



ARMANINO

Generative AI: Internal Audit and Risk Management Considerations



Speaker Bio

Liam Collins

Liam has more than 20 years of assurance and consulting experience, including 10 years with Big Four firms. He leads growth for the firm's Risk Assurance and Advisory Services practice, which includes the firm's Cybersecurity, Privacy, AI Risk Management, Service Organization Control (SOC) audit, HITRUST, ISO27001, Sarbanes-Oxley (SOX), Internal Audit and IT Compliance service lines.

Before joining Armanino, Liam served as a Managing Director at KPMG, where he was an engagement Partner on several large assurance and consulting projects. He has also held audit, assurance and IT leadership roles at PricewaterhouseCoopers (PwC) and Clare Chapman.

Liam is a member of the American Institute of CPAs and the Information Systems Audit and Control Association (ISACA). He received a BSc. in Accounting from Golden Gate University, a JD from the University of San Francisco School of Law and an MBA from the Wharton School at the University of Pennsylvania.





Speaker Bio

Tommy Canfield

Tommy is a cybersecurity professional with over 7 years experience ranging from IT services and cybersecurity consulting. Currently he is a Manager in Armanino's Trust Services practice specializing in risk assessments, penetration testing, vulnerability management, incident response, security configuration benchmarking, and developing cybersecurity best practices for organizations.

Before joining Armanino Tommy served 10 years in the United States Army. He currently holds several industry certifications including OSCP, PNPT, PWPT, CSAP, CySA+, and Security +.





Generative AI

Learning Objectives

- The Use of A.I. & Organizations
- Internal Audit and Risk
- Leveraging Industry Frameworks
- Practical Steps For Your Organization

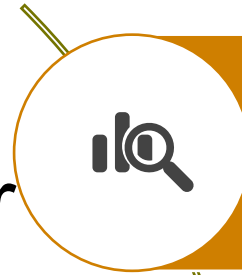


The Use of AI & Organizations

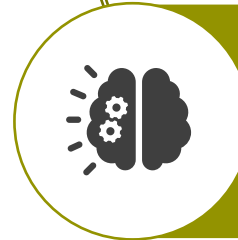
Statistics to Consider

More than half of employees hiding their use of AI from their Bosses!

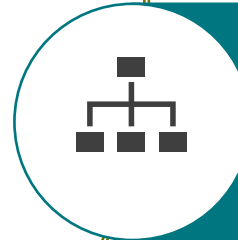
Most people say the tools they use in their personal life are far better than what they have at work.



67% of respondents say they use AI at work and 69% of organizations are using AI.
60% say they have had no training on how to use their AI tools.



43% of organizations are reporting increased revenue generating activity.
Only 60% of organizations have an AI strategy in place.
Less have responsible use policies.

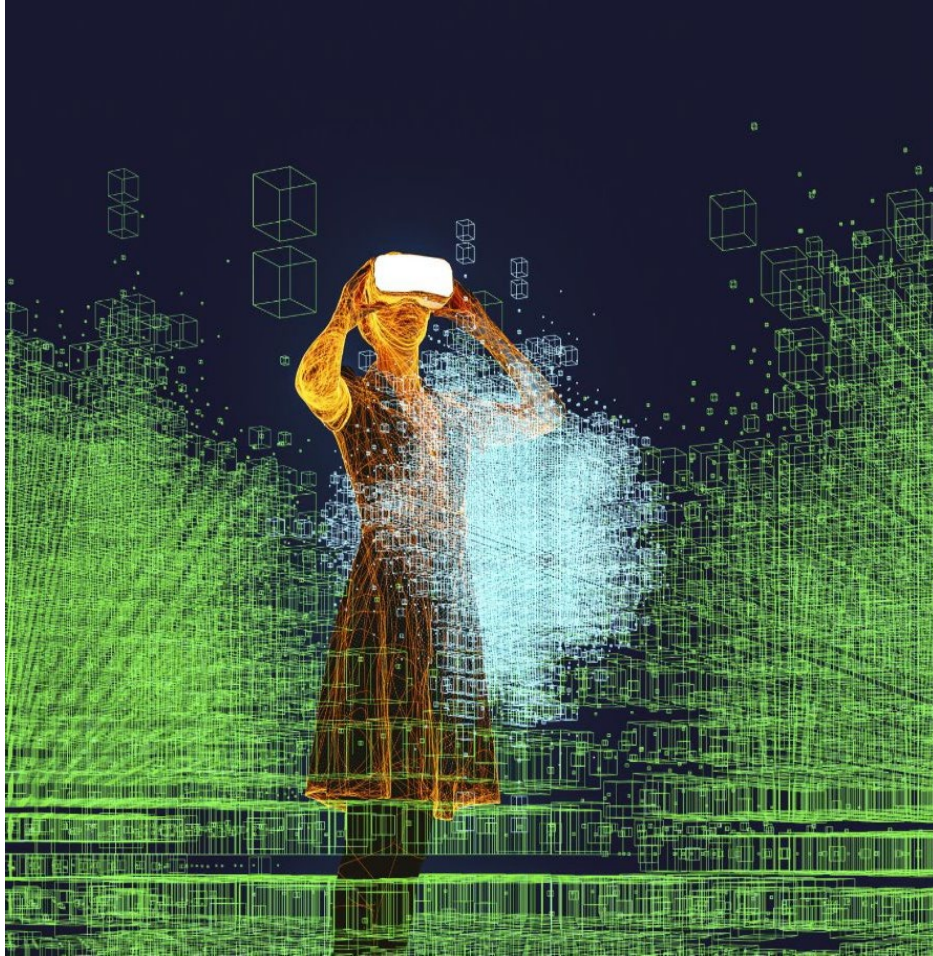


BYOAI – 57% of employees are hiding their use of AI tools from their managers. 50% of employees are presenting AI generated content as their own.



