Session 2

10:15 – 11:55 AM

Harnessing AI:

Revolutionizing Internal Audit, Cybersecurity, and Governance

ARC|Hybrid

Sharing Wisdom Together

Learning Objectives

1. Understanding the Role of AI in Enhancing Internal Audit.
2. Apply effective audit approaches to identify and manage risks in AI systems.
3. Exploring the Synergy between Cybersecurity, AI, and Organizational Culture.
4. Apply strategies to maintain compliance with evolving global AI regulations.

ARC Hybrid

Illusion of Understanding

> AI's capability is a powerful form of statistical prediction that can mimic reasoning and comprehension, but it operates without genuine awareness, intent, or a human-like mental model of the world.
>
> It is a very powerful tool for pattern recognition and information synthesis, but its "intelligence" is fundamentally different from human cognition.

ARC Hybrid

Which statement best describes your current experience with artificial intelligence (AI) technologies?

I have never used any AI tools or applications.

4.76%

I occasionally use AI-powered features (like smart assistants, chatbots, or recommendation systems) without deep understanding.

14.29%

I actively use AI tools and have some understanding of how they work.

80.95%

I have hands-on experience building, training, or deploying AI models or systems.

0%

What excites you most about AI in audit? (e.g., efficiency gains, new insights, risk detection, etc.)

digest more data

new insights

accuracy

control descriptions

full pop testing

writing reports

risk detection.

efficiency

gaining efficiency

risk coverage

other-perspectives

risk identification

efficiency gains

audit questions

other perspective

issue writing

summarizing

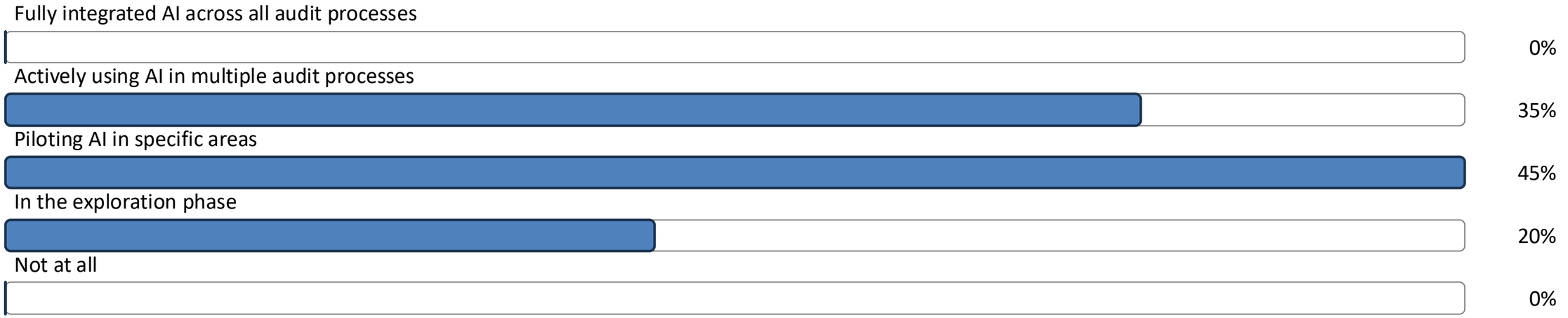
improved efficiency

templates for audits

value add service

Preparing Results

To what extent is your internal audit function currently utilizing AI?



AI for Internal Audit

ARC Hybrid

Sharina Wisdom Together

AI in Audit: The Big Picture

AI adoption among internal auditors is expected to **double from 39% to 80%** by **2026**.

Source: Wolters Kluwer survey (April 2025, 4,214 internal audit professionals)

Current usage varies:	Training is key:	Technology access matters:	Efficiency and productivity:	Strategic focus:	Accuracy:
• **46%** say AI adoption in audit is lower than other business areas • **21%** say it's higher	• **45%** believe that training in AI skills and tools will most enhance adoption • **84%** would consider AI skills when hiring for audit roles	• **27%** say dedicated AI-powered audit technology drives adoption	• **54%** expect AI to boost auditor productivity in the next year	• **24%** believe AI will free auditors to focus on higher-value tasks	• **13%** expect AI to improve accuracy and reduce human error

"How does this match your organization?"

ARC Hybrid

Sharina Wisdom Together

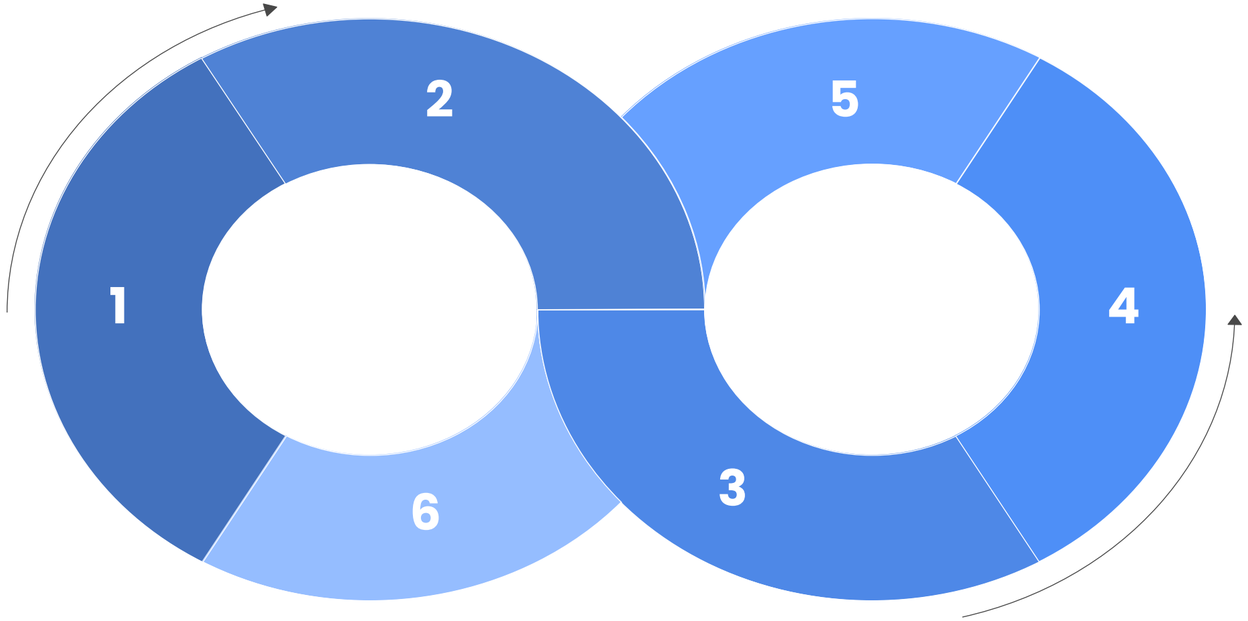
AI Transformation in Audit

Continuous Auditing

AI monitors processes in real-time.

Streamline Compliance

AI ensures adherence to regulations.



