# Strike First, Audit Hard: No Mercy for AI Risk

MAY 11, 2026

# Our Agenda Today

1. Why does this matter?
2. AI Context
3. Auditing Scope and Steps
4. Conclusion

# With You Today


**ANDREW BELSICK**

Director, Cyber Practice

abelsick@bdo.com



**KELLY AUSTIN**

Senior Associate, Cyber Practice

kaustin@bdo.com

# Why does this matter?

1

WHY THIS MATTERS

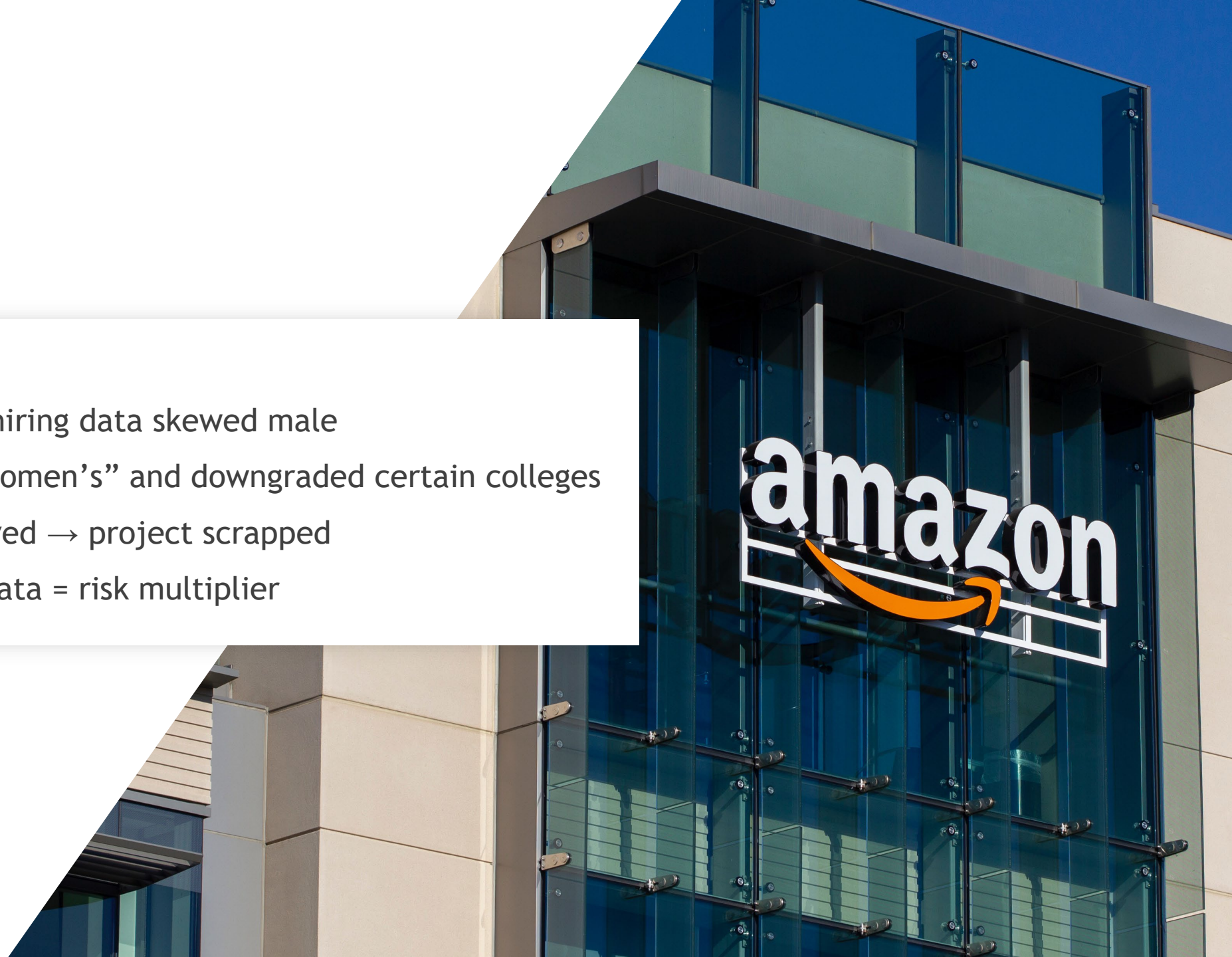
# AI In the Wild

- McDonald’s Drive-Thru
- AI-powered order taking piloted in 100+ U.S. restaurants (IBM partnership)
- Viral videos of bizarre order errors (noise, accents, edge cases)
- System removed nationwide in 2024
- Audit lesson: Lab accuracy ≠ real-world performance

WHY THIS MATTERS

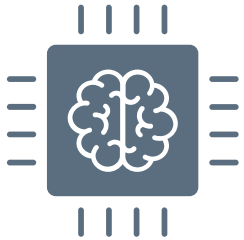
# AI In the Wild

- Amazon Hiring
- Trained on 10 years of hiring data skewed male
- Penalized terms like “women’s” and downgraded certain colleges
- Bias could not be removed → project scrapped
- Audit lesson: Training data = risk multiplier



WHY THIS MATTERS

# AI Adoption is Ever-Increasing



95% of companies using/ experimenting with GenAI[1]

GenAI work usage grew 39% in 9 months[2]