Over Half admit to uploading company sensitive information to public AI tools. 66% rely on the output of AI without reviewing in detail.

*Source: KPMG and University of Melbourne – Trust, Attitudes and the use of AI



How is Generative AI Impacting Organizations?

Broad Use

- Generative AI new and exciting, but it isn't one thing. It is a technology, akin to the internet, or electricity. The benefit of the tool is in the detail.

Boosting Productivity

- At a high level – we've seen obvious advantages of upleveling productivity in nearly every task – but's almost impossible to define exactly when users will leverage the tool. Additionally the output of these tools are inconsistent and difficult to predict.

Understanding Capabilities

- While tools such as ChatGPT, Copilot, or Google Gemini have some pre-defined uses (be it labeled prompts, agents, or something else) these tools can be used for nearly any task imaginable. The reality is that we need to assume these tools are being used in nearly any and every process.

Navigation

- Progress Status
- Back to Assessments

CIS Controls

- Control 01: Enterprise Asset Management
- Control 02: Software Inventory
- Control 03: Data Protection
- Control 04: Secure Configuration
- Control 05: Account Management
- Control 06: Access Control
- Control 07: Continuous Vulnerability Management
- Control 08: Audit Log Management
- Control 09: Email and Web

{{ assessment.client_name }}

Assessor: {{ assessment.assessor_name }} | Period: {{ assessment.start_date }} to {{ assessment.end_date }}

{% for section_id, section in controls.items() %}

CIS Control {{ section_id }}: {{ section.name }}

{% for control in section.controls %}

Control {{ control.id }}: {{ control.title }}

{{ control.description }}

Control Detail

{{ control.details }}

Implementation Level

Met
Not Met
Partially Met
Not Assessed

Testing Procedures

Evidence

Enter evidence here...

Save Control

Navigation

- Progress Status
- Back to Assessments

CIS Controls

- Control 1: Inventory and Control of Enterprise Assets
- Control 2: Inventory and Control of Software Assets
- Control 3: Data Protection

Progress Status

Control	Completion Status
Inventory and Control of Enterprise Assets	
1.1 - Establish and Maintain Detailed Enterprise Asset Inventory	Not Started
1.2 - Address Unauthorized Assets	Not Started
Inventory and Control of Software Assets	
2.1 - Establish and Maintain Software Inventory	Not Started
2.2 - Ensure Authorized Software is Currently Supported	Not Started
2.3 - Address Unauthorized Software	Not Started
Data Protection	
3.1 - Establish and Maintain Data Management Process	Not Started

Internally developed tool using AI assisted coding techniques.



