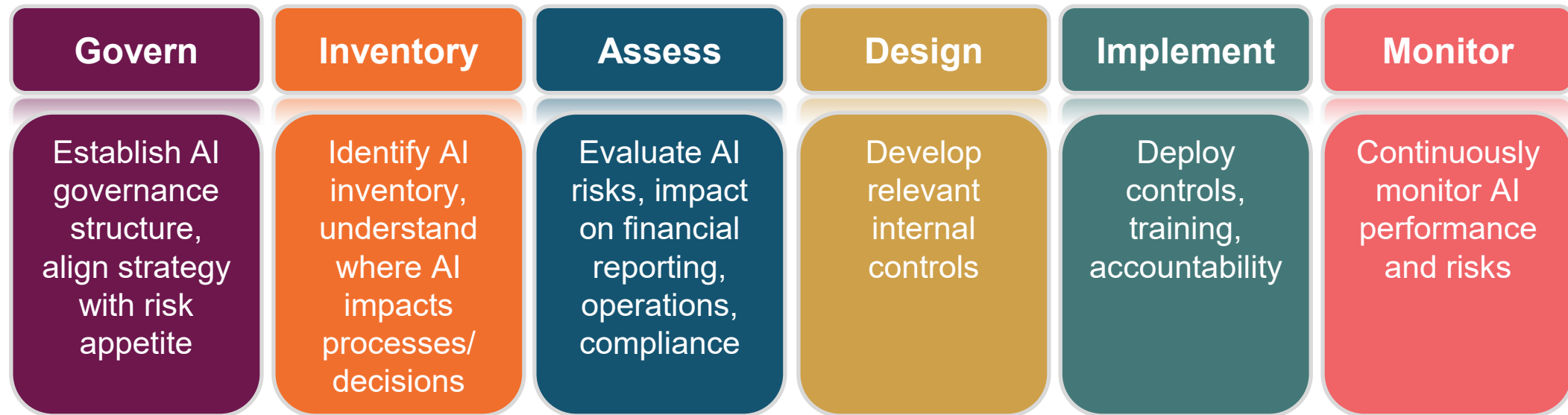
- Helps organizations:
 - Apply the COSO Internal Control Framework to AI
 - Manage AI risks while capturing benefits
 - Ensure reliable operations, reporting, and compliance
 - Provide audit-ready controls and governance practices



Reference: <https://www.coso.org/generative-ai>

COSO AI Implementation Roadmap

Six step approach





AI Environment & Strategic Imperative

Why This Matters Now

Financial institutions are growing into a more digital, AI-enabled, fraud-exposed environment.

144.7M

Members in federally insured credit unions

\$2.43T

Credit union system assets in Q4 2025

79%

Credit unions researching or implementing AI

\$12.5B

Consumer fraud losses reported to FTC in 2024

77%

Credit unions surveyed had at least one cyber incident

Interpretation

The conversation has changed. AI is no longer a novelty topic. It is embedded in vendor platforms, fraud tools, analytics and employee workflows.

Hard message

AI is already in the building. The issue now is how to govern it, where to trust it and what management can explain to the board.

Sources used for this framing include NCUA system performance data and FTC fraud-loss data

AI Risk Oversight: Why It Matters in 2026

Expanded AI risk landscape

AI in fintech introduces probabilistic outcomes and continuous model evolution, complicating traditional risk oversight.

Cross-enterprise risk impact

A single AI model can create compliance, operational, cyber, and reputational risks simultaneously across enterprises.

Innovation vs. assurance gap

Rapid adoption of generative AI and autonomous agents outpaces traditional control frameworks and audit capabilities.

Strategic governance importance

Strong governance and auditable controls enable responsible AI deployment and regulatory compliance in 2026.

Summary of Key AI Risk Themes

Pervasive AI adoption

AI systems are integral to fintech, handling fraud detection, credit decisions, pricing, and member service automation.

Expanded regulatory expectations

Regulators demand accountability, fairness, explainability, and traceability in AI systems to ensure ethical fintech operations.

Dynamic AI risk

AI risks evolve continuously through model changes, data quality shifts, and external factors, requiring agile risk management.

AI Adoption in the 2026 Fintech Landscape

AI in risk management

AI-driven fraud detection and anti-money laundering systems analyze large datasets in real time for complex pattern recognition.