Enhance Risk Assessment

AI identifies potential risks more effectively.

Improve Fraud Detection

AI detects anomalies indicating fraud.

Augmented Decision-Making

AI supports informed decisions.

Advanced Analysis

AI analyzes data for insights.

ARC Hybrid

Sharing Wisdom Together

Achieving AI Adoption in Internal Audit

Common Obstacles:

High Costs
Software, integration, and training.

Resistance to Change
Fear of replacement.

Data Quality
Fragmented/ unstructured data.

Upskilling Teams
Focus on training and development to enhance AI skills.

Continuous Training
Implement ongoing AI learning programs to keep skills up-to-date.

Foster Innovation Culture
Encourage a mindset of creativity and experimentation with AI.

Measure Impact
Evaluate both quantitative and qualitative benefits of AI adoption.

AI Usage in *Planning and Risk Assessments*

Planning

- **Longitudinal Analysis** — AI identifies recurring control deficiencies from past data
- **Predictive Risk Assessment** — AI forecasts potential risks, enabling proactive risk management
- **Mitigating Cognitive Biases** — AI challenges assumptions with broad context, preventing biases
- **Brainstorming and Analysis** — AI externalizes reasoning for comprehensive risk analysis
- **RACM Development** — AI systematically builds and analyzes RACMs from process narratives

Reporting

- **Drafting Formal Findings** — AI converts workpaper notes into formal audit findings
- **Executive Summaries** — AI distills detailed reports into one-page summaries
- **Multi-Perspective Review** — AI simulates stakeholder reception and interpretation
- **Risk Rating Calibration** — AI ensures consistency in risk ratings across reports
- **Chatbots for Information Retrieval** — AI chatbots assist auditors by automating tasks
- **Fine-Tuned Models** — AI models developed using historical reports and management letters

Fieldwork

- **Data Extraction from Unstructured Sources** — Use multimodal models to convert unstructured sources into structured data
- **Automating Key Procedures** — Automate tasks such as the 3-way match by extracting and comparing essential data points
- **Complex Compliance Analysis** — AI can replicate this reasoning across several documents
- **Integrated Workflows** — Integrate AI to identify and link related evidence, presenting exceptions
- **Test Script Generation** — Draft detailed audit test procedures for specific controls

ARC Hybrid

Sharina Wisdom Together

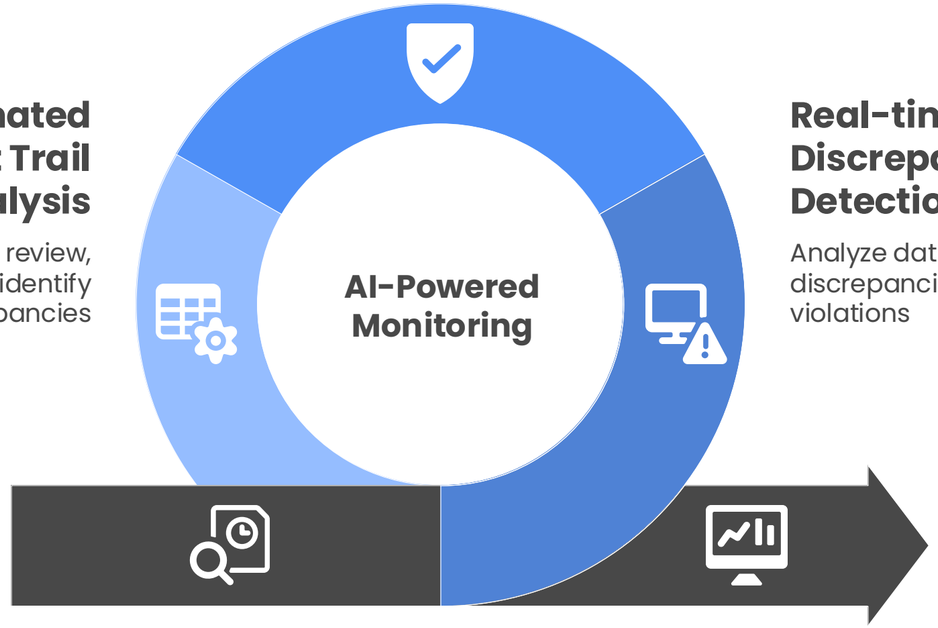
AI Usage in *Monitoring*

Proactive Fraud Detection

Identify irregular transactions, patterns in real-time

Automated Audit Trail Analysis

Automate review, identify discrepancies



Real-time Discrepancy Detection

Analyze data, flag discrepancies, violations

Traditional Periodic Audits

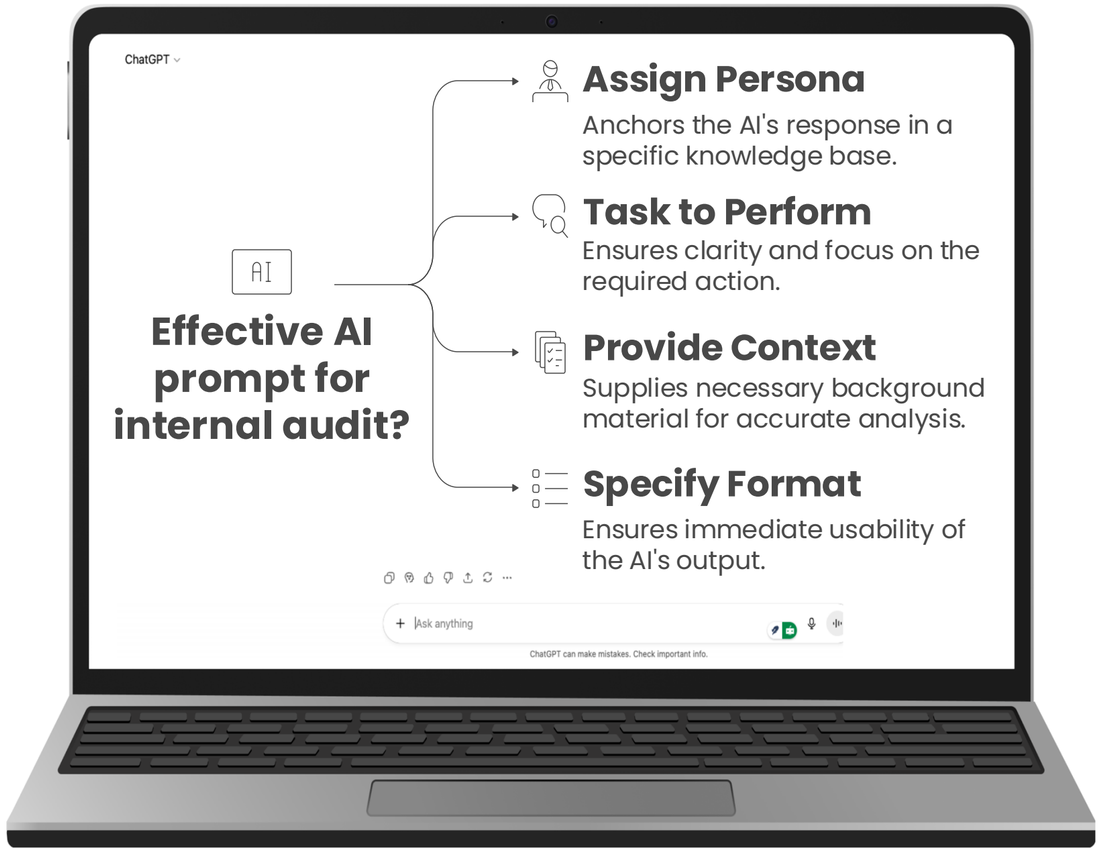
Limited real-time insights

Continuous Monitoring

Real-time insights, immediate action

What's the risk if monitoring is too reliant on AI?

The Art of Prompting



Actionable Prompt: Cybersecurity Audit of Workday Solution

1) Persona:
You are an **experienced IT Internal Auditor** with over 10 years of experience conducting **cybersecurity and ITGC audits** for enterprise SaaS solutions, including **Workday, SAP, and Oracle Cloud**. You have expertise in **cloud security, data protection, SOC 2 controls, and ISO 27001 frameworks**, and you understand both **technical configurations** and **business process risks** in HR and Finance systems.

2) Task:
Analyze the organization's **Workday environment** to **identify cybersecurity risks, control weaknesses, and improvement opportunities**, and then **summarize findings** with clear, prioritized recommendations.

3) Context:
The organization uses **Workday** as its central **HR, Payroll, and Finance** system. It is a **cloud-hosted SaaS** solution integrated with several third-party platforms, including **Okta (SSO)** for authentication, **ADP** for payroll, and **ServiceNow** for support tickets.

Audit objectives:
- Validate the **effectiveness of Workday's security configuration** and controls.
- Assess compliance with **corporate cybersecurity policies**, **SOC 2**, and **ISO 27001** standards.
- Confirm that data access, integrity, and confidentiality are maintained.

Focus Areas:
1. **Access Management:** Role-based access control, SSO configuration, MFA enforcement, privileged access reviews.
2. **Data Protection:** Encryption (at rest and in transit), data residency, and backup/recovery mechanisms.
3. **Change Management:** Configuration control, versioning, and testing of changes before deployment.
4. **Vendor Risk & Compliance:** Review of Workday SOC 1/SOC 2 reports, incident response procedures, SLAs.
5. **Audit Trail & Monitoring:** System logging, anomaly detection, and access review evidence.
6. **Governance & User Awareness:** Policy enforcement, security awareness, and segregation of duties (SoD).
7. **Assume** you have access to recent **Workday configuration reports**, **SOC 2 documentation**, and **internal audit policies**.

4) Format:
Provide your response in the following **table format**, prioritizing risks by potential impact on confidentiality, integrity, or availability (CIA triad):

| Control Area | Risk Identified | Impact (C/I/A) | Existing Controls | Control Gap | Recommended Action | Priority (High/Med/Low) | Reference (e.g., SOC 2 CC, ISO 27001) |

After the table, include a short **executive summary (≤200 words)** highlighting the top three risks and suggested next steps for management.

ARC Hybrid

Just Remember!

Use Secure AI Tools

Ensures data is processed in a controlled environment, reducing risk of exposure.

1

Follow Data Sanitization Checklist

Protects sensitive information by removing or generalizing personal and financial data.

2

Design Objective Prompts

Mitigates AI bias by using clear, unbiased criteria in prompts.

3

Data Sanitization Checklist

Ensure privacy and confidentiality when using and auditing AI.

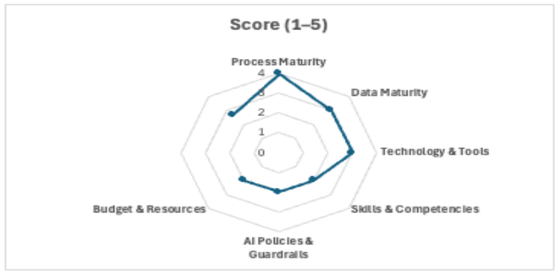
Checklist Items:

- ☐ **Remove PII and sensitive data before model testing**
  Example: *Redact employee names and SSNs from HR data before uploading to AI tool.*
- ☐ **Use only approved, secure AI tools**
  Example: *Confirm use of Microsoft Azure OpenAI, not public ChatGPT, for sensitive data.*
- ☐ **Document data minimization steps**
  Example: *Keep only necessary fields (e.g., job title, department) for analysis.*
- ☐ **Separate test and production datasets**
  Example: *Use anonymized test data for model validation, not live payroll data.*
- ☐ **Obtain management sign-off on data handling**
  Example: *Email approval from HR Director before data upload.*
- ☐ **Log all data access and sanitization actions**
  Example: *Maintain an access log showing who handled the data and when.*
- ☐ **Red-team prompts for inadvertent leakage**
  Example: *Test prompts like "List all employee names" to ensure no leakage occurs.*

Internal Audit AI Opportunity and Readiness Toolkit

Dimension	Description	Score (1–5	Maturity Label
Process Maturity	Standardization & repeatability of IA processes	4	High
Data Maturity	Data availability, structure, quality	3	Moderate
Technology & Tools	AI platforms, analytics tools, enterprise access	3	Moderate
Skills & Competencies	AI literacy, analytics skill level	2	Low
AI Policies & Guardrails	Existence & maturity of org AI policies	2	Low
Budget & Resources	Dedicated resourcing for AI growth	2	Low

Average Score **3**



AI Tool Demonstation

The "Initech" Audit Sprint

ChatGPT 5.1

pgsql

Copy code

```
Employee | Expense Type | Amount | Date | Notes
A Carter | Meals        | 145.23 | 3/4  | -
A Carter | Meals        | 148.50 | 3/4  | Client meeting?
J Park   | Hotel        | 0      | 3/5  | Prepaid?
R Lin    | Gifts        | 600    | 3/6  | Vendor holiday gift
S Gomez  | Meals        | 900    | 3/6  | Client? No receipts
```

Prompt:

> *Analyze this expense data for internal audit red flags. Identify potential fraud indicators, policy violations, anomalies, duplicate claims, and unusual patterns.*

AI will output:

- High-risk items (e.g., gifts over threshold)
- Duplicate costs
- Missing receipts
- Same-day multiple meals
- Out-of-policy items

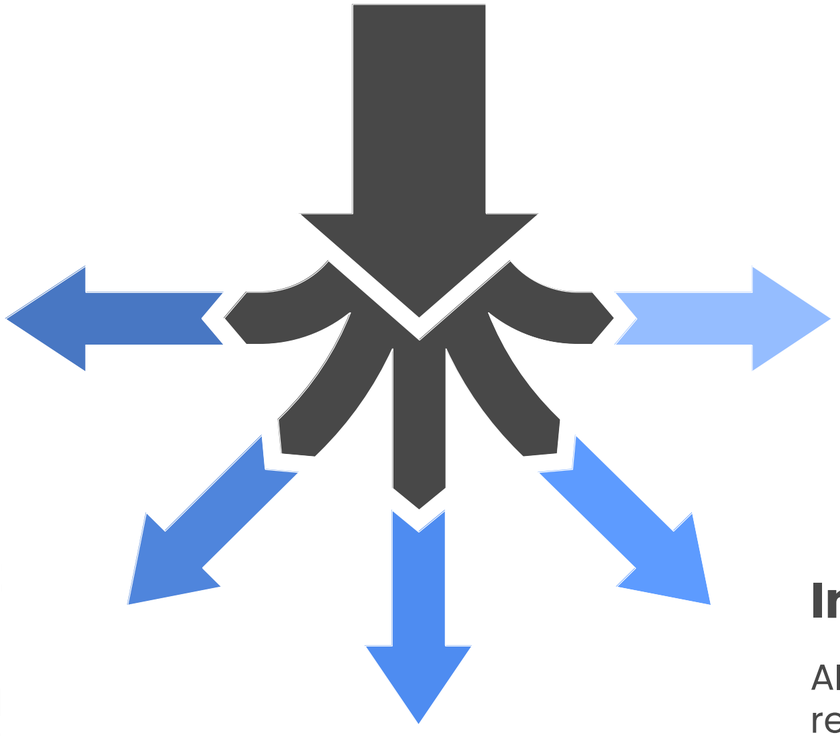
Takeaway: AI can assist auditors with **quick analytic insights**, even if not running scripts in ACL/IDEA/Python.

It’s Time to Audit the AI!

It’s Time to Audit AI

High AI Adoption

Rapid AI adoption across various organizational functions.



Guidance Demand

Organizations seek guidance on AI governance and compliance.

Significant Investment

Substantial financial investment in AI technologies.

Inherent Risks

AI poses inherent risks requiring careful management.

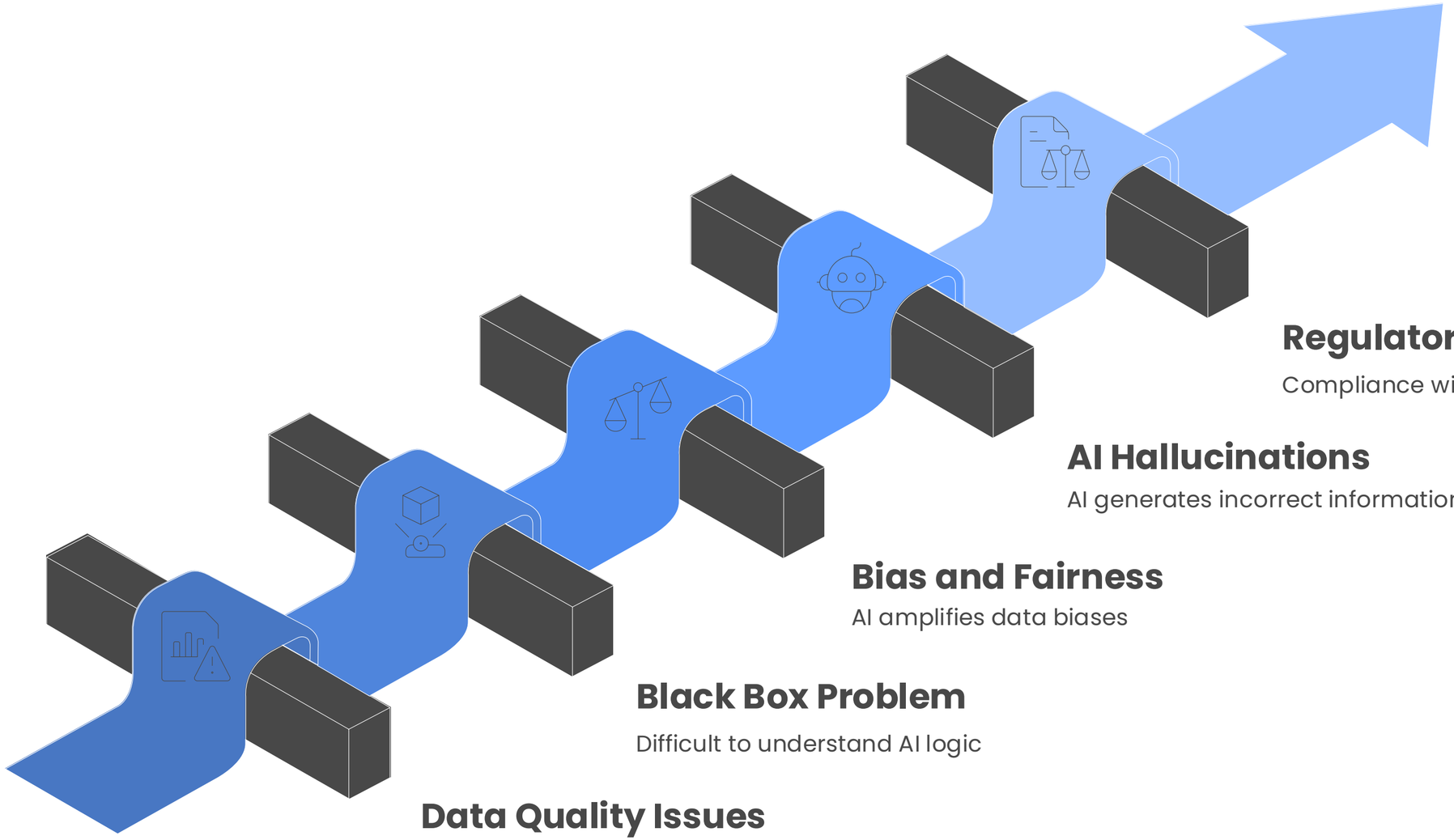
Organizational Reliance

Increasing organizational dependence on AI systems.

ARC Hybrid

Sharina Wisdom Together

The Unique Challenge of AI Risk



Regulatory Uncertainty

Compliance with AI laws is hard

AI Hallucinations

AI generates incorrect information

Bias and Fairness

AI amplifies data biases

Black Box Problem

Difficult to understand AI logic

Data Quality Issues

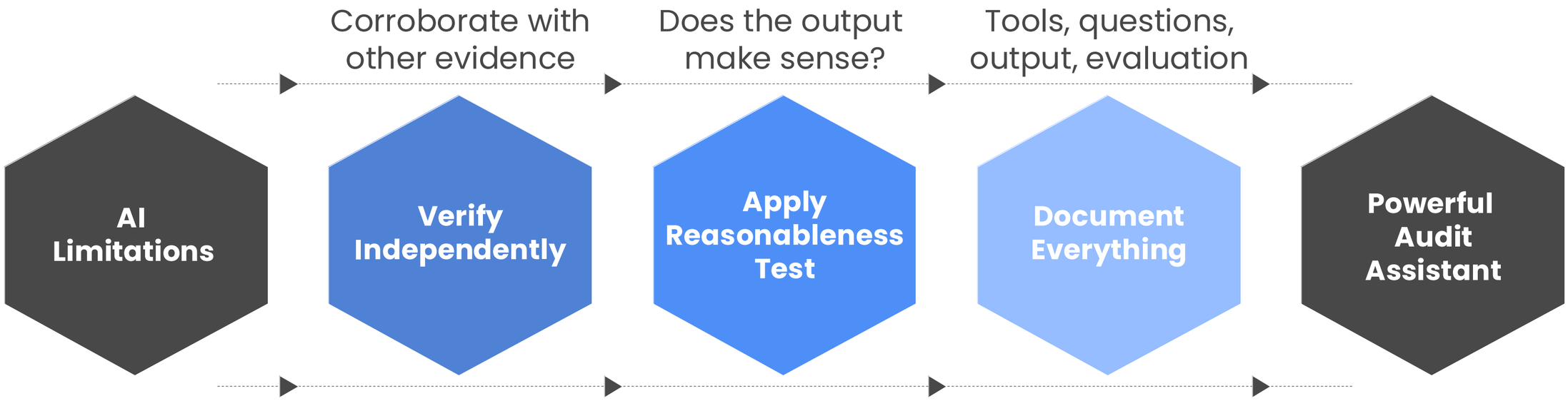
Inconsistent data leads to errors

ARC Hybrid

Sharina Wisdom Together

Managing AI Risk

"AI-generated data constitutes evidence for interpretation, not final judgment."



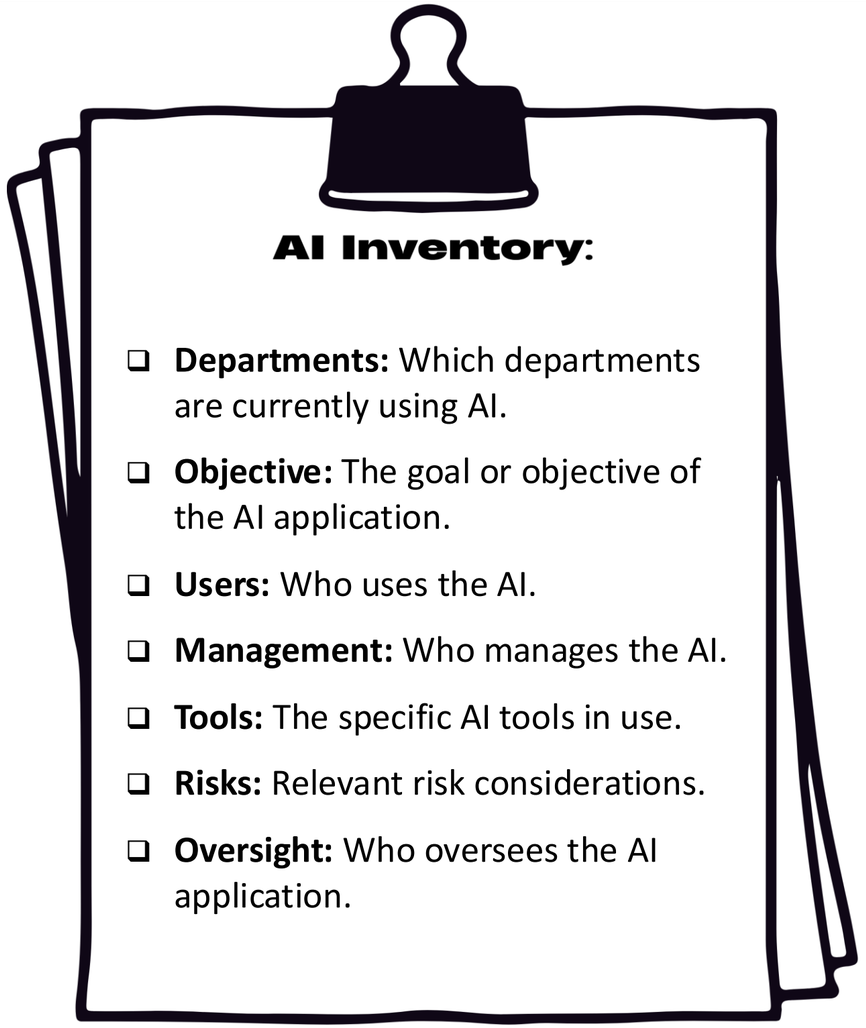
Requires professional auditor judgment

AI enhances auditor capabilities

"When is AI-generated evidence 'good enough' for audit?"

Step 1: Baseline Knowledge & Planning

1. **Establish Baseline Knowledge**
   Internal audit team gains initial understanding of AI use
2. **Perform Research**
   Conduct internal and external research on AI frameworks and policies
3. **Engage Executive Leadership**
   Discuss AI strategy and accountability with executive leaders
4. **Speak with AI Team**
   Gather information on algorithms, data sources, and risks from the AI team
5. **Create AI Inventory**
   Develop a comprehensive inventory of current and planned AI uses



ARC Hybrid

Step 2: Assess Data and Cybersecurity Controls

Assess Data Integrity

Ensure AI data meets integrity criteria

Restrict Data Access

Limit access based on job duties

Obtain SOC Reports

Gather SOC reports from third-party vendors

Verify IT Controls

Check IT controls for data protection

Monitor Input Data

Confirm management monitors data quality

Determine External Data Storage

Identify where external data is stored

Ensure Audit Rights

Include audit rights in SLAs

Step 3: Execute the AI Audit

Unverified AI System

Potential issues and non-compliance

Define Project Requirements

Objectives, resources, legal, regulatory

Validate AI System

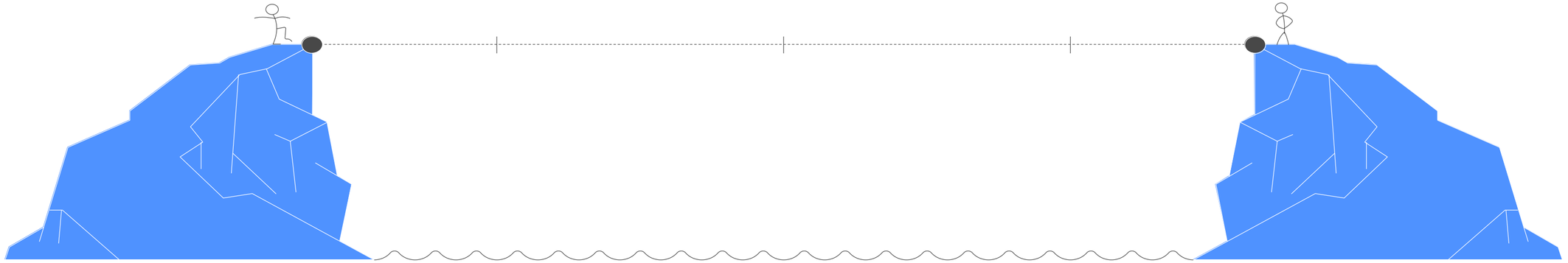
Testing before and after launch

Identify Potential Biases

Ethical and social considerations

Assured AI System

Minimized issues and compliant



During the execution of AI projects, management should ensure four crucial attributes are met.

- **Transparency:** Able to easily understand the purpose of the AI or algorithm.
- **Explainability:** Able to explain the mechanics, calculations, or results processed by the AI.
- **Responsibility:** Using the AI in an ethical, safe, fair, and trustworthy manner.
- **Auditability:** Maintaining traceability through effective audit logs or related information.

ARC Hybrid

HITL vs. HOTL

Human-in-the-Loop

Human-led control for high-risk domains

VS

Human-on-the-Loop

Supervisory control for customer service and logistics

Internal Audit AI Testing Framework

Domain	Key Risks	Control Objective	Testing Focus	Red Flags
Data Quality	Incomplete, biased, corrupted data	Data is accurate, complete, authorized	Trace data lineage, review data controls	No lineage, unclear sources
Model Development	Incorrect logic, weak design	Sound, documented design	Review requirements, methodology	"Black box" model
Model Validation	Poor performance, unvalidated models	Independent validation	Review validation reports	No validation or outdated
Explainability	Inability to justify outputs	Transparent logic	Assess interpretability	"We can't explain why it did that"
Drift Monitoring	Degraded accuracy	Performance continuously monitored	Review drift logs	No drift tracking
Security & Change Control	Unauthorized access, shadow AI	Controlled access, documented changes	Review logs and approvals	No access logs
Responsible Use	Data leakage, policy violations	Compliant, ethical AI use	Check policy alignment	Prompts contain confidential data
Output Quality	Incorrect results	Human review ensures accuracy	Reperform outputs	Staff using AI without validation

AI Audit Testing Toolkit

Domain 1: Data Quality

Test Objective	Pass Criteria	Fail Criteria
Validate data lineage	Complete lineage covering source → transformations → model	Missing nodes; undocumented manual steps
Data quality checks	Logs show checks run; exceptions reviewed	No log evidence; no review of exceptions
Data representativeness	Dataset balanced; bias tests performed	Skewed data; no bias tests

Domain 2: Model Development

Test	Pass	Fail
Model documentation	Business Requirement Document, assumptions, architecture clear	No documentation
Reproducibility	Versioning + fixed seeds	Manual runs, no version control

Domain 3: Validation

Test	Pass	Fail
Independent validation	Clear evidence of independence	Developer validated their own model

Auditing AI-Driven Threats

What internal auditors must know about AI-driven cyber risks and how to assess organizational readiness.

ARC Hybrid

Sharina Wisdom Together

The AI-Driven Threat Landscape

Experts' top concerns around AI

39% PRIVACY CONCERNS

37% UNDETECTABLE PHISHING ATTACKS

33% ATTACKS VOLUME & VELOCITY

Source: Techopedia

75%
SEEN AN INCREASE IN CYBERATTACKS

85%
BLAME AI

Audit Risk Lens: How does this shift the likelihood/impact scoring in your cyber audits?

ARC Hybrid

Sharina Wisdom Together

The Cost of AI-Cyber Attacks

WITHOUT AI - ENABLED CYBERSECURITY

WITH AI - ENABLED CYBERSECURITY

$4.45 million

277 DAYS

$1.8 MILLION DIFFERENCE

40% LESS

TIME TAKEN TO IDENTIFY DATA BREACH

$2.65 million

177 DAYS

The U.S. remains the costliest region for data breaches.

ARC Hybrid

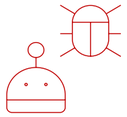
Sharina Wisdom Together

AI-Enhanced Exploitation

The Attacker's Play

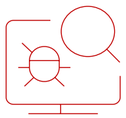
Automated Weakness Identification

AI continuously scans internet-facing systems, APIs, VPNs, and cloud environments, mapping to reconnaissance tactics.



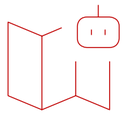
Rapid Vulnerability Weaponization

AI accelerates the creation and deployment of exploits immediately after public disclosure, targeting unpatched assets.



Dynamic Evasion

Malware behavior is modified in real-time to bypass traditional signature-based defenses.



Intelligent Lateral Movement

AI tools map internal networks to identify and execute the most efficient attack paths post-breach.

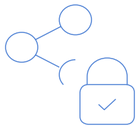
Audit's Counter-Play

Vulnerability & Patch Management

Audit the AI-informed prioritization of critical patches based on business risk and monitor recurring vulnerabilities.

Endpoint Detection & Response

Verify behavior-based detection and test model validation and containment strategies to enhance threat detection capabilities.



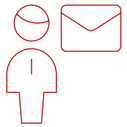
Network Segmentation & Zero Trust

Confirm segmentation of critical functions and restricted paths for privileged accounts. Audit for monitoring of unusual internal traffic.

ARC Hybrid

AI Social Engineering at Scale

The Attacker's Play



Hyper-Personalized Phishing

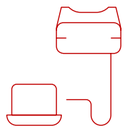
AI mimics the tone and style of trusted individuals to create convincing requests at scale.

Deepfake Audio & Video

Voice and visual likenesses are cloned from small samples to bypass identity verification through direct psychological manipulation.

Automated Document Forgery

Generates plausible contracts, invoices, or credentials to support complex fraud schemes.



Behavioral Spoofing

Emulates human-like keystrokes or mouse movements to bypass advanced behavioral security tools.

Audit's Counter-Play

Security Awareness & Training

Ensure training explicitly covers deepfakes, AI-phishing, and MFA fatigue. Review feedback loops from simulations.

Challenge Culture & Verification

Audit for clear, enforced protocols (e.g., dual controls, callbacks) for sensitive instructions, supported by the tone at the top.

Identity & Access Management (IAM)

Verify the use of modern, phishing-resistant MFA and the detection of login anomalies.

ARC Hybrid

Accelerated Data-Driven Attacks

The Attacker's Play

Automated Data Mining

Once inside, AI rapidly sifts through exfiltrated content to identify the most valuable data (PII, financial, IP).

High-Value Target Refinement

Cross-references disparate data sources to build detailed profiles of individuals for blackmail, fraud, or espionage.

Automated Follow-On Attacks

Launches subsequent fraud or phishing campaigns based on the intelligence gathered from the initial breach.

Audit's Counter-Play

Data Minimization & Retention

Audit the classification of high-risk data and the enforcement of data lifecycle and retention policies.

Access Governance

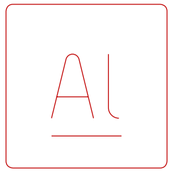
Test for least privilege and segregation of duties. Review risk-based recertification processes.

Logging & Monitoring

Verify that tamper-resistant logs enable full event reconstruction. Validate the accuracy and stability of any AI-based anomaly detection systems.

Fault Line in the Human Firewall

Overreliance on Automated Tools

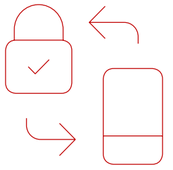


Risk: A false sense of security leads to a lack of human oversight and validation for AI security tool outputs.

Audit Check: Review documentation for AI tool scope and limitations. Verify processes for regular model validation and drift detection.

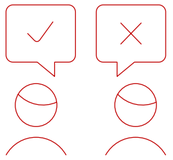
MFA Fatigue & Alert Overload

Risk: Desensitized users approve malicious security prompts out of habit or frustration.



Audit Check: Assess the strength of MFA configurations (e.g., number-matching, device-bound) and review logs for abnormal MFA behavior.

Weak Challenge Culture



Risk: Fear of questioning authority or prioritizing speed over security allows manipulated instructions to go unchallenged.

Audit Check: Look for evidence of policies that encourage verification, review culture surveys, and confirm safe escalation paths are defined and understood.

Deepfake Fraud & Exec. Pressure

Risk: Simulated executive instructions exploit authority dynamics to compel urgent, high-risk actions.

Audit Check: Test whether processes require independent validation of unusual instructions and that senior leaders adhere to the same standards.

ARC Hybrid

Sharina Wisdom Together

Internal Audit AI Testing Matrix

Characteristics	AI Use Case	Audit Focus
Anomaly Detection	Behavioral analysis for insider threats	Validate model purpose, accuracy, tuning, and governance
Identity & Access	AI risk-scores access requests	Review decision thresholds, auditability, and override mechanisms
Threat Intelligence	Correlate external feeds with internal signals	Check source credibility, integration, and triage processes
Third-Party Risk	Analyze SOC reports and contracts	Treat key vendors as high-risk; ensure security clauses are enforced
Compliance & Privacy	NLP scans for sensitive data	Assess classification accuracy and retention policy enforcement
Malware Analysis	Classify malware, accelerate forensics	Evaluate time-to-detect and integration of post- incident learnings
Cloud Security	Scans for misconfigurations	Audit cloud asset coverage, remediation workflows, and control links
Data Loss Prevention	Detect unauthorized data movement	Examine rule tuning, exception handling, and shadow IT visibility

AI Governance and Regulation

Key Governance Principles

Risk Classification

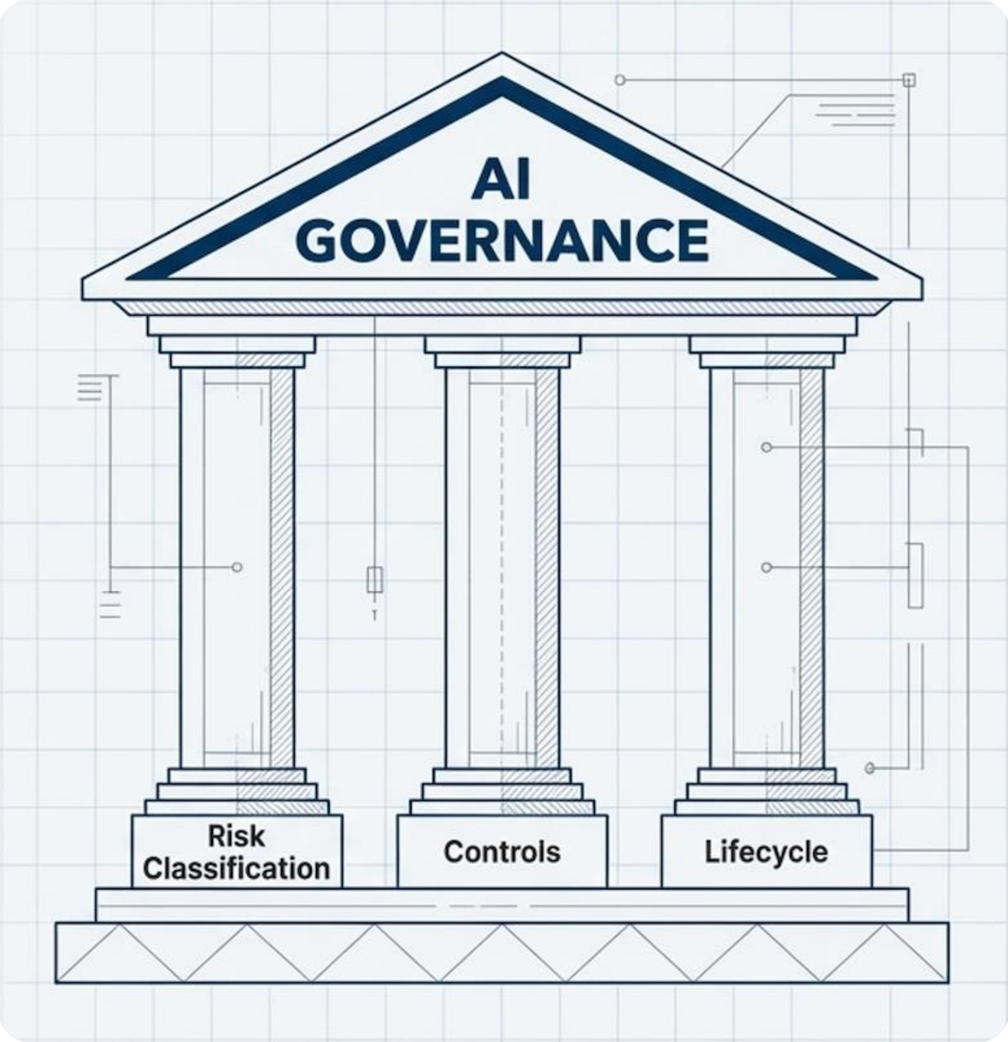
Classify AI systems by risk level to ensure appropriate controls are applied.

High-Risk Controls

Implement robust controls for high-risk systems to mitigate potential harm.

Lifecycle Governance

Align AI management with lifecycle models for comprehensive oversight.



Foundation & Principles of AI Governance

Foundations

Policies

Formal guidelines ensuring ethical and safe AI practices

Standards

Benchmarks for AI system quality and performance

Guidelines

Recommendations for AI system development and deployment

Procedures

Step-by-step processes for AI system management

Practices

Established methods for AI system implementation

Principles

Human Oversight

Ensures ethical and responsible AI decision-making through human supervision.

Transparency and Explainability

Promotes understanding of AI behavior and decision processes.

Fairness and Non-Discrimination

Prevents biased outcomes and ensures equitable treatment.

Safety, Reliability, and Privacy

Maintains system integrity and protects sensitive data.

ARC Hybrid

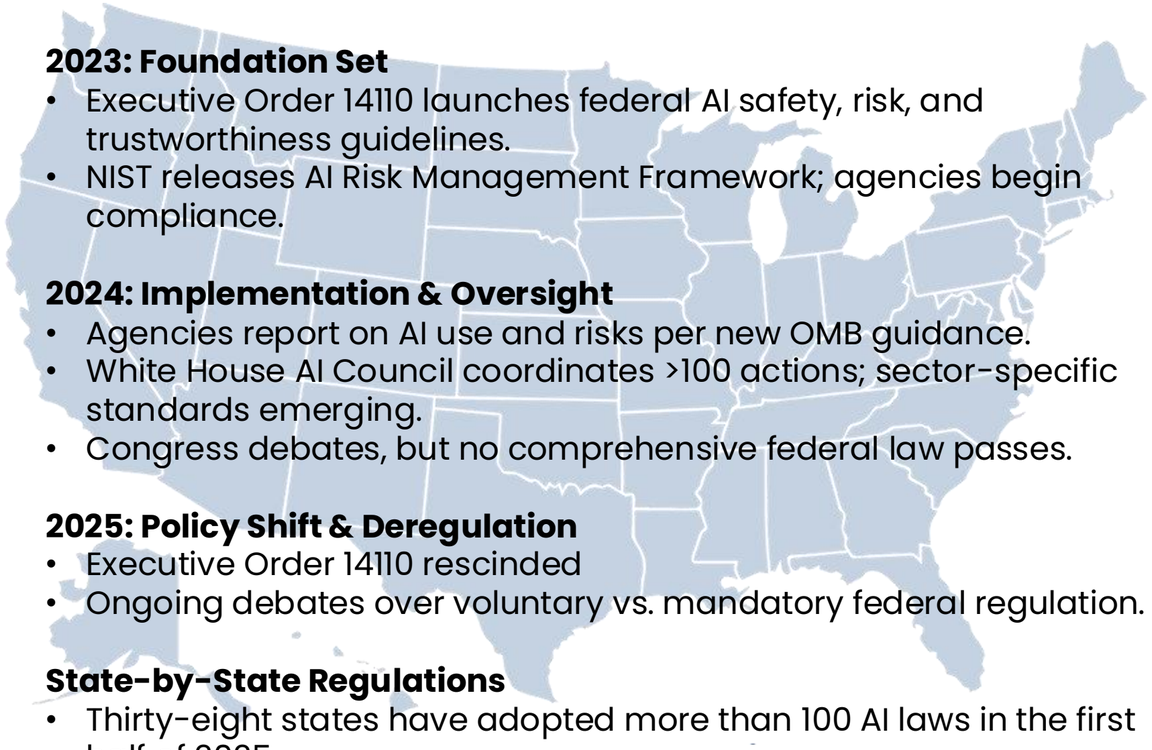
Sharina Wisdom Together

Key Frameworks for Responsible AI Governance

Framework	Type	Scope and Focus	Status (Oct 2025)
EU AI Act	Legally Binding Regulation	Risk-based approach focusing on fundamental rights, safety, transparency, and human oversight.	In force, with obligations for general-purpose AI models active.
ISO/IEC 42001	International Standards	AI management systems (42001), impact assessments (42005), audit/certification (42006), lifecycle (5338), bias (24027), risk (23894), data quality (5259). Framework for operationalizing responsible AI and aligning with EU AI Act.	42001 published Dec 2023; adoption growing globally; related standards in various stages of adoption.
NIST AI RMF	Voluntary Guidance Framework	Practical guidance for identifying, assessing, and managing AI-specific risks; widely used for risk management.	Widely adopted in the US and internationally; updated regularly.
OECD AI Principles	International Policy Principles	High-level principles for trustworthy, ethical, and transparent AI; foundation for national and organizational policies.	Adopted by 46+ countries; informs policy and regulation.
Industry/Vendor Frameworks	Company/Industry Frameworks	Organization-specific governance (e.g., Microsoft Responsible AI, Gartner TRiSM) for operationalizing responsible AI.	Widely used as best practice references; updated as AI evolves.

Global AI Regulations

The United States **does not** have a **comprehensive federal law specifically regulating artificial intelligence** (AI).



2023: Foundation Set
- Executive Order 14110 launches federal AI safety, risk, and trustworthiness guidelines.
- NIST releases AI Risk Management Framework; agencies begin compliance.

2024: Implementation & Oversight
- Agencies report on AI use and risks per new OMB guidance.
- White House AI Council coordinates >100 actions; sector-specific standards emerging.
- Congress debates, but no comprehensive federal law passes.

2025: Policy Shift & Deregulation
- Executive Order 14110 rescinded
- Ongoing debates over voluntary vs. mandatory federal regulation.

State-by-State Regulations
- Thirty-eight states have adopted more than 100 AI laws in the first half of 2025.

Europe is quickly **shifting from voluntary guidelines to binding requirements**, especially for high-risk AI applications.

EU: The EU AI Act—world's first comprehensive, binding AI law; strict rules for "high-risk" AI systems; enforcement starts 2026.

UK: Sector-specific guidance, no single law; emphasis on transparency, accountability, and regulatory "sandboxes."

Canada: Artificial Intelligence and Data Act (AIDA) targets "high-impact" AI; requires risk assessments, transparency.

China: Expanding regulations for generative AI and algorithms; mandatory security and compliance reviews.

Other regions:
- **Japan**: Principles-based, voluntary guidelines; some sectoral rules in finance and healthcare.
- **Brazil**: Drafting national AI law.
- **Singapore**: Voluntary AI governance framework, regulatory sandboxes.

ARC Hybrid

AI Governance – What this means for you?

Regulation is shifting: Moving from advisory standards to enforceable requirements, especially in high-impact sectors (e.g., finance, healthcare, critical infrastructure).

Audits must adapt: Focus shifts to verifying compliance, not just providing recommendations.

Expanded Audit Responsibilities:

Assess AI risk levels: Determine which AI systems pose the greatest risk and require the most scrutiny.

Follow the logic: Be able to trace how AI-driven decisions are made, ensuring transparency and accountability.

Test for fairness and compliance: Evaluate whether AI systems meet requirements for openness, responsibility, and ethical use.

Responsible AI Governance for Internal Audit

Governance Domain	*What IA Evaluates*	*Evidence Required*	*Framework Alignment*
AI Inventory & Classification	Existence, completeness, risk tiering	Inventory, use case register	EU AI Act, ISO 42001, NIST Govern
Policies & Governance Structure	Policies, committees, roles, RACI	Policy documents, charters	ISO 42001, NIST Govern
Data Governance	Lineage, quality, bias controls	Lineage diagrams, DQ logs	ISO 42001, NIST Map/Measure, OECD Fairness
Model Development	Requirements, documentation, code controls	BRD, model card, version control logs	NIST Map, ISO 42001 lifecycle
Model Validation	Independence, accuracy, fairness	Validation reports, test results	EU AI Act, NIST Measure
Human Oversight	Intervention criteria, escalation	SOPs, override logs	EU AI Act, OECD Accountability
Monitoring & Drift	Alerts, KPIs, retraining	Drift dashboards, performance metrics	NIST Manage, ISO 42001
Security & Access Control	Access reviews, change control	Access lists, change tickets	ISO 27001