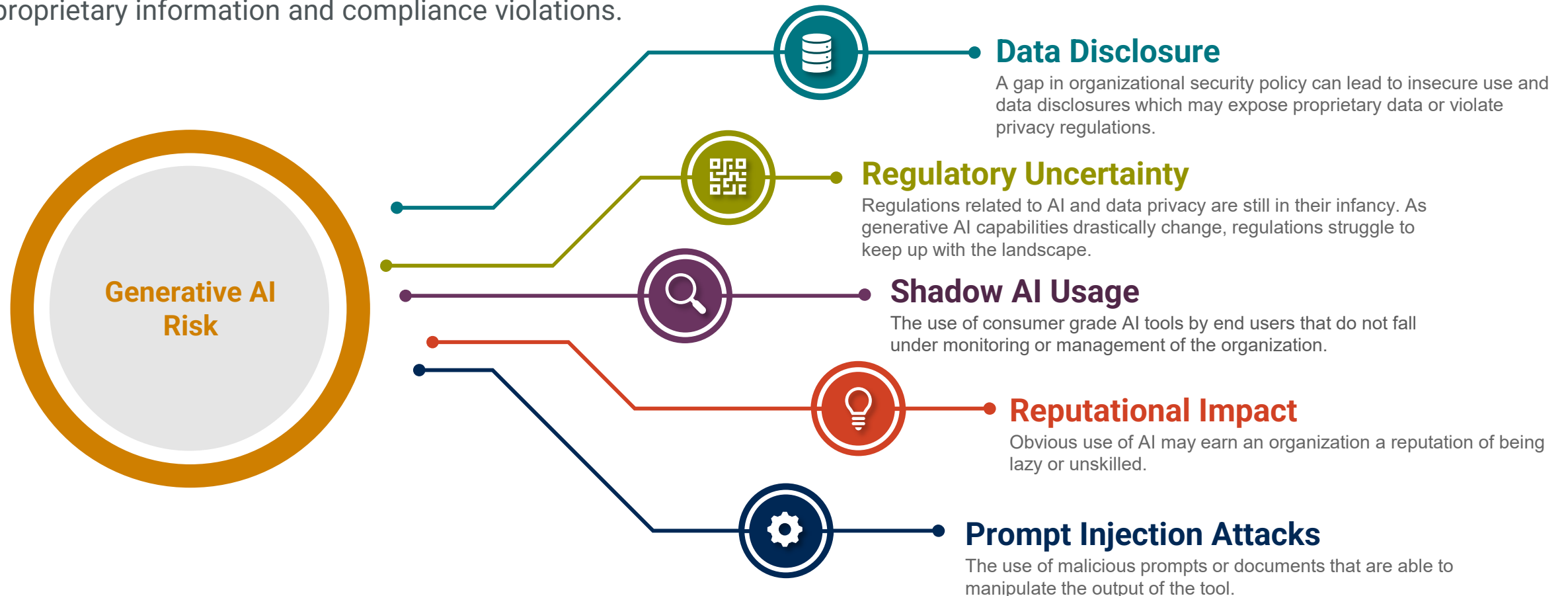
Audience Interaction

- In your organization there is not yet a policy governing the use of AI. An employee begins generating customer emails using sensitive data or private data.
- What internal audit concerns does this raise?



Downside: Key Risks Associated with Generative AI

Generative AI can pose risks to data security by requiring access to sensitive information, potentially leading to vulnerabilities. Using generative AI without proper oversight can increase risks, such as data breaches, loss of proprietary information and compliance violations.





Advanced Threats Emerge

Increased Fraud Capabilities

- Deepfakes can be used to impersonate individuals
- Potential for financial scams and identity theft
- Ultimately - importance of verifying the authenticity of audio and video, can't just believe your eyes





Internal Audit and Risk



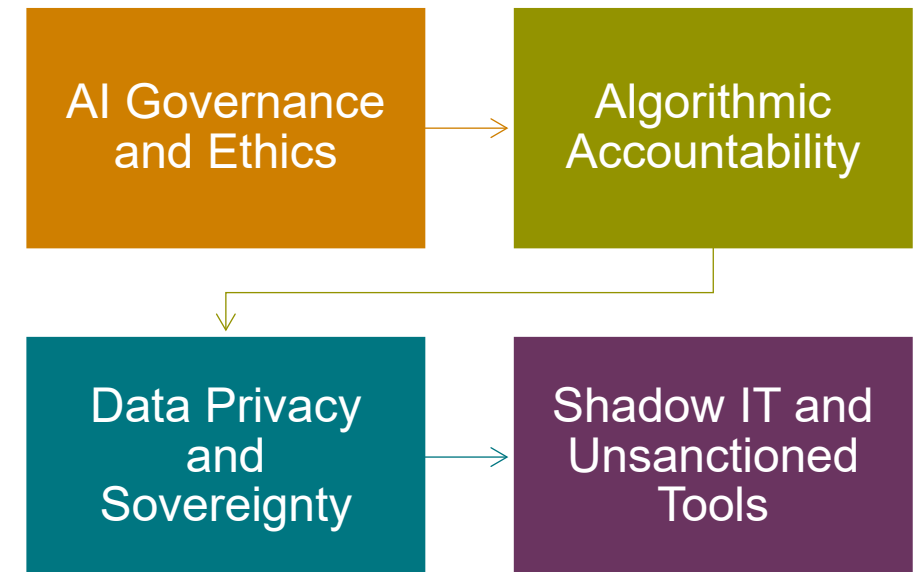
The Evolving Role of Internal Audit in Tech Governance

Previously IA: has been focused on financial controls, compliance, and post-event reviews.

New Role: Active partner in digital transformation, advising on AI, cloud, automation, and cybersecurity.

Internal audit is shifting from being **reactive** to being **risk-forward and technology-aware**.

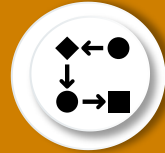
Emerging IA Domains





Risk Strategy

01 Mitigating Potential Threats



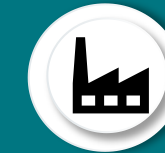
- Partner with the business in developing a Risk Management Governance Structure
- IA should have a key role in any effective governance model
- Utilize best practice approaches for vulnerability considerations such as OWASP Top 10 LLM & Generative AI security risks.

02 Maximizing Opportunities



- Effective strategies not only mitigate risks but also explore opportunities for innovation and growth through generative AI.
- Increase the effectiveness of team member through the use of AI to speed up tasks.

03 Evolving AI Technologies



- Organizations should monitor the latest advancements in generative AI technologies to leverage their potential benefits effectively.
- All while verifying newest technologies are safe and effective, without bias.

04 Strategic Adaptation



- Adapting strategies in response to emerging AI trends is crucial for maintaining competitiveness in the market.
- AI should be used to reduce audit time, streamline processes, enhance accuracy, and deliver greater value to the organization or client.

05 Compliance and Regulation



- Staying compliant with AI regulations and guidelines is essential for organizations to avoid potential legal issues and maintain trust.
- This is vastly different country by country and changing almost daily.



Integrating AI governance and oversight into the Audit Plan





What are the current challenges we are hearing from IA Leaders?