AI enhancing member services

Regulators demand accountability, fairness, explainability, and traceability in AI systems to ensure ethical fintech operations.

Generative AI models

Shift towards generalized AI systems performing multiple functions, increasing efficiency but also raising operational risks.

Governance & oversight challenges

Rapid AI deployment challenges governance, requiring effective audit, risk prioritization, and control enhancements.

How AI Fundamentally Changes Risk Profile

Non-deterministic AI models

AI models produce varying outputs for similar inputs, making outcomes unpredictable and testing difficult.

Expanded regulatory expectations

AI 'black box' nature complicates understanding decision logic, hindering regulatory compliance and audits.

Continuous learning & model drift

AI systems continuously learn and change, requiring ongoing monitoring to detect bias and performance decline.

Evolving governance & oversight

Supervisory committees must adapt governance to manage AI risks characterized by uncertainty and rapid change.



AI Risk Categories & Regulatory Expectations

AI Risk Classification from an Audit Perspective

Model Risk

AI models face risks from flawed assumptions, poor validation, and performance degradation over time.

Data Risk

Data quality, lineage, and unauthorized usage critically affect AI system reliability and compliance.

Ethical & Bias Risk

Unintended bias in AI can cause discrimination, regulatory issues, and reputational damage.

Operational & Cyber Risk

Failures in AI processes and security vulnerabilities increase operational and cyber risks.

If It Moves Dollars or Decisions, the Control Bar Changes

Not every AI tool deserves the same controls, but impact changes the standard.

Tier 1: High Impact

Examples:

- Credit decisioning
- CECL
- Pricing
- Material reporting support

What to insist on:

- Validation plan
- Explainability
- Change control
- Independent review

Tier 2: Operational

Examples:

- Automation
- Authentication
- Workflow routing
- Alert triage

What to insist on:

- Audit trail
- Thresholds
- Exception review
- Vendor monitoring

Tier 3: Productivity

Examples:

- Meeting notes
- Drafting tools
- Research support
- Policy Q&A

What to insist on:

- Data rules
- Acceptable use
- Logging
- Training

Core Point: Risk tiering lets leaders move faster where risk is lower and insist on stronger evidence where AI influences member outcomes, dollars, reporting, fraud response, or regulatory treatment.

Top AI Risks Facing Fintech Institutions

Bias & discrimination risk

Bias in AI models can cause unfair credit decisions reflecting historical inequities, requiring proactive mitigation by institutions.

Model drift challenges

Changes in market or consumer behavior may degrade AI model accuracy, making continuous monitoring essential to avoid errors.

Data privacy concerns

Large language models risk exposing sensitive data unintentionally, heightening the need for strict data privacy controls.

Explainability & AI errors

Lack of explainability hinders regulatory compliance and trust, while AI hallucinations can cause operational disruptions.

Regulatory & Supervisory Expectations in 2026

Accountability in AI governance

Institutions must clearly assign responsibility for AI decisions from development to monitoring, ensuring accountability at all stages. (Policies and Procedures)

Explainability & transparency

Regulators require AI decisions to be explainable to consumers and stakeholders using documentation and interpretability tools. (Training, Skills)

Data governance & consumer protection

Emphasis on data quality, lawful use, and bias remediation to protect consumers in AI-driven financial services.

Supervisory oversight responsibilities

Supervisory Committees are expected to challenge management and ensure AI strategies adhere to regulatory compliance.

Emerging & Forward-Looking AI Risks

Autonomous AI agent risks

Autonomous AI agents introduce accountability and control challenges due to their independent action capabilities.

Synthetic identity fraud threat

AI-generated synthetic identities exploit onboarding and authentication weaknesses, increasing fraud risk.

Sophisticated AI cyberattacks

AI-driven cyberattacks use machine learning to evade detection and automate large-scale exploits.

Third-party & concentration risks

Reliance on few AI vendors or cloud providers increases systemic risks from outages or security incidents.



Governance, Controls, and Lifecycle Management

AI Governance Framework & Accountability

Governance structure

Board and management committees set AI risk appetite and translate expectations into policies and procedures.

Three lines of defense

Data science teams operate AI systems; risk and compliance monitor adherence; Internal Audit assures governance effectiveness.

Clear roles & accountability

Defined roles, escalation paths, and decision thresholds prevent fragmented accountability and control failures.

Proactive risk management

Strong AI governance enables innovation while ensuring safety, compliance, and trust within set boundaries.

