

Internal Audits role in evaluating AI risks



The Institute of
Internal Auditors



Cherry Bekaert
Your Guide Forward

Presenters



Scott Peyton

*Partner, Risk Advisory Practice Leader
Cherry Bekaert Advisory LLC*
scott.peyton@cbh.com



Kurt Manske

Partner, Cyber and Information Assurance Leader
kurt.manske@cbh.com
Cherry Bekaert Advisory LLC



Types of Artificial Intelligence



Artificial Intelligence (AI): Simulates human decision making. Great for evaluation of mass amounts of data.



Machine Learning (ML): Perform repetitive tasks but also learn from the data. Examples: Netflix suggesting videos based on watch history from you and others or SPAM filtering.



Large Language Model (LLM): Models applying algorithms pretrained on mass amounts of data. Interprets language. Example Chatbots, Siri, Alexa



Generative AI (Gen AI): Models or algorithms that create new/original content based on mass amounts of data. Predict wording and responses based on patterns from training data. Example ChatGPT, music composition- Beetles Now and Then, This-person-does-not-exist.com



Areas where AI may already be in use



Technical Tools



**Virtual Assistants/Chatbots –
Customer Service**



**Fraud Detection
and Prevention**



**Customer Relationship
Management (CRM)**



**Risk Analysis, Financial
Forecasting, Marketing, Human
Resources**

Discussion Question

What is your institutions view of AI?

- a. Overhyped or holds too much risk to consider
- b. Others may use it, but we never will
- c. Has some potential, but only in niche areas of our organization
- d. AI has broad opportunity across our institution



The Good, Bad, and the Ugly

Why organizations are considering AI?

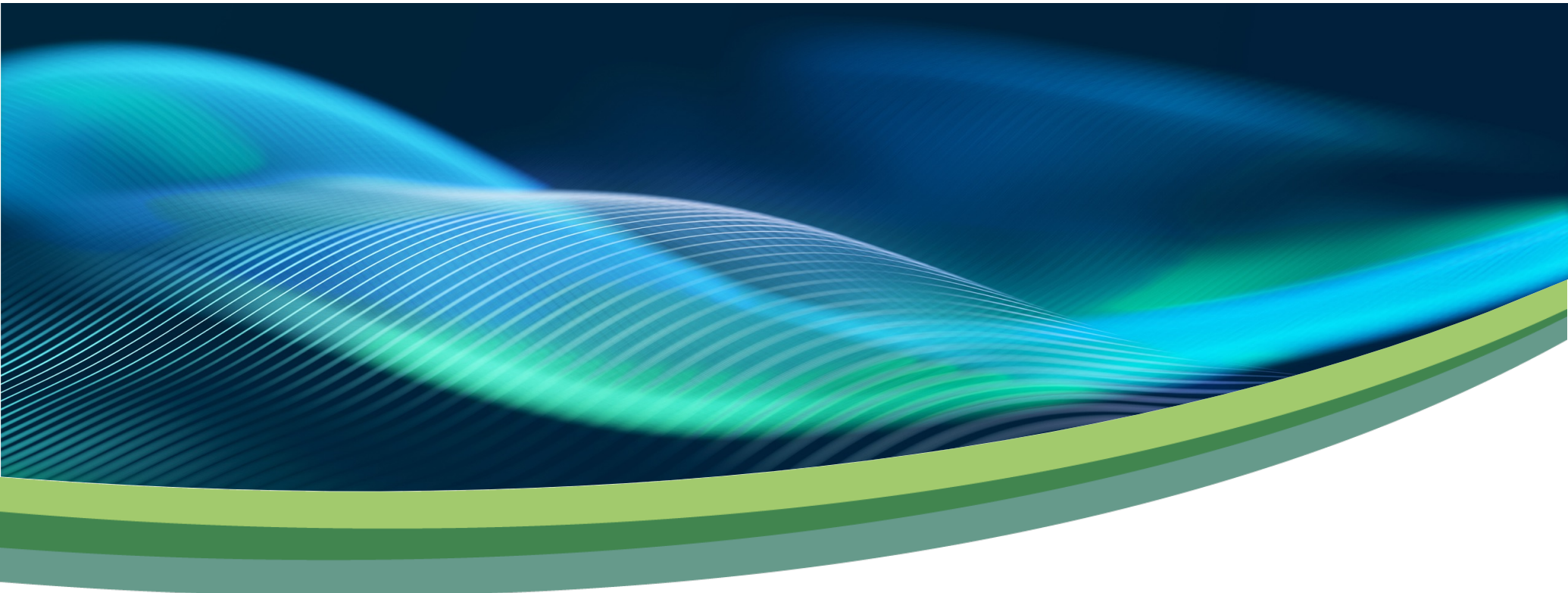
- ▶ Automation of data collection and analytics
- ▶ Speed of decision making
- ▶ Responsiveness to customers
- ▶ Automated workflow
- ▶ Continuous Monitoring and Fraud Detection
- ▶ Efficiency and accuracy of repetitive tasks (i.e. loan processing, online account opening)