Keeping Up

- Regulations and Compliance Frameworks are changing at a faster pace than ever before. Keeping up with them is becoming an arduous and expensive task with many inconsistencies and gaps.
- Many changes are not optional anymore but mandatory, urgency to ensure proper risk identification, mitigation and monitoring with updated policies



Lack of Experience

- With digital transformation, many companies require talent with advanced skills to analyse digital data and provide assurance while ensuring updated risk management frameworks (especially with AI tools and solutions). The rate at which demand for such talent is increasing is not in sync with supply thereby creating a big gap in skilled auditors with experience

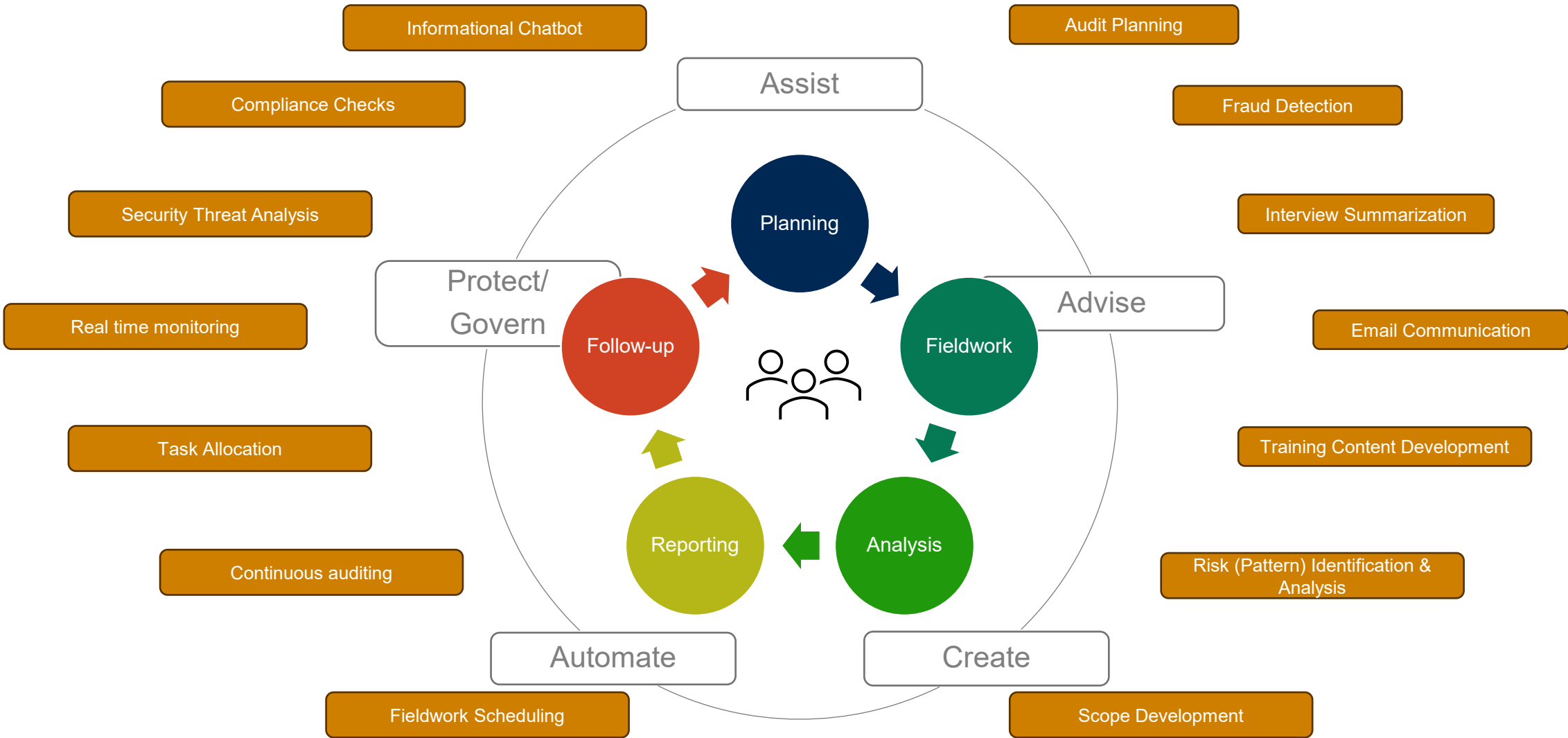


Data Overload

- With many companies investing in data warehouse and other tools, there is an unprecedented growth in diverse data sets and volume in the last decade. Sifting through data and provide contextual analysis is becoming challenging and time consuming.
- Timely analysis of data is becoming a real problem across many auditors with already strained capacity.