Control Environment for AI Systems

Independent model validation

Validation assesses model soundness, data suitability, and performance before AI deployment, requiring multidisciplinary expertise.

Data governance & security

Ensuring data accuracy, lawful use, access control, and protection against unauthorized AI system access are essential controls.

Continuous monitoring & human oversight

Ongoing monitoring detects AI model drift or bias, complemented by human review for high-risk decisions to ensure safety.

Internal Audit & compliance

Internal Audit evaluates AI controls' design and effectiveness, supporting compliance and risk management confidence.

Managing AI Risk Across the Model Lifecycle

Design & development controls

Assess AI suitability and risks during design; focus on data, algorithms, and documentation during development.

Validation & deployment

Validate models for performance, bias, and robustness before deployment; implement operational safeguards during deployment.

Continuous monitoring

Monitor AI models continuously post-deployment to track performance, detect drift, and manage incidents.

Retirement & oversight

Retire outdated models responsibly; lifecycle oversight enables sustained risk assurance for auditors and committees.

Third-Party and Vendor AI Risk Management

Challenges of vendor transparency

Limited visibility into vendors' models and data complicates risk assessment and regulatory compliance.

Due diligence & contract management

Effective risk management requires thorough vendor due diligence and clear contract terms defining responsibilities.

Managing concentration risk

Supervisory Committees must monitor reliance on single AI providers and ensure contingency plans are prepared.

Role of internal audit

Internal audits evaluate third-party risk processes and validate vendor control effectiveness to ensure resilience.

Third-Party AI Risk is Not Outsourced Risk

Most institutions will experience AI first through vendors, data providers and embedded product features.

Due Diligence Scope

- What AI is actually used (not just the product label)
- What data is used for training, inference, tuning or logging
- How performance is monitored
- What human review exists
- How drift, errors, bias & incidents are identified

Contract & Monitoring

- Audit rights or independent audit report access
- Cooperation with regulatory exams
- Prompt written incident notification
- Data-security, privacy & retention obligations
- Limits on data use & disclosures
- Sub-processor / model provider visibility

Vendor claims are not control evidence.

Management must evidence vendor oversight is **documented, risk-ranked** and actually **performed**.



Oversight Roles, Audit Focus, and the Path Forward

Role of Internal Audit in AI Assurance

Independent AI governance assessment

Internal Audit assesses AI governance and risk management to ensure policies meet regulatory expectations and are consistently applied.

Technical audit areas expansion

Auditing now includes data governance, bias testing, and model monitoring, requiring specialized skills and collaboration.

Continuous auditing techniques

Using analytics and automated monitoring helps auditors identify emerging AI risks and deliver timely insights.

Trusted advisor role

Internal Audit supports responsible AI innovation and regulatory compliance by evolving audit approaches and clear communication.

Practical AI Risk Management Roadmap

AI inventory & risk assessment

Establish an enterprise-wide AI inventory and assess risks to prioritize high-impact use cases effectively.

Governance & regulatory alignment

Align governance frameworks with regulations by clarifying accountability and updating policies.

Enhanced controls & validation

Strengthen model validation, data governance, and monitoring to enhance AI risk controls.

Continuous monitoring & review

Integrate AI risk into ongoing monitoring and audits, adapting the roadmap to evolving risks.

Key Takeaways and Closing Discussion

Central AI risk challenge

AI risk presents complexity and uncertainty requiring advanced governance and assurance in fintech.

Collaborative oversight importance

Supervisory Committees and Internal Auditors must collaborate to ensure effective AI governance frameworks.

Proactive risk management

Embedding controls and maintaining accountability reduce regulatory, operational, and reputational risks.

Harnessing AI benefits safely

Effective AI risk management protects consumers and maintains trust while leveraging AI advantages.

Key Takeaways for Internal Audit/Supervisory & Audit Committees

- AI requires continuous monitoring (not point in time audits)
- Controls must evolve as models change
- Internal Audit plays a role in
 - AI governance
 - Model risk validation
 - Data and control testing
- COSO emphasizes traditional approaches must adopt to dynamic AI risks



Joseph A. Zito, CPA, MBA
Principal
zito@doeren.com
248.244.3068



Lindsey Becker, CRCM
Sr. Manager Internal Audit
becker@doeren.com
810.210.4446

Thank you ▶