BerryDunn

ELEVATE

Annual Commercial Summit | 2025

AI in the Enterprise: Critical Controls and Next Steps After Implementation

BerryDunn

December 11, 2025

Agenda highlights

01 The Transformation of AI

02 Risks of AI

03 Governing AI in a Business

04 AI Compliance and Assessments

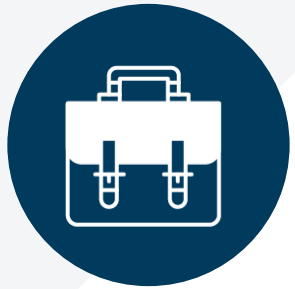
Learning objectives

- **Identify** the key risks that emerge after AI implementation, including data security, model integrity, bias, and regulatory exposure.
- **Understand** the critical governance frameworks, access controls, and monitoring practices needed to manage enterprise AI responsibly.
- **Apply** practical risk assessment and control strategies to strengthen the resilience and long-term value of AI initiatives.

Section 1

The Transformation of Artificial Intelligence

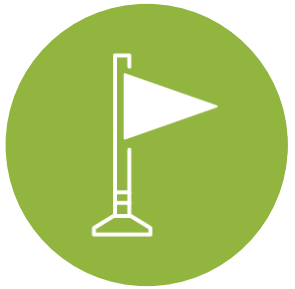
How we got here



Organizations have been talking about AI for five-plus years now.

Rapid advancements in technology.

Millennials, Generation Z are all but demanding AI in the workplace.



Your employees are likely using AI even if you don't formally have it (red flag!)

Now is the time to integrate AI use into your policies and GRC programs.

AI is everywhere

Transforming from a buzz word to a practical tool

78% of companies globally have implemented AI in some part of their organization. Most common areas are marketing, customer service, HR, and information security

1% of companies say their use of AI is “mature”

92% of companies plan to invest in AI use over the next three years

64% of leaders believe AI will improve productivity

80% of those using AI have reported efficiency gains

There is excitement for AI, but...

- 43% of leaders say that data issues are a significant roadblock to demonstrating AI's value to their organization
- 56% of organizations say data reliability is acting as a barrier to piloting AI
- …the old accounting adage "garbage in = garbage out" in any system. **This is a critical hurdle to clear for AI**

Before any organization implements AI, it is beyond critical that you have:

- Data and system inventory
- Data management process
- Data quality programs
- Data classification

Types of AI

A quick refresher

Generative AI

The AI you are likely using; this is CoPilot, ChatGPT, etc.

Likely where your organization has implemented AI; prompts and questions result in answers or generated content.

Agentic AI

AI that can accomplish a specific goal with limited supervision.

This is where organizations want to be. Agentic AI can improve efficiency if it works as designed.

Polling question #1

Section 2

Artificial Intelligence Risks

Risks of using AI

Risk	Impact	Mitigation
Personnel are using public AI for work purposes	• You may be violating intellectual property rights: AI uses information that is on the web, much of which is trademarked (see below). • Exposing your business data to the internet. AI systems take what you provide it and use it to “learn” from. • Exposing your customer’s data to the internet without their consent. • Personnel could be using AI generated products/information that isn’t vetted or correct.	• Do NOT allow the use of Chat GPT and other public facing, non-enterprise AI systems for work related tasks • Use scanning tools to review files and information for AI generated material, including trademarked material • If AI is used, require that sources are provided
Over-dependence on AI	• AI generated materials are not reviewed or validated • Errors in products or reports • Biased results	• Always have a human in the loop (HITL) as a control that involves anything with AI (the plane mostly flies itself, but the pilot is there just in case) • Testing AI output and confirming sources and its correctness • Understand how AI decisions were made – traceability

Risks of using AI

Risk	Impact	Mitigation
Data Access	• AI uses PII, confidential, or restricted data to make decisions or provide content	• Data classification policy integrated with AI access • Access policies • Human in the loop review
Reputational risk with customers	• Garbage in = garbage out… If not vetted, low-quality products, incorrect information, appears shortcuts were taken	• Human in the loop review • Require sources for all outputs • Traceability and decision logic review
Data Bias	• Decision-making and output generate biased results	• Extensive testing before implementation • Frequent assessments of data output with a process to retrain AI if bias results are detected • Human in the loop review of results
Intellectual Property Violations	• AI uses trademarked information and media	• Traceability • Data management • Require sources

Risks of using AI

Risk	Impact	Mitigation
Cyber Security	• Attacks on AI to mess with outputs – fake data, bad data, biased data, etc. • AI can create deepfakes to deceive • Malicious attackers use AI to gather information about your organization	• Access policies • Human in the loop review • Machine learning policies and governance • Security monitoring tools
Job loss	• AI replaced roles within the organization	• Re-train employees on using AI tools and focusing on higher value

AI mistakes make the news

Deloitte was caught using AI in $290,000 report to help the Australian government crack down on welfare after a researcher flagged hallucinations

NBC News

Australian lawyer sorry for AI errors in murder case, including fake quotes and made up cases

Defense lawyer Rishi Nathwani, who holds the prestigious legal title of King's Counsel, took "full responsibility" for filing incorrect...