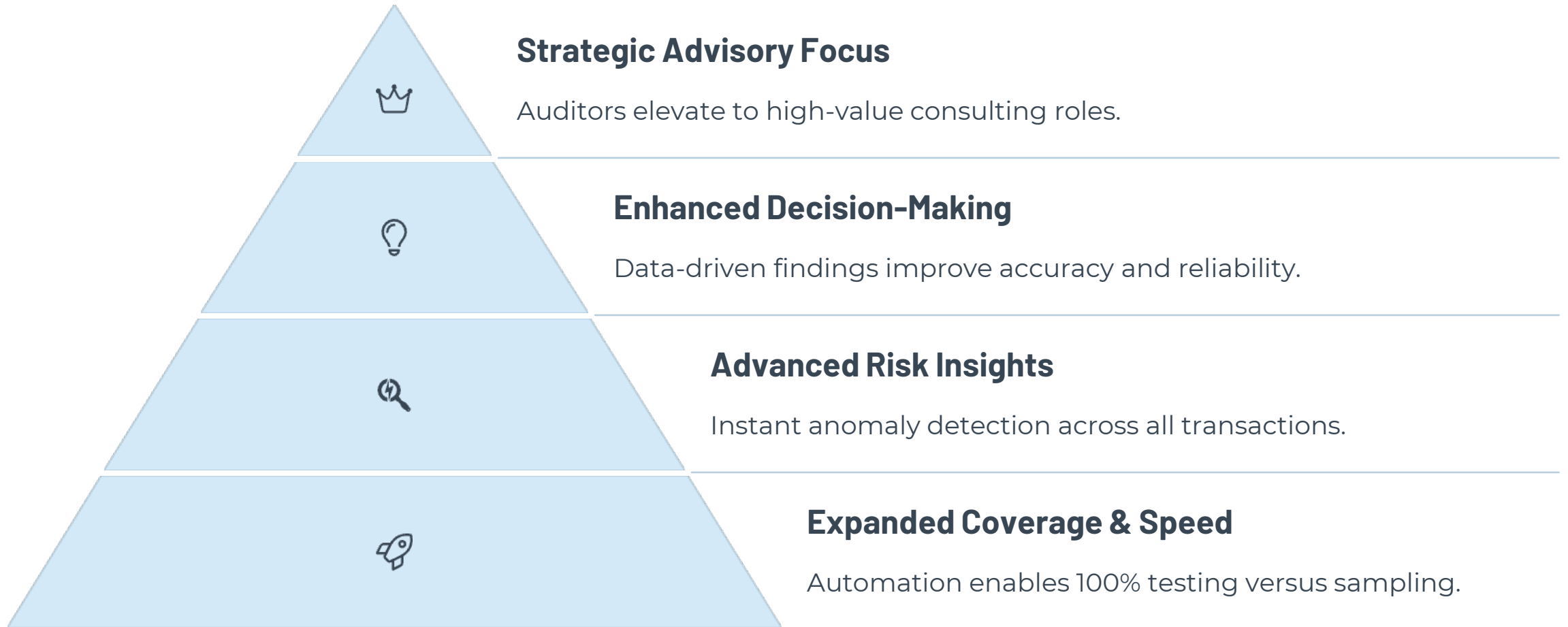


How can AI benefit Internal Audit Process?



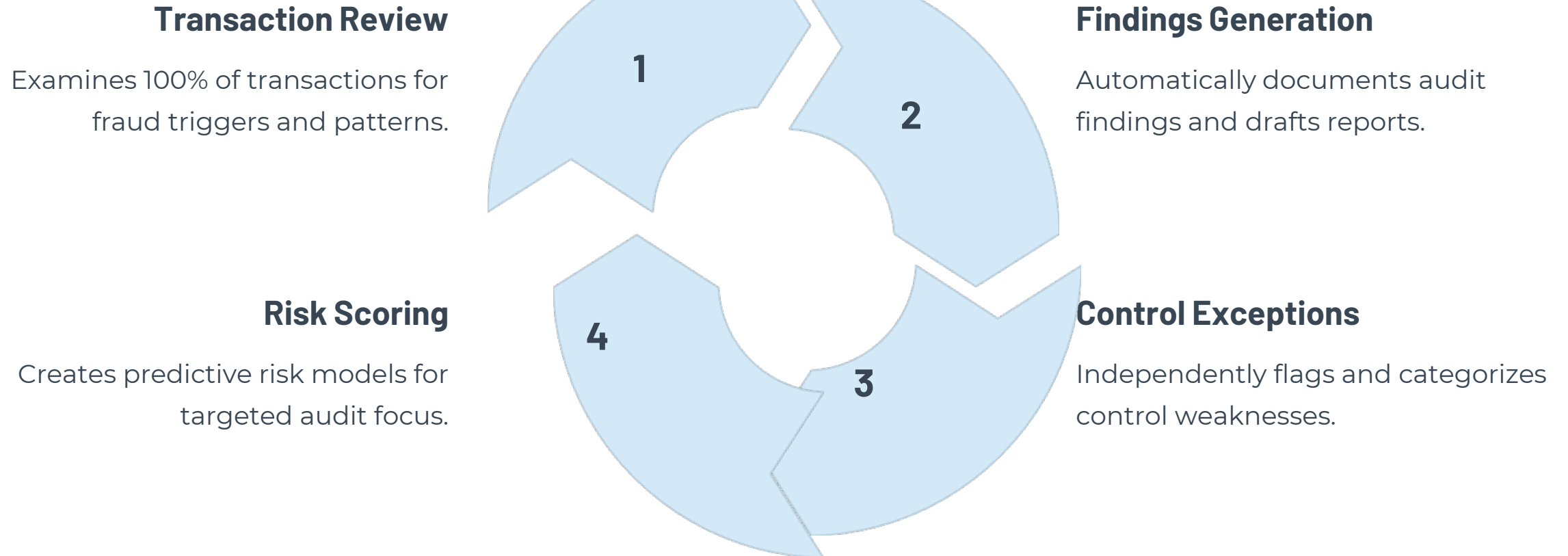


Key Benefits for Internal Audit Functions





Practical Examples of AI Agent Applications





Roadmap for AI Agent Adoption in Audit

Pilot Projects

Start with clearly defined, repeatable audit tasks for initial AI implementation.

Training & Culture

Invest in upskilling auditors and fostering technology adoption mindsets.

Governance Framework

Develop comprehensive oversight mechanisms for responsible AI use.

Impact Measurement

Track KPIs including reduced manual effort and increased audit accuracy.



Audience Interaction

- What are some real-world examples you have of partnering with across your organization to address AI related risks?



Audience Interaction

- What are some real-world examples you have of partnering with across your organization to address AI related risks?
- Have you been able to leverage AI to enhance your audit processes?



Industry Frameworks

How an Organization Can Securely Onboard AI



Internal Audit and Risk

Framing Risks – Understanding and Addressing Risks

- While risk management processes generally address negative impacts, frameworks may offer approaches to minimize anticipated negative impacts of AI systems and identify opportunities to maximize positive impacts.





Why should we adhere to Responsible AI Frameworks?

Applying a Framework

Key Tenets:

- Transparency
- Accountability
- Security
- Privacy
- Fairness
- Inclusion/ Bias prevention



Illustrative Frameworks



AI Assurance: A Repeatable Process for Assuring AI-enabled Systems



Key Regulatory Frameworks

European Union: AI Act

- First comprehensive AI law categorizing AI systems by risk levels
- Bans on high-risk applications like social scoring
- Stricter obligations for high-risk AI systems

■ United States: Executive Orders & State Law

- No federal AI law yet, but sector-specific regulations (e.g., healthcare, finance)
- AI Bill of Rights guiding ethical AI principles
- Emerging state laws (e.g., California AI regulations)

China: AI Guidelines & Algorithm Regulation

- Strict AI content moderation laws
- Regulations on deep synthesis and recommendation algorithms
- Emphasis on government oversight

Other Countries & Initiatives

- UK: Pro-innovation regulatory framework
- Canada: AI and Data Act (AIDA) for responsible AI use
- OECD & UN: Global AI governance principles



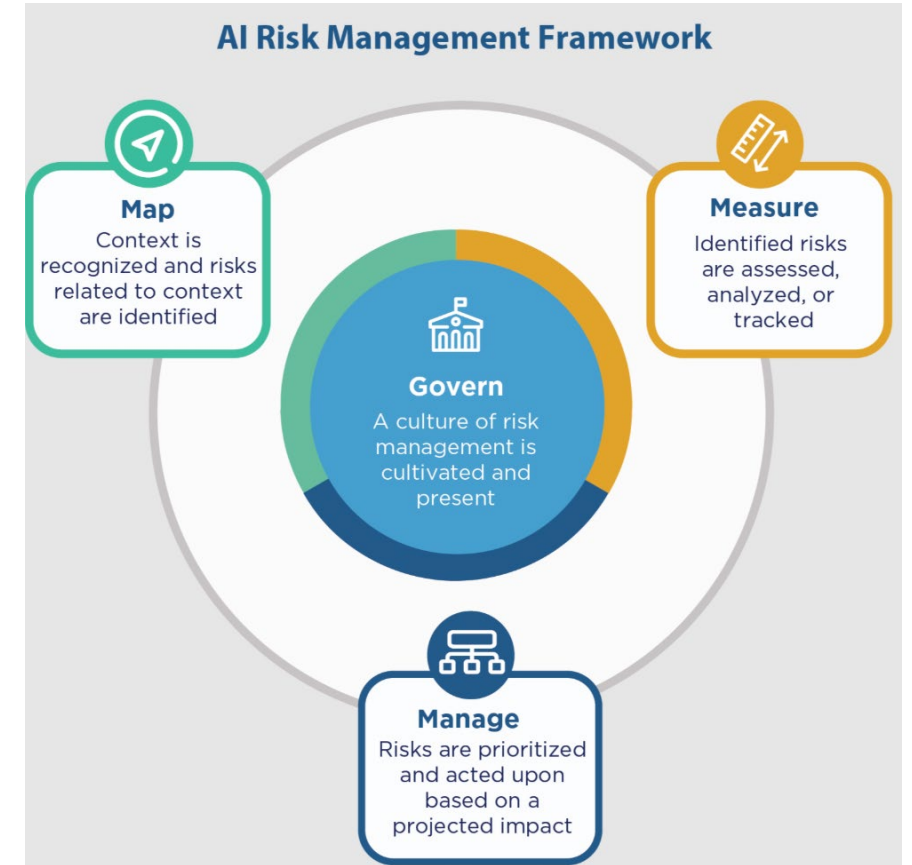
NIST Compared to ISO 42001

Breakdown	ISO 42001	NIST AI RMF
Objective Focus	AI Management system that covers governance, risk management, and compliance.	Risk management framework with a focus on guiding organization implementation.
Tenants	Governance Risk Management Compliance and Legal requirements Continuous Improvement	Govern Map Measure Manage
Principles	Ethical implementation considering fairness, transparency and privacy.	Ethic implementation considering fairness, transparency and community impact.
Scope	Broad and applicable across many industries.	Focus on enhancing AI trustworthiness across multiple industries.
Implementation	Develop a governance strategy, conduct risk assessments, validate compliance, and perform ongoing evaluation.	Develop governance strategy, map the content, measure and manage risk.
Potential Negative Outcomes	Complexity in implementation with the need for costly resources and skilled personnel.	Complexity in implementation with the need for costly resources and skilled personnel.



NIST AI Risk Management Framework (RMF)

- The AI RMF is a voluntary framework to improve the ability to incorporate trustworthiness into the design, development, use, and evaluation of AI products.
- Organizations can create a use case RMF profile as well as a temporal profile to identify the desired state.
- Composed of four components; Governance, Map, Measure., Manage
- **AI RMF Roadmap:** key activities for advancing the AI RMF
- **AI RMF Crosswalks:** Enhance the frameworks alignment with other AI frameworks and international standards

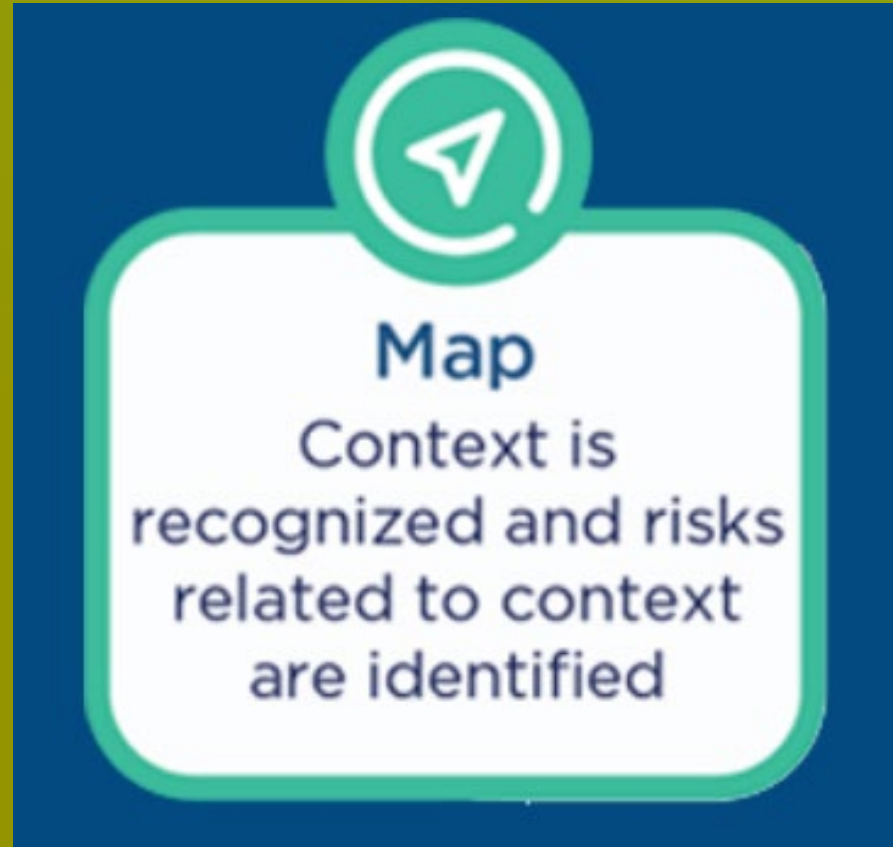




RMF Govern

- NIST RMF Govern function acts as the underlining principle, requiring a solid foundation.
- This step requires the provisioning of policies, procedures and practices that guide the organization as it maps, measures. And manages AI
- Key areas of focus
 - Legal and regulatory requirements
 - Risk Management
 - Identify roles, responsibilities and assign training
 - Executive leadership involvement
 - Organization AI strategy





RMF Map

The Map function identifies the contextual use and need for the AI tool. The organization must identify the objectives surrounding the development of the AI such as the intended use, benefits, costs, and potential impact.

Key areas of focus:

- Understanding the current organization's skills in A.I. and required additional skills.
- Define the business value to include a cost/benefit analysis
- Tasks and methods to implement tasks that the AI will support



Manage

Risks are prioritized
and acted upon
based on a
projected impact

RMF Manage

The manage function provides a process to assign prioritization to risks which guides the organization on response based on projected impact.

Key areas of focus:

- Assessment of the effectiveness for the AI to meet organization objectives
- Risk Assessment Capabilities (prioritization)
- Risk management
- Risk response capabilities
- Third-Party AI Risk
- Incident communication



RMF Measure

- The measure function requires the organization to effectively identify, analyze, and manage risks associated with A.I. implementation.
- **Key areas of focus:**
 - Metrics and methods of measuring AI risk
 - Control measurement for effectiveness
 - Independent, ongoing AI analysis
 - Qualitative & quantitative AI analysis
 - Privacy risks evaluated
 - Fairness and bias evaluation



OWASP Top 10 for LLMs

The OWASP Top 10 for LLMs is a more technical approach to reviewing the risk of Generative AI. For internal audit, it is important to understand these risks in relation to third-party tooling or internally developed tools

The OWASP Top 10 for Large Language Model Applications Project aims to educate organizations about the potential security risks when deploying and managing Large Language Models (LLMs) and Generative AI applications.

Education is focused on technical roles such as:

- Developers
- Designers
- Architects
- Managers

OWASP | **TOP 10** LLM APPLICATIONS & GENERATIVE AI

<p>LLM01</p> <p>Prompt Injection</p> <p>LLM01: Prompt Injection</p>	<p>LLM02</p> <p>Insecure Output Handling</p> <p>LLM02: Insecure Output Handling</p>	<p>LLM03</p> <p>Training Data Poisoning</p> <p>LLM03: Training Data Poisoning</p>	<p>LLM04</p> <p>Model Denial of Service</p> <p>LLM04: Model Denial of Service</p>	<p>LLM05</p> <p>Supply Chain Vulnerabilities</p> <p>LLM05: Supply Chain</p>
<p>LLM06</p> <p>Sensitive Information Disclosure</p> <p>LLM06: Sensitive Information Disclosure</p>	<p>LLM07</p> <p>Insecure Plugin Design</p> <p>LLM07: Insecure Plugin Design</p>	<p>LLM08</p> <p>Excessive Agency</p> <p>LLM08: Excessive Agency</p>	<p>LLM09</p> <p>Overreliance</p> <p>LLM09: Overreliance</p>	<p>LLM10</p> <p>Model Theft</p> <p>LLM10: Model Theft</p>



Ethical AI Framework

ISO 42001 provides guidelines for organizations to implement ethical practices in the use of AI technologies.

Responsible AI Usage

The standard promotes responsible AI usage that respects individual rights and promotes fairness within society.

Alignment with Societal Values

ISO 42001 emphasizes the importance of aligning AI applications with societal values to enhance public trust.

Responsible AI Use

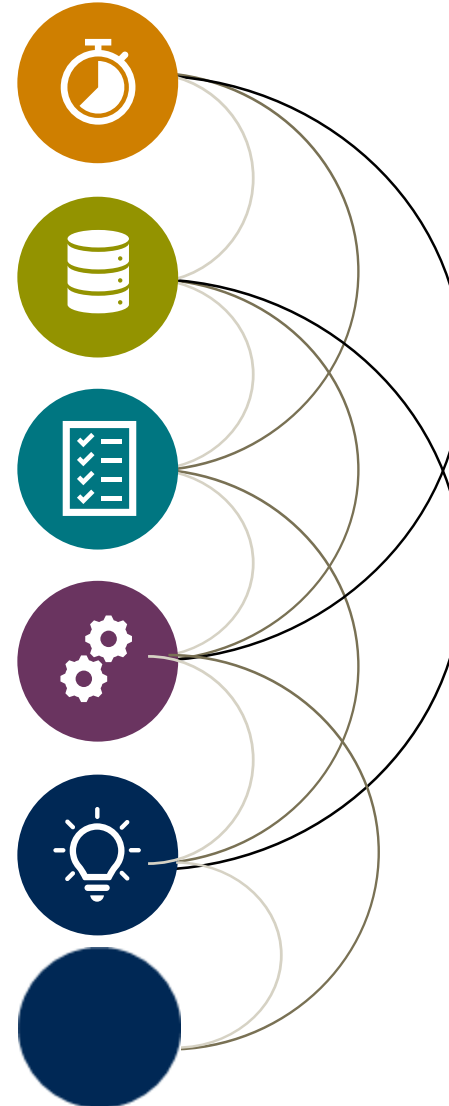
Organizations must adhere to ethical principles to ensure AI technologies are used responsibly and safely.

Transparency in AI

Transparency is crucial for building trust in AI systems, allowing stakeholders to understand decisions made by AI.

Fairness and Accountability

Ensuring fairness in AI algorithms is essential to prevent bias and promote accountability in AI applications.








ISO 42001 Summary

Integrating AI means having a strong framework to build from.



Practical Steps for Your Organization

				
Establish AI Strategy	Conduct Risk Assessment	Governance Alignment	Deploy Control group	Training & Culture Enablement
Define the Why	Identify technical readiness: required tech resources	Data access controls: least privilege	Target high-risk users	Appropriate use of AI tool
Identify similar industry use cases	Identify organizational readiness: licenses and eligibility	AI Policy Published	Target high-value users	Prompt hygiene: prevent PII leak
Identify relevant frameworks	Data classification & access control policies enforced	Audit Align and AUP	Test prompt injections and data leakage	The AI tools prohibited



Enterprise-Wide Application and Continuous Monitoring

Phased Roll Out



Roll out the use of the AI in waves to target audiences. This reduces overwhelming IT tickets and issues and helps a smooth transition.

Continuous Monitoring

Use security tools to monitor the AI to ensure company policies are met. This may require new tool sets specifically to monitor AI tools.

Reassess Risk Posture

Ongoing risk assessments to ensure that as AI changes, new risks are not introduced into the environment. Evaluate how the organization has used AI and where improvements can be made.

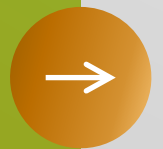
Successful AI Integration



THANK YOU
Questions?



Zania Demo



Armanino Operates in an Alternative Practice Structure:

“Armanino” is the brand name under which Armanino LLP, Armanino CPA LLP, and Armanino Advisory LLC, independently owned entities, provide professional services in an alternative practice structure in accordance with law, regulations, and professional standards. Armanino LLP and Armanino CPA LLP are licensed independent CPA firms that provide attest services, and Armanino Advisory LLC and its subsidiary entities provide tax, advisory, and business consulting services. Armanino Advisory LLC and its subsidiary entities are not licensed CPA firms.