...and why not?

- ▶ Fear of the unknown/newer technology
- ▶ Security/privacy of data
- ▶ Regulatory scrutiny
- ▶ Potential for masked bias or inaccurate results – May put the institution out of compliance with certain regulations, such as Fair Lending
- ▶ Transparency for Audits and Examinations
- ▶ Short term implementation and training costs
- ▶ Job displacement
- ▶ Lack of Human touch (usually more applicable to customer facing functions)





Risks to Consider

Risks to Consider

Regulatory Risks

- ▶ Auditability (explainability, complexity, transparency, accountability, etc.)
- ▶ Data protection laws
- ▶ Anti-discrimination laws
- ▶ Customer protection laws
- ▶ Unclear legal regulation

Technical Risks

- ▶ Data leakage
- ▶ Cyber Attacks
- ▶ Adversarial Attacks – cause the AI system to make incorrect predictions or decisions
- ▶ Customer impact from fraudsters (phishing, voice cloning, deepfake, etc.)
- ▶ AI Supply Chain (i.e. data sources, pre-trained AI, third-party and black box components, code libraries)

Operational Risks

- ▶ Sharing of inaccurate or protected information through chatbots (also applies to Regulatory risks)
- ▶ Embedding of bias into algorithms (also applies to Regulatory risks)
- ▶ Inaccurate decision making
- ▶ Intellectual Property/proprietary Information disclosure
- ▶ Inoperability or integration issues with existing/legacy systems
- ▶ Trust

Reputational/ Financial Risks

- ▶ Combinations of all the above



AI Risk Framework

GenAI processing capabilities present a significant roster of risks ranging from enterprise strategy, to misuse of data, to unreliable AI results.

Safety & Security

AI systems are protected from logical and physical threats to ensure the integrity of the AI system.

Transparency

AI systems are explainable to stakeholders and users are informed of use of AI and potential impacts

Accountability & Responsibility

Ownership and responsibilities are clearly defined for governing the use of AI technology

Privacy

AI systems are in compliance with privacy controls to protect individual privacy rights.

Reliability & Resiliency

AI systems are reliable and resilient to enable business processes and minimize the impact of disruptive events

Fairness

AI systems are set up with minimal bias or favoritism to ensure equitable outcomes for all

Risk Based

AI systems are classified using a risk-based approach to evaluate and mitigate risks introduced

Enterprise
AI Adoption

Additional Risk Considerations

- Internal GenAI Development
- Third Party Use of GenAI
- Cybersecurity and Technology





Leading Regulations & Guidance

- ▶ Gramm-Leach-Bliley Act (GLBA)
- ▶ California Privacy Rights Act (CPRA)
- ▶ Executive Order 14179 "Removing Barriers to American Leadership in Artificial Intelligence"
- ▶ EU's General Data Protection Regulations (GDPR)
- ▶ EU AI Act
- ▶ Individual State legislation

<https://www.ncsl.org/technology-and-communication/artificial-intelligence-2023-legislation>

- ▶ NIST AI Risk Management Framework
- ▶ ISACA Auditing Guidelines for AI
- ▶ FFIEC Architecture, Infrastructure, and Operations (AIO) Booklet, section VII.D Artificial Intelligence and Machine Learning
- ▶ FRB SR 117 Guidance on Model Risk Management

<https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf>





Governance and Oversight

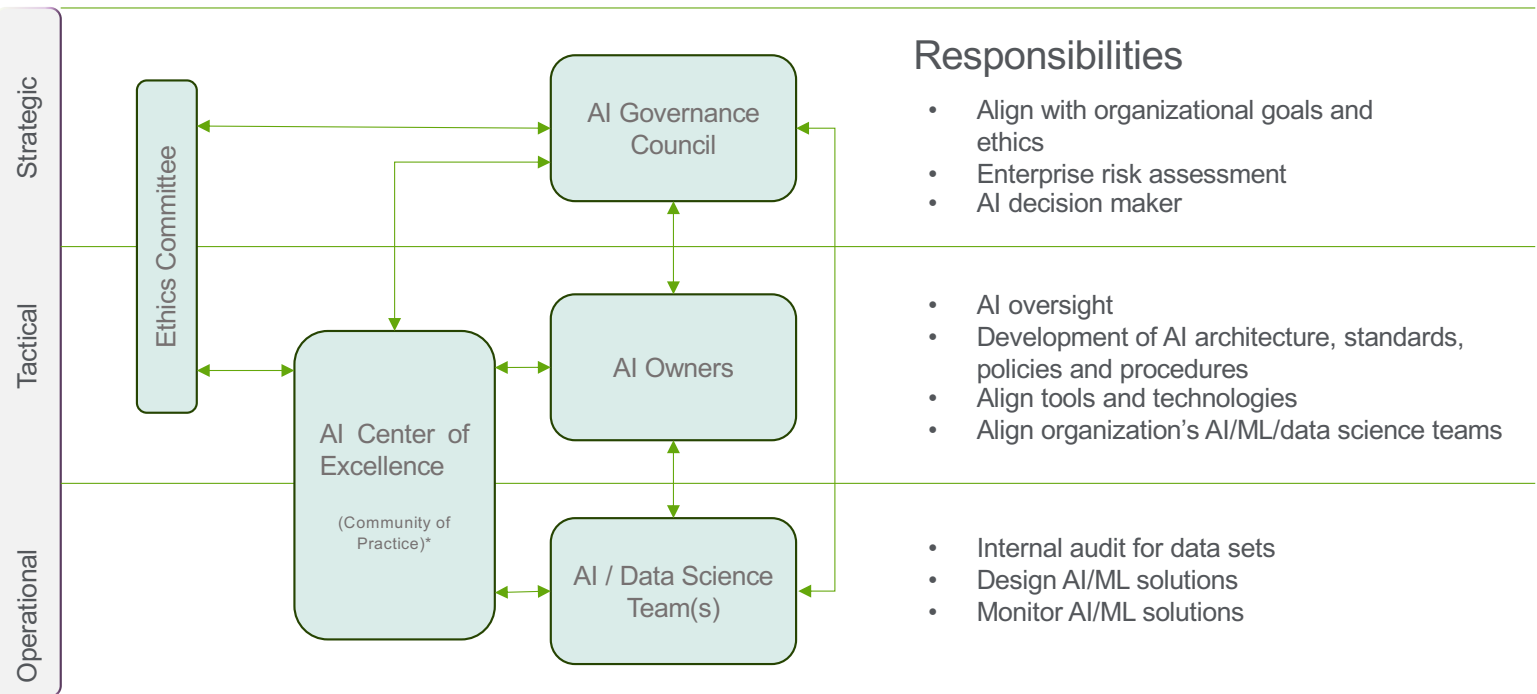
Integrated AI Governance

Risks

As the risk of an AI project increases, higher levels of governance become necessary.

Governance Factors

- Development difficulty
- Data sensitivity
- Need for accuracy
- Regulatory pressure
- Amount of change required



Responsibilities

- Align with organizational goals and ethics
- Enterprise risk assessment
- AI decision maker
- AI oversight
- Development of AI architecture, standards, policies and procedures
- Align tools and technologies
- Align organization's AI/ML/data science teams
- Internal audit for data sets
- Design AI/ML solutions
- Monitor AI/ML solutions

Policy and Procedure Addressing Key Risks



Establish AI Risk
Management



System Training



Ongoing
Monitoring



Committee/Board
Reporting

Key AI Policy and Procedure Domains



Algorithm processing and validation (i.e. credit approval)

- ▶ Manual validation procedures
- ▶ Ongoing model validation procedures (independent of development and administrative access)
- ▶ Expected decision boundaries to detect “AI Drift”



GenAI algorithm training and monitoring

- ▶ Threshold and confidence percentages used in decision making
- ▶ Procedures for data and/or prompts encountered outside of the algorithm’s trained purpose
- ▶ Human validation of algorithm processing and output



GenAI Specific Change Management

- ▶ AI Algorithm training and testing
- ▶ Analysis and validation of GenAI impact on business processes
- ▶ User acceptance testing
- ▶ Acceptable use including specific requirements for data used in production algorithm

Key Cyber Policy and Procedure Domains

Data Leakage

- ▶ Secure the system (physical, data, and model)
- ▶ Defend against testing and training attacks (encryption, statistical verification, algorithmic improvements, cross validation of datasets)
- ▶ Test for evidence of a successful attack (Integrity violation, availability violation, privacy violation – to learn about the model and its data)
- ▶ Includes information from outside the training dataset used to create the model.

Adversarial Attack

- ▶ Data or algorithmic compromise
- ▶ Data Masking or Manipulating – confuses the AI
- ▶ Synthesizing or Poisoning data – Misleads the AI
- ▶ Example: IBM researchers trick ChatGPT into hacking (<https://www.axios.com/2023/08/08/ibm-researchers-trick-chatgpt-hacking>)

Common Integrity Attacks specific to

- ▶ Direct or Indirect (i.e. a website that the AI reaches out to for input) Parameter Injections
- ▶ Infection (i.e. Malware) – when the AI reaches out to other sources, or if you download models from an infected source
- ▶ Evasion – modification of the inputs to come up with unintended results by fooling the AI
- ▶ Poisoning – addition of erroneous data used to train the AI (doesn't take large amounts of error to cause wrong results)
- ▶ Extraction – query/ask the AI for information to gather the sensitive data and functionality
- ▶ Denial of Service – overload the system



Discussion Question

Does your organization have a formal AI program?

- a. No.
- b. Sort of: IT and/or business operations management provide guidance and guardrails over AI use.
- c. Yes: Our organization has a formal AI steering committee, program and supporting policies and procedures





AI Use Cases

Basic uses of AI



Tools your organization might allow

- ▶ Co-Pilot (integrated with Microsoft O365)
- ▶ Gemini (integrated with Google)
- ▶ DALL – E 3



How can these tools help in every day (examples)

- ▶ Draft emails
- ▶ Content creation
- ▶ Policy development

What to look out for

- ▶ AI responds based on all of the content available to the tool, so if using a tool with access to all of the internet, there may be inaccurate information produced. **Always review for accuracy.**
- ▶ If your organization doesn't have guardrails on the tool being used, need to be very careful about feeding it sensitive information about the organization or customers. **Know where the data is going.**
- ▶ Depending how you ask your question, you might not get the details you were expecting. For larger content, like policy development, you may need to break it down into smaller detailed questions. **Fine tune your AI prompts.**



Example

To develop an Artificial Intelligence Policy using OpenAI:

Prompt: “Create an outline for an artificial intelligence policy for a bank”

Creating an artificial intelligence (AI) policy for a bank involves outlining principles, guidelines, and governance structures to ensure the responsible and effective use of AI technologies. Here's a comprehensive outline for such a policy:

1. Introduction

- **Purpose:** Define the objectives of the AI policy, emphasizing the role of AI in enhancing banking services and operations.
- **Scope:** Specify the policy's applicability across various departments and functions within the bank.

2. Governance Framework

- **Oversight:** Establish an AI governance committee responsible for overseeing AI initiatives and ensuring compliance with the policy.
- **Roles and Responsibilities:** Define roles for key stakeholders, such as data scientists, IT, legal, compliance, and risk management teams.

3. Ethical Principles

- **Fairness:** Ensure AI systems are designed to treat all customers equitably without bias.
- **Transparency:** Promote transparency in AI decision-making processes, making them understandable to stakeholders.
- **Accountability:** Assign accountability for AI systems' outcomes and maintain mechanisms for addressing grievances.

4. Data Management

- **Data Quality:** Establish standards for data accuracy, completeness, and timeliness used in AI systems.
- **Privacy and Security:** Implement measures to protect customer data privacy and ensure data security in compliance with regulations.

5. Risk Management

- **Risk Assessment:** Conduct regular risk assessments to identify and mitigate potential risks associated with AI applications.
- **Monitoring and Evaluation:** Develop systems for ongoing monitoring and evaluation of AI systems to detect anomalies and ensure performance aligns with objectives.

6. Compliance and Regulatory Considerations

- **Legal Compliance:** Ensure AI systems comply with existing banking regulations and data protection laws.
- **Industry Standards:** Adhere to industry best practices and standards for AI implementation.

7. Innovation and Research



Example

Fine Tuning: Then take each area one by one to spell out the details. For example: “provide a narrative for governance framework section of an AI policy using NIST framework”

You would need to modify some of the wording to model your environment. However, if you started with a scenario describing the internal control environment, the details would be included in the narrative.

Even if you don’t like the way it’s written, you will have the relevant content to use as a guide.

Governance Framework Narrative

In the rapidly evolving landscape of artificial intelligence, establishing a robust governance framework is crucial for ensuring the responsible and ethical deployment of AI technologies within the banking sector. Guided by the principles of the NIST AI Risk Management Framework (AI RMF), our governance framework is designed to manage AI-related risks while optimizing its benefits, aligning with both organizational goals and regulatory requirements.

Oversight and Accountability

At the heart of our governance framework is the establishment of an AI governance committee, a dedicated body responsible for overseeing AI initiatives across the bank. This committee serves as the central authority, ensuring that AI systems are developed and deployed in alignment with our strategic objectives, ethical standards, and regulatory obligations. By defining clear roles and responsibilities for data scientists, IT professionals, compliance officers, legal advisors, and risk managers, we create an environment of accountability where every stakeholder understands their contribution to the AI lifecycle.

Risk Management

Adhering to the risk management principles outlined by the NIST AI RMF, our governance framework emphasizes proactive risk identification, assessment, and mitigation throughout the AI system’s lifecycle. We implement comprehensive processes to monitor AI systems continuously, ensuring they operate within acceptable risk

parameters and deliver expected performance outcomes. By embedding risk management into every phase of AI deployment, we safeguard against potential adverse impacts while maximizing technological benefits.

Policy and Process Integration

Our governance framework integrates AI practices seamlessly into existing organizational policies and processes, creating a cohesive approach to risk management and compliance. We establish protocols for decision-making and escalation concerning AI system management, ensuring that our governance practices are not only effective but also adaptable to the changing technological and regulatory landscape.

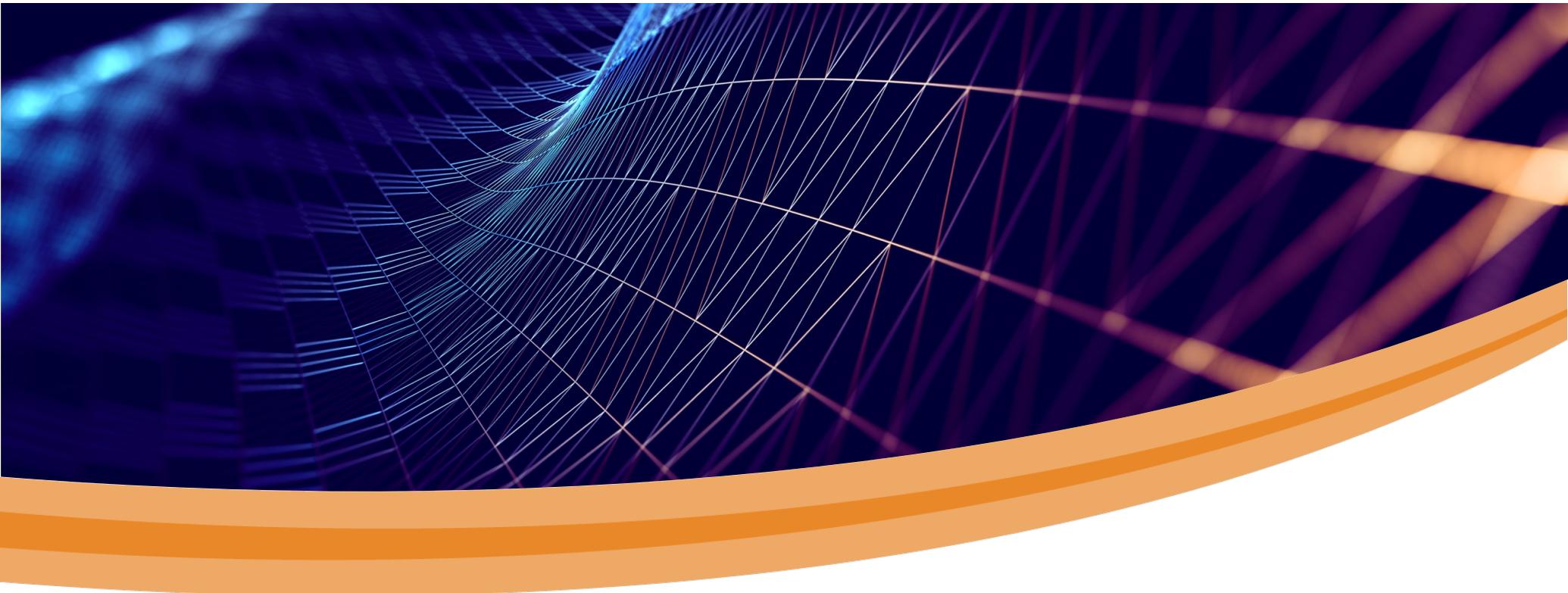
Stakeholder Engagement

Recognizing the importance of transparency and collaboration, our framework fosters active engagement among stakeholders. Through structured communication channels, we facilitate dialogue that enhances understanding and accountability across all levels of the organization. Education and awareness initiatives are integral to our approach, empowering stakeholders with the knowledge needed to navigate AI technologies, risks, and ethical considerations confidently.

Continuous Improvement

In alignment with the NIST AI RMF, our governance framework commits to continuous improvement. We regularly review and refine our practices to reflect advancements in AI technology, shifts in regulatory landscapes, and changes in organizational priorities. By supporting ongoing research and innovation, we ensure that our AI capabilities evolve responsibly, adhering to ethical standards and robust risk management practices.





Where to Start

AI Risk Framework

Consider your organizations maturity across the core risk domains and capabilities

	Security	Transparency	Accountability	Privacy	Fairness	Risk Based	Reliability & Resiliency
Principles	AI systems are protected from logical and physical threats to ensure the integrity of the AI system.	AI systems are explainable to stakeholders and users are informed of use of AI and potential impacts	Ownership and responsibilities are clearly defined for governing the use of AI technology	AI systems are in compliance with privacy controls to protect individual privacy rights.	AI systems are set up with minimal bias or favoritism to ensure equitable outcomes	AI systems are classified using a risk-based approach to evaluate and mitigate risks introduced	AI systems are reliable and resilient to enable business processes and minimize the impact of disruptive events
Capabilities	<ul style="list-style-type: none"> • Security Controls • Software supply chain risk • Vulnerability management • Data protection • SSDLC • Access controls • Change management 	<ul style="list-style-type: none"> • Fit for purpose • Explainability • Disclosure of usage and impact • Communication with stakeholders 	<ul style="list-style-type: none"> • Oversight body • Roles and responsibilities • Strategy, policies, standards and procedures • Human review and control • Stakeholder inclusiveness • Cost of ownership 	<ul style="list-style-type: none"> • Privacy regulatory compliance • Data training and use • Privacy impact assessment 	<ul style="list-style-type: none"> • Quality of service • Reducing impact on marginalized groups • Allocation of adequate resources • Data bias, detection, test and migration 	<ul style="list-style-type: none"> • AI Model Risk • AI system risk classification • AI risk/impact assessment • Risk mitigation • Risk tracking and reporting • Third party • Intellectual property • Regulatory compliance 	<ul style="list-style-type: none"> • Evaluation of potential failure, error and mitigation plan • AI drift monitoring • Operational resiliency • System health check • Ongoing monitoring • Optimization



Phased AI Evaluation Approach

With many institutions in the early stages of AI adoption, a two-phased evaluation approach will help provide the greatest insight and value-driven observations from the evaluation.

Assessment Phase 1

Objective: Discover and risk assessment

Core Activities

- Evaluation of AI Governance and Strategy
- Identification of AI use
- Assessment of AI risk
- Evaluation of data privacy and protection
- Consideration of ethical use

Primary Outcome: Validation of AI governance, program, risks and controls

Primary Deliverables

- High-level AI risk profile
- AI inventory and risk assessment
- Summary governance, policy and procedure gap assessment

Assessment Phase 2

Objective: Testing of AI procedures and controls

Core Activities

- Validation of AI Governance and Strategy
- Refinement of AI risk profile, data privacy requirements and ethical use considerations
- Inventory of internal and external AI platforms
- Testing of AI procedures and controls

Primary Outcome: Validation of AI governance, program, risks and controls

Primary Deliverables

- In-depth AI risk profile
- AI risk and control matrix
- Detailed governance, policy and procedure gap assessment

Thank you

Contact Us

- ▶ **Scott Peyton**, CISSP, CISA, DDN.QTE, NACD.DC
 - ▶ *National Practice Leader, Risk Advisory*
 - ▶ **Scott.payton@cbh.com**
- ▶ **Kurt Manske**, CISSP, CISA, DDN.QTE, NACD.DC
 - ▶ *National Practice Leader, Cybersecurity and Information Assurance*
 - ▶ **Kurt.manske@cbh.com**
 - ▶ **913.915.2666**

About Cherry Bekaert

"Cherry Bekaert" is the brand name under which Cherry Bekaert LLP and Cherry Bekaert Advisory LLC, independently owned entities, provide professional services in an alternative practice structure in accordance with applicable professional standards. Cherry Bekaert LLP is a licensed CPA firm that provides attest services, and Cherry Bekaert Advisory LLC and its subsidiary entities provide tax and advisory services. For more details, visit cbh.com/disclosure.

This material has been prepared for general informational purposes only and is not intended to be relied upon as tax, accounting, or other professional advice. Before taking any action, you should consult a professional advisor familiar with your particular facts and circumstances.



cbh.com