Executives expecting ROI and efficiency gains

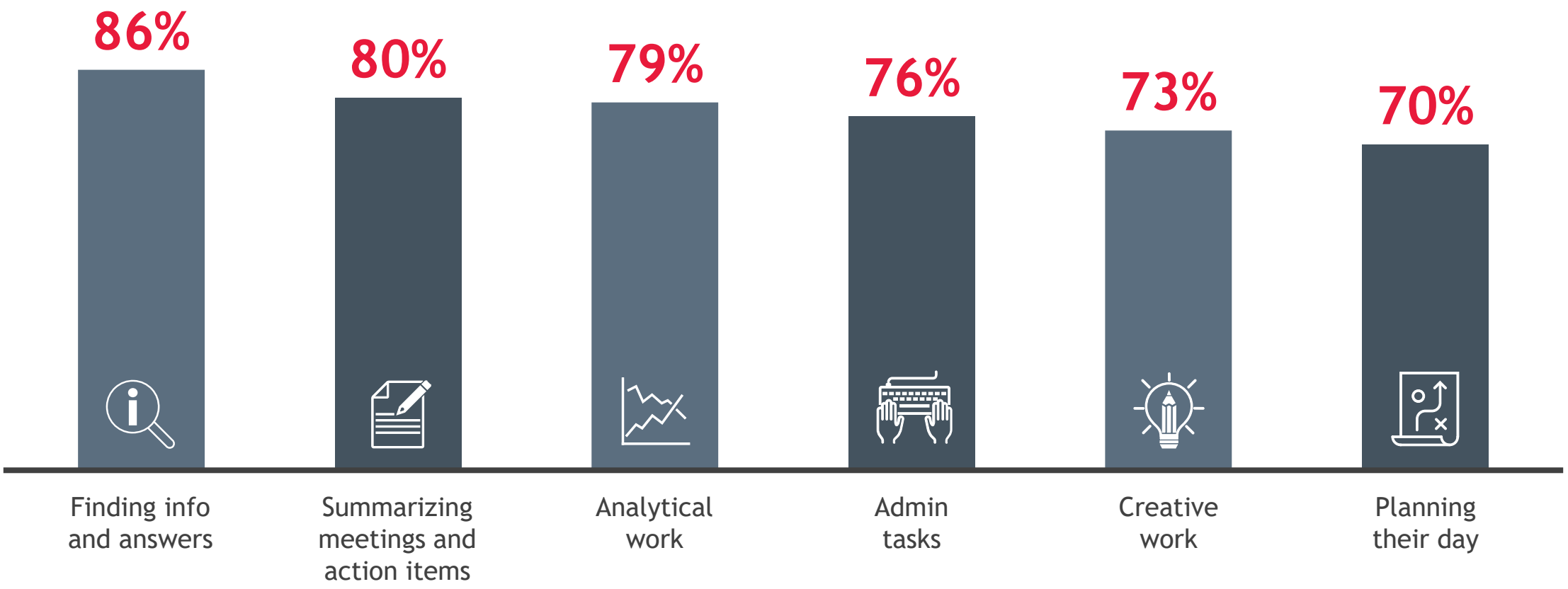
Workers seeking productivity boosts

~95% of AI pilots fail[3]

1. Bain, 2015
2. University of Phoenix
3. Massachusetts Institute of Technology

WHY THIS MATTERS

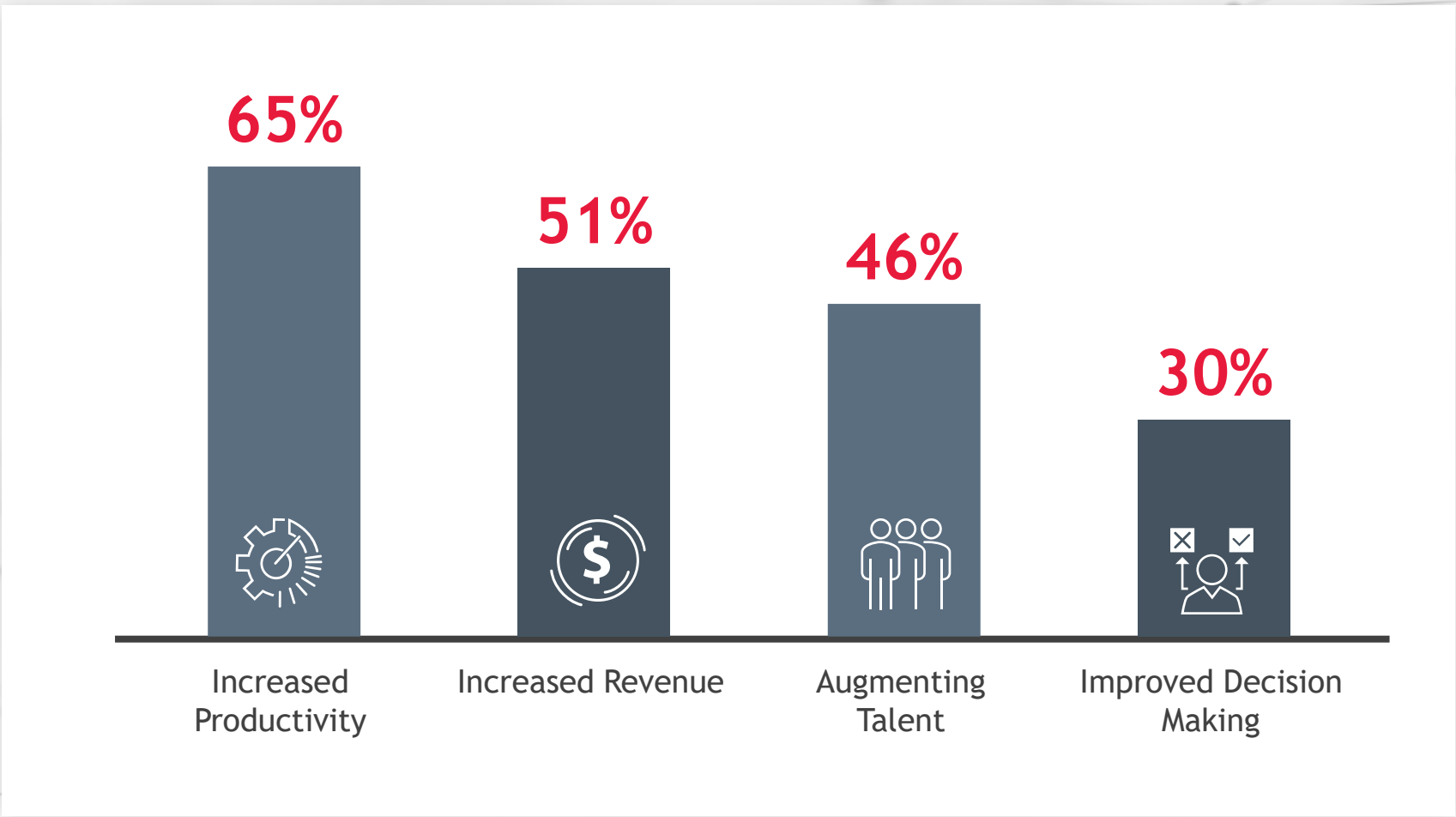
# What Employees Want




Source: 2024 Work Trend Index Annual Report from Microsoft and LinkedIn

WHY THIS MATTERS

# What Executives Want




**Source:** 2024 McKinsey US CxO Survey

# Digital Disruption = Audit Risk

IIA asked global internal audit leaders how they rank risk right now and in the next three years.

- 34% say digital disruption is one of the top five risks
- 55% say digital disruption will be top five in three years

The Institute of Internal Auditors

TONE at the TOP

WHY THIS MATTERS

# The Auditor's Role

Provide assurance over trustworthy AI

Evaluate governance, data, and model controls

Identify shadow AI and unmanaged adoption

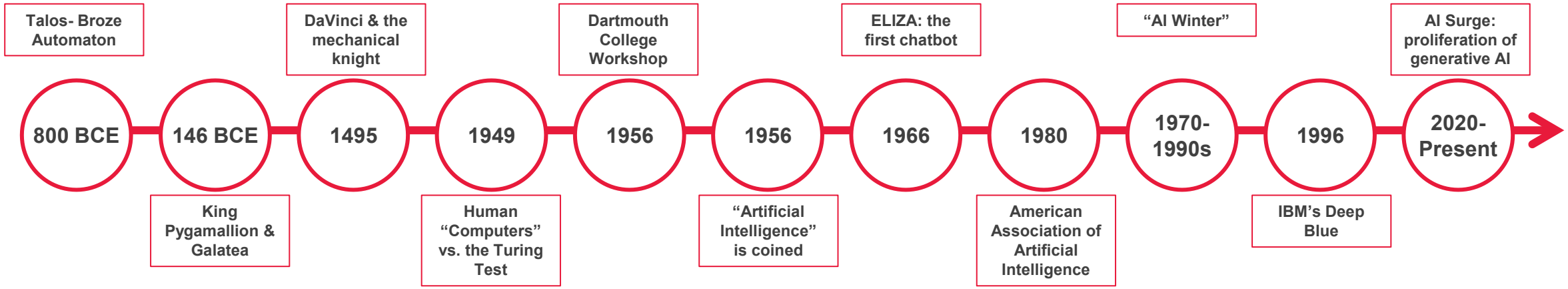
Enable safe, compliant, strategic AI usage

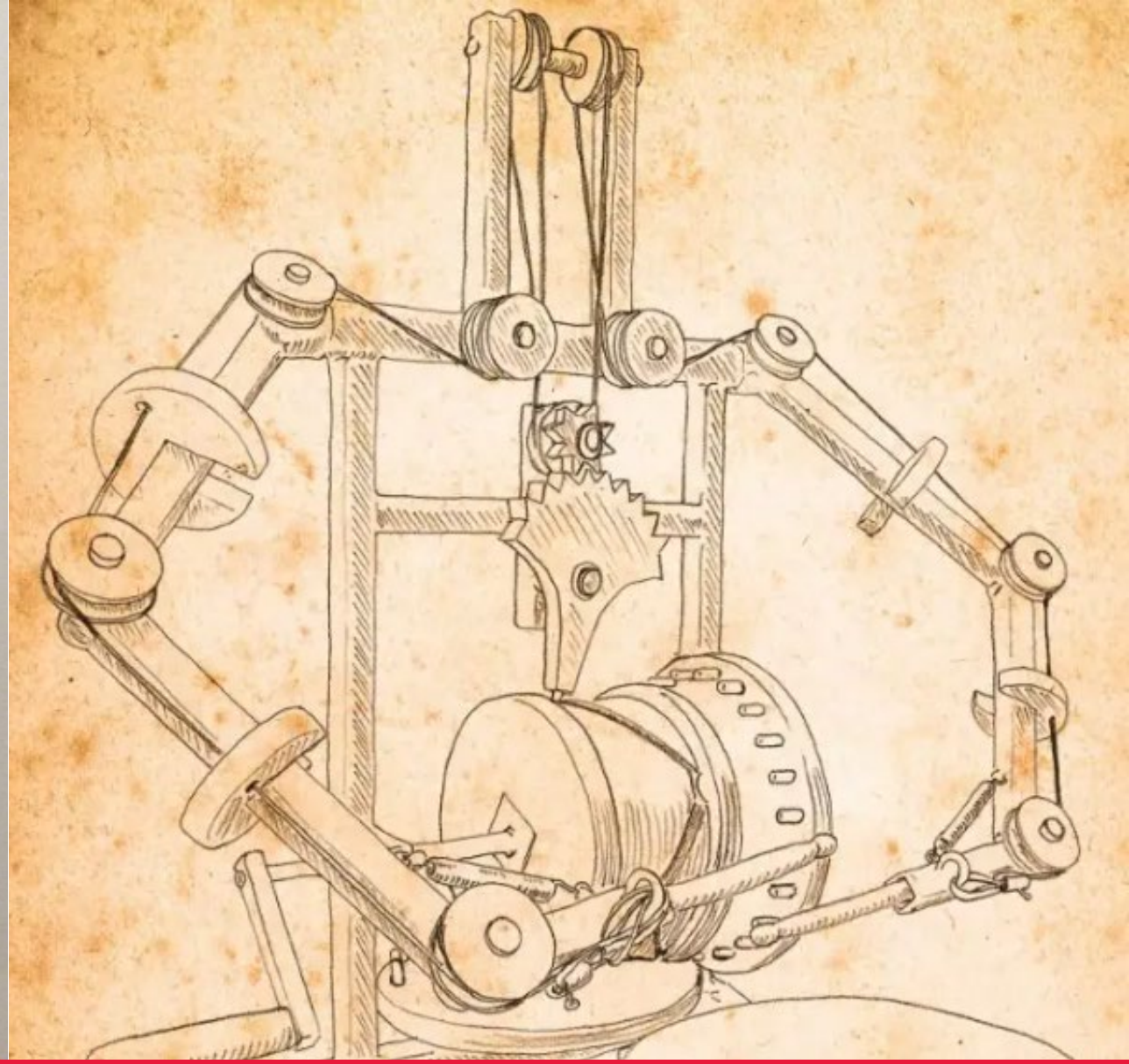
Bridge business, technology, cybersecurity, privacy, and risk

# AI Context

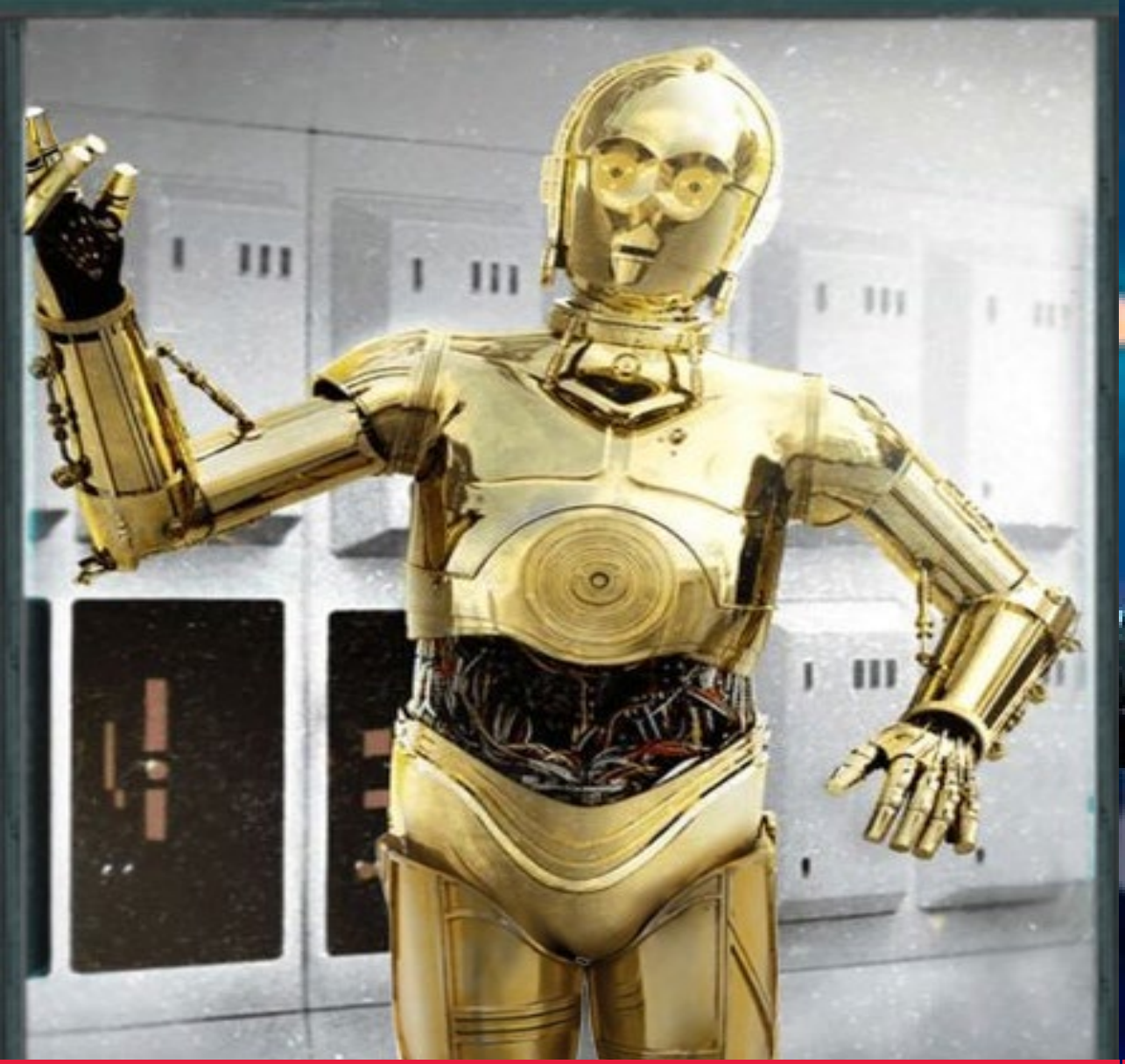
2

# The Origins of Artificial Intelligence – Dreams of Mechanical Minds





# DaVinci’s Mechanical Knight



C3PO by Anakin Skywalker

T-800 by Cyberdyne Systems

AI CONTEXT

# AI Definition Guide

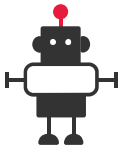
**AI:** The umbrella of computer science capabilities focused on building smart machines capable of performing tasks that typically require human intelligence.

**GENERATIVE AI:** Algorithms (such as ChatGPT) that can be used to create new content, including audio, code, images, text, and videos. Think of it as a highly skilled assistant that can generate creative and original ideas.

**DEEP LEARNING:** An advanced branch of machine learning that mimics the neural networks of the human brain to process data and create patterns for decision making.

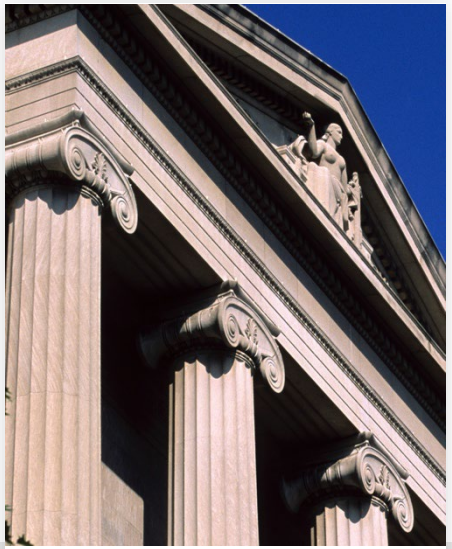

**MACHINE LEARNING:** A field of AI that enables software applications to become more accurate at predicting outcomes without being directly programmed to do so.

**PREDICTIVE ANALYTICS:** The use of data, statistical algorithms, and machine learning techniques to identify the likelihood of future outcomes based on historical data. It helps organizations make informed decisions and anticipate future trends.



**AGENTIC AI:** Artificial intelligence that can make decisions and take actions on its own to achieve specific goals, rather than just following instructions.