Reuters

Large US law firm apologizes for AI errors in bankruptcy court filing

Gordon Rees Scully Mansukhani, an 1,800-lawyer firm that had been representing a creditor in an Alabama hospital bankruptcy case, in a Thursday...

Deloitte allegedly cited AI-generated research in a million-dollar report for a Canadian provincial government

Air Canada pays damages for chatbot lies

In February 2024, Air Canada was ordered to pay damages to a passenger after its virtual assistant gave him incorrect information at a particularly difficult time.

AI Misfire: Teen Handcuffed After AI Mistakes Doritos for Gun

AI Misfire: Teen Handcuffed After AI Mistakes Doritos for Gun. AI error leads police to handcuff teen after mistaking Doritos for a gun, raising...

NBC News

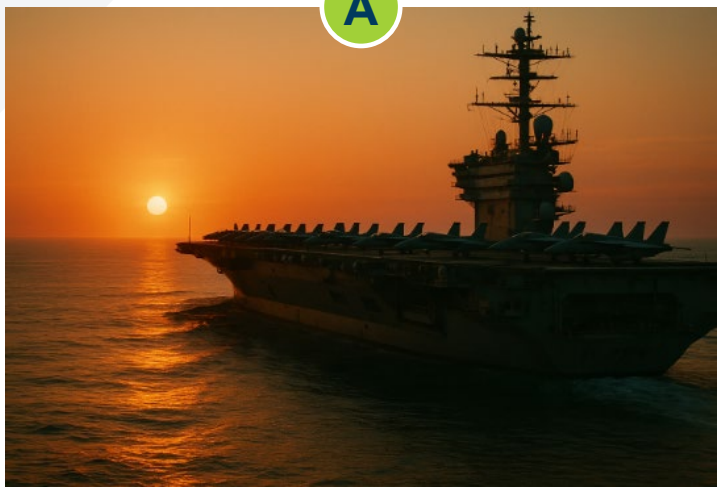
Driverless Waymo vehicle goes through tense police stop in L.A.

Video shows the Waymo passing a white pickup pulled over in Los Angeles by several police cruisers with their lights flashing as the...

Polling question #2

Which one is real?

A



B

C

D

Section 3

AI Governance – Effective ways to Manage AI

Polling question #3

Why AI governance?

AI is constantly changing, and it needs to be managed

- AI governance is critical for
  - Maintaining ethical standards
    - Establishing processes and controls for testing and avoiding bias, while enforcing need for explainability and traceability
    - Maintaining and revisiting how AI is used in business and if it aligns with your goals and ethics
  - AI models can “drift” impacting the quality and accuracy of outputs
    - Governance sets tone for procedures (including machine learning, testing, etc.) and for assessments and audits

Select a framework. Many current IT frameworks work for AI, but several have been updated for AI considerations. For this discussion we'll focus on ISACA's CoBIT framework and how to integrate AI into that.

Organizations must integrate AI into your overall GRC program

- Though somewhere between 78% – 88% of organizations report using AI, only about 30% have considered controls and governance of AI in their management programs

Organizational structure

Assigning leadership of your AI program is paramount. Someone must make important decisions on policy and strategy as AI can be very impactful to business.

- Innovation Committees – to provide strategy and guidance, sponsor community of practices to knowledge sharing
- Chief Innovation Officer/ Chief Technology Officer
- Legal involvement in policy and use decisions
- Information Security involvement
- Risk Officer

Principles, policies, and procedures

Policies must be updated to reflect how your organization uses AI. Considerations include:

- Acceptable use
- Access policies
- Security policies
- Communication and disclosure
- Risk assessment should be completed and mitigating controls established
  - Human in the loop
  - Data classification
  - Traceability and accountability

The other areas of AI GRC will fall into place naturally as these two are addressed

Section 4

AI Compliance and Regulations

Monitoring and auditing AI is critical to your success

Like with other technology, continuous monitoring of AI is imperative for your success.

1. Regular reviews of how AI is being used in your organization and understanding the impacts to controls and processes
2. Regular audits of AI output needs to be done to detect biased, AI drift, AI slop, and AI hallucinations and accuracy
3. If AI is new to your organizations, consider an AI assessment of your governance program and controls
4. If you have a SOC exam, ensure controls are updated to address how you use and manage AI

AI regulation

- There is currently no approved federal regulation on the development or use of AI
  - Some states are looking into regulations (this is a hot topic issue)
- The EU AI Act is considered the gold standard of AI regulation, though some claim this limits the development of AI
- There are plenty of frameworks to consider as guidance. ISACA, Institute of Internal Auditors, NIST AI Risk Management Framework (RMF) among the most popular

We can help!

- Our team of Certified Information System Auditors have ISACA's new Advanced in AI Auditing certificate
- We have developed a questionnaire for you to gauge your AI governance maturity
- Using the results of that, we offer an assessment of your organization's AI governance and provide recommendations and guidance on how to mature the program
- Within the next few months, we will offer AI audits of your output to test for bias, traceability, and accuracy
- Sign up for more information!

Questions?

BerryDunn

ELEVATE

Annual Commercial Summit | 2025

Chris Ellingwood, CISA

Principal | Berry, Dunn, McNeil & Parker, LLC
Practice Area Lead, IT Assurance and SOC Services

802.310.0361
cellingwood@berrydunn.com