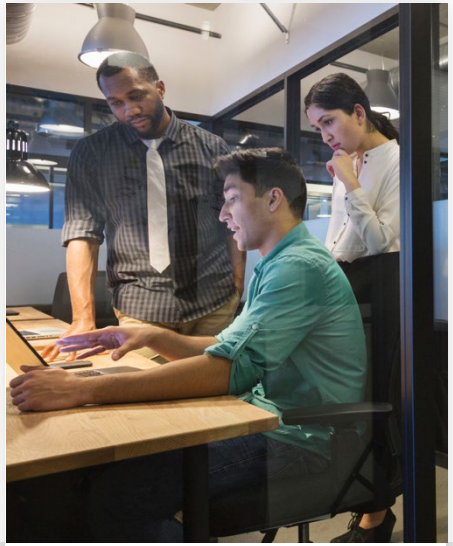
# Emerging AI Regulations



**RAPIDLY EVOLVING LEGAL LANDSCAPE**

**RISK-BASED REGULATORY APPROACH**

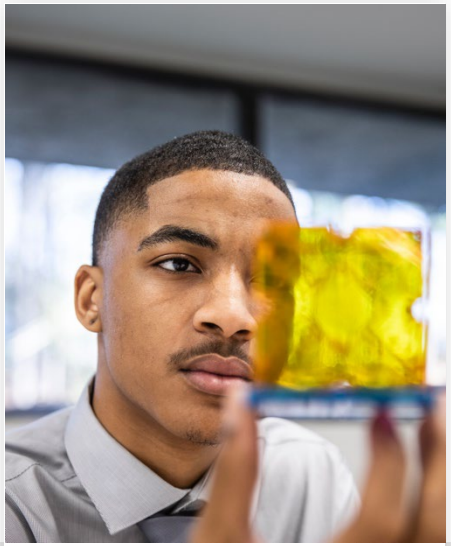
**KEY JURISDICTIONS INTRODUCING LAWS**



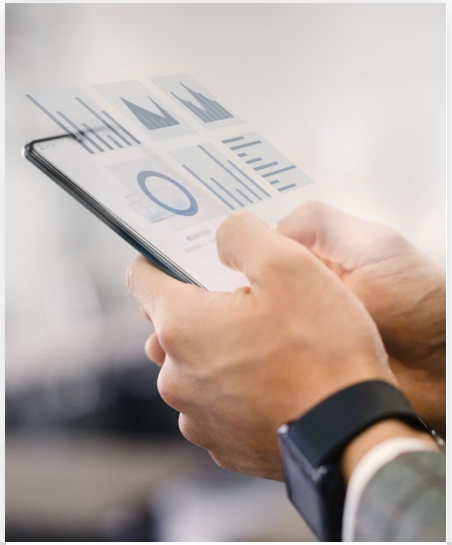
**SECTOR-SPECIFIC COMPLIANCE**

**GLOBAL TREND**

# Global Standards and Frameworks

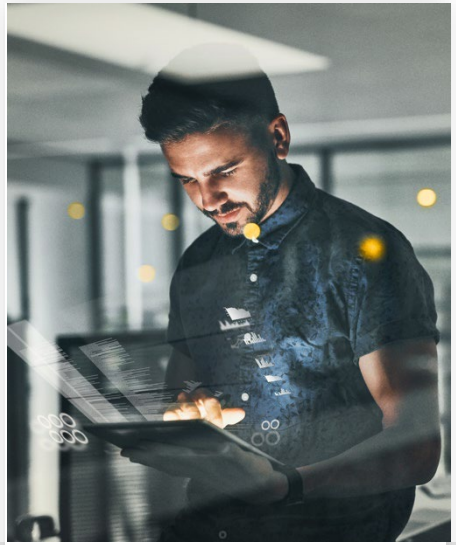


ISO STANDARDS

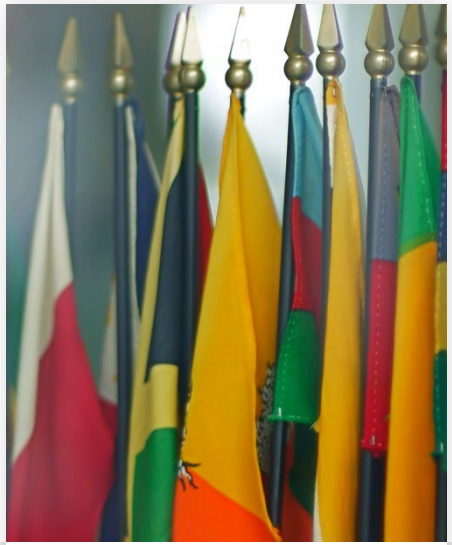


RISK MANAGEMENT FRAMEWORKS

ETHICAL AND GOVERNANCE FRAMEWORKS



INDUSTRY ADOPTION



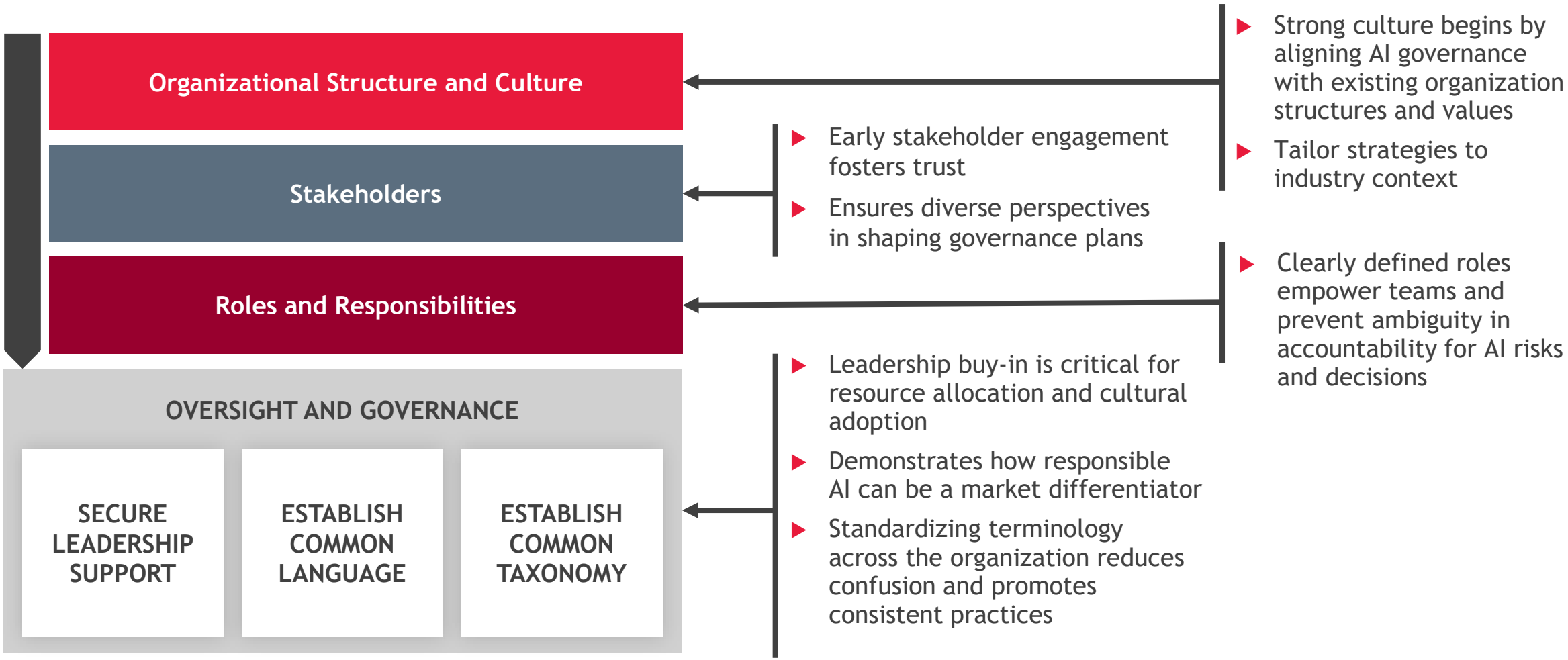
INTERNATIONAL STANDARDS

# The Principles of Responsible AI

The core principles of responsible AI define its use, support governance, and guide employee training. They can help you assess and mitigate risk, implement effective controls, and assist with regulatory compliance.

FOUNDATIONS FOR A RESPONSIBLE AI CULTURE

# Building a Culture of Responsible AI Development



# Risks of AI

## Privacy and Cyber Security

- Privacy
- Identity
- Data Security
- Secure Cloud
- Incident Response

## Responsibility & Accountability

- Acceptable use
- Societal/ Market Impacts
- Regulatory Environment
- Accountability of Outcome

## Misinformation & Inaccuracies

- Output Integrity
- Validation
- Intellectual Property Concerns

## Bias and Discrimination

- Unintended Bias
- Unrecognized data patterns
- Market Fit

## Regulations and Requirements

- Regulatory Alignment
- Governance of Program

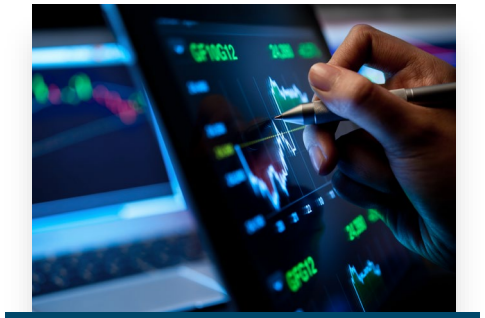
# Auditing Scope & Steps

3

# Types of AI Audits

## Data Audit

- Accuracy
- Completeness
- Representation
- Quality
- Governance

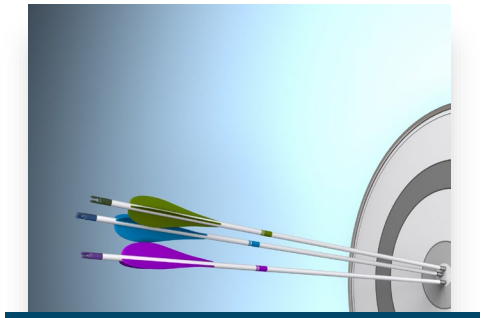


## Model Audit

- Pre-deployment
- Model validation
- Accuracy, fairness, robustness
- Model risk management

## Process & Control Audit

- Integration of AI into processes
- Segregation of duties
- Human review
- Change management



## Outcome Audit

- Human intervention
- Decision-making
- Error rate
- False positives or negatives
- Bias indicators
- Hallucinations

## Bias & Performance Audit

- Independent algorithm audit
- Inherent bias
- Results are published

# Audit Scope

## Business Impact

- What problem is AI solving?
- What type of AI is being implemented?
- Assistive vs. automated decisions
- Criticality (financial, safety, regulatory)
- Customer-facing impacts
- Failure modes and business consequence

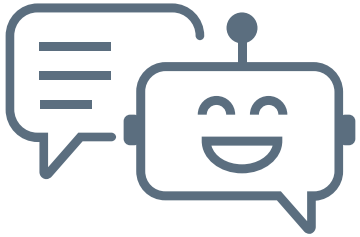
## Data Inputs/Outputs

- Training data sources and quality
- Personal/sensitive data usage
- Data lineage, retention, cross-border flows
- Output accuracy, hallucination risk
- Where outputs travel next

## Model Lifecycle

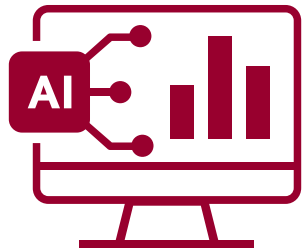
- Design and purpose
- Training and documentation
- Validation and stress testing
- Deployment controls
- Monitoring and drift detection
- Retirement

# Use Case Examples



Customer-facing
Chatbot:

**“Daniel”**

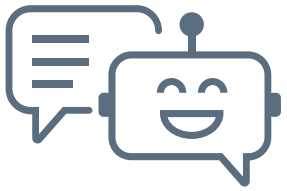



3rd Party
GAI Tool:

**“Johnny”**

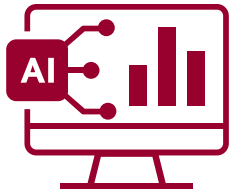
AUDIT

# Governance



## DANIEL CHATBOT

- Ownership and accountability
- Alignment to policies and standards
- Model documentation and transparency
- Monitoring
- Regulatory implications
- 3rd party oversight for components

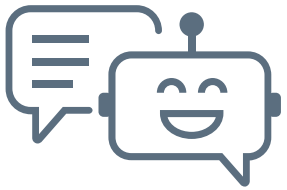



## JOHNNY VENDOR GAI

- Acceptable use
- Shadow AI
- Vendor risk management
- Human review

AUDIT

# Security/Privacy



## DANIEL CHATBOT

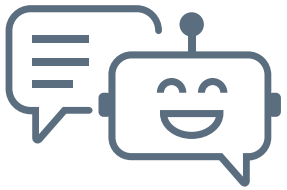
- Prompt injection
- API security
- Logging/anomaly detection
- Transparency requirements


## JOHNNY VENDOR GAI

- Restrictions on sensitive data input
- Data residency
- DLP

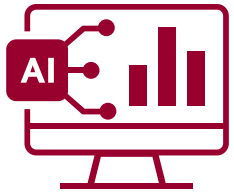
AUDIT

# Data Quality and Ethics/Bias



## DANIEL CHATBOT

- Knowledgebase accuracy/freshness
- Hallucination monitoring
- Bias in responses
- Metrics for human escalation

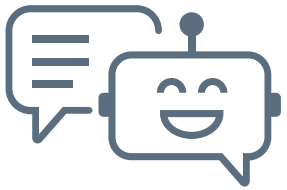



## JOHNNY VENDOR GAI

- Human review
- Detection of bias/discriminatory language
- IP considerations
- Alignment with company ethics principals

AUDIT

# Model Risk Management



## DANIEL CHATBOT

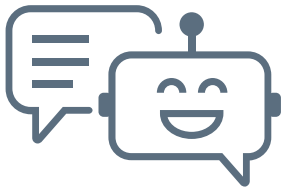
- Pre-production testing: noisy inputs, adversarial prompts
- Periodic evaluations: model drift
- Explainability: ability to reconstruct why content was produced


## JOHNNY VENDOR GAI

- Usage-based risk
- Overreliance
- Model training
- Vendor updates
- Guardrail testing

AUDIT

# Operational Resilience



## DANIEL CHATBOT

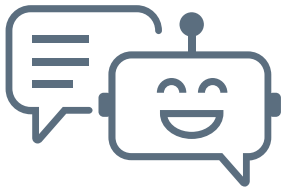
- Uptime
- Scalability
- Failsafe behavior


## JOHNNY VENDOR GAI

- Business continuity
- Vendor dependency

AUDIT

# Summary Considerations



## DANIEL CHATBOT

- Can materially affect customer trust, regulatory compliance, and brand reputation
- Requires strong user interface controls, back-end controls, and continuous monitoring


## JOHNNY VENDOR GAI

- Broad impact across the organization, primary risks being data leakage, hallucinations, overreliance, and model training

While use cases differ, the core themes of governance, data/training, security/privacy, and resilience apply to both.

# Conclusion

4

# The Internal Audit Function of the Future

**The internal audit and compliance function of the future has the following characteristics:**

**PROCESS**

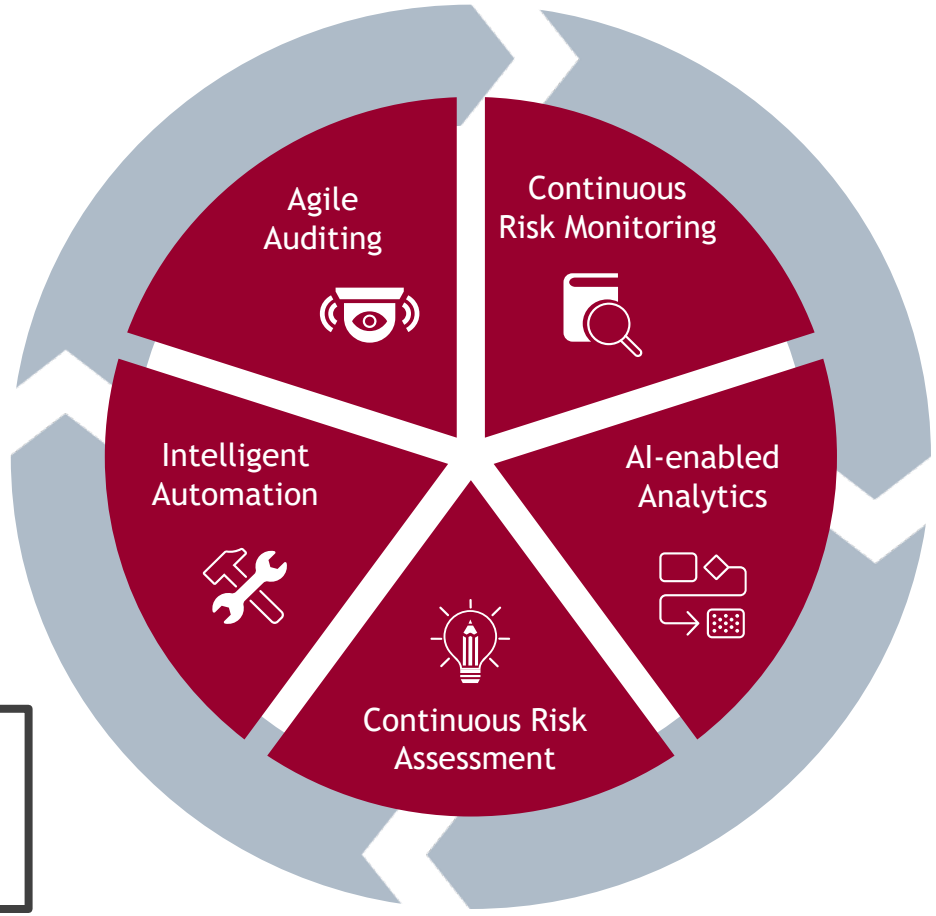
- Focuses on risks that are strategically important
- Is built on common risk taxonomy and indicators
- Is positioned as a value creator for the enterprise

**TECHNOLOGY**

- Is dynamic and agile
- Is powered by data leveraging automation and analytics
- Utilizes continuous risk monitoring solutions (proactive vs. reactive)

**PEOPLE**

- Established a common sense of purpose for all risk stakeholders
- Puts risk managers and auditors on the forefront of the transformation




**TECHNOLOGY ENABLERS**

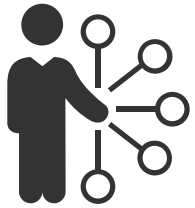
Advanced Analytics | Process Intelligence | Robotics | Artificial Intelligence (AI)

# How IA can prepare for AI

AI has the potential to transform the way internal audits are conducted, as well as how assurance is approached more broadly. No matter the size of your internal audit team, BDO recommends the following foundational steps to get started with AI efficiently, effectively, and responsibly.

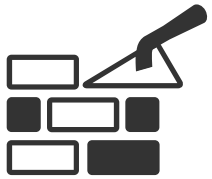
### Educate

All team members need to grasp what AI is, what it can do, and its implications for the function.



### Identify Use Cases

AI is not a one-size-fits-all solution. It's important to pinpoint those areas where AI has the potential to deliver the most significant impact.



### Prepare & build

The strength of an internal audit team's AI initiatives lies in the foundation. Strong data is critical as it feeds AI, and its quality informs the system's success.

### Enable & Adopt

A tool is only as good as its user. It is important to train, provide proper resources, dispel myths, and most importantly, help the team understand the 'why' behind AI.

### Go & Grow

The internal audit team's journey to AI does not end at launch; it's an ongoing, iterative process.

# Opportunity to Leverage Next-Generation Digital Tools Can Be Found Throughout the Internal Audit Lifecycle

**TECHNOLOGY ENABLERS**


Advanced Analytics

Process Intelligence

Robotics

Artificial Intelligence (AI)

- Training and Skill Development using ChatGPT
- Continuous Learning & Knowledge Sharing using ChatGPT
- Control Rationalization and Automation Assessment
- Digital Maturity Assessment

- Predictive Analytics
- Automated Data Testing
- 100% Coverage
- Control Validation
- Chat Bots for Auditors
- AI-Enabled Fraud Detection
- Risk-Based Sampling

**Planning & Information Gathering** → **Risk Assessment & Audit Plan** → **Assess Plan & Perform Audits** → **Deliver Results and Reporting**

- Risk Assessments using AI and ChatGPT
- Interactive Risk Register
- Audit Planning & Resource Allocation

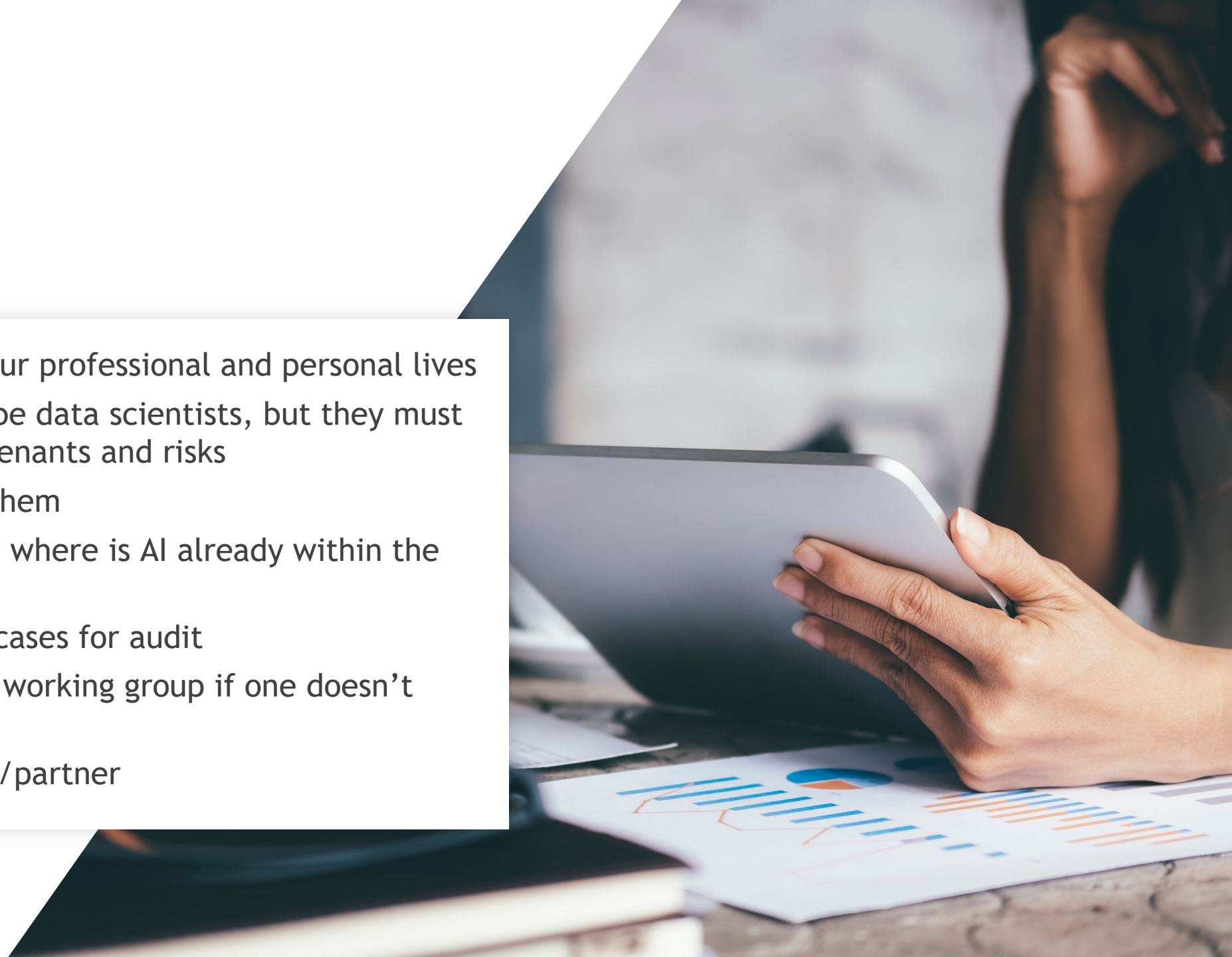
- Automated Audit Reports
- Interactive Status Dashboards and Reporting
- Continuous Monitoring of Compliance Metrics

# Setting Short- and Long-Term Goals

## AI GOVERNANCE FIT-FOR-PURPOSE

# Wrap It Up

- AI is pervasive in both our professional and personal lives
- Auditors don’t need to be data scientists, but they must understand AI’s major tenants and risks
- Frameworks exist- use them
- Start with an inventory- where is AI already within the environment?
- Select high-impact use cases for audit
- Build a cross-functional working group if one doesn’t already exist
- Become a trusted guide/partner




**About BDO USA**

Our purpose is helping people thrive, every day. Together, we are focused on delivering exceptional and sustainable outcomes and value for our people, our clients and our communities. BDO is proud to be an ESOP company, reflecting a culture that puts people first. BDO professionals provide assurance, tax and advisory services for a diverse range of clients across the U.S. and in over 160 countries through our global organization.

BDO is the brand name for the BDO network and for each of the BDO Member Firms. BDO USA, P.C., a Virginia professional corporation, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. For more information, please visit: www.bdo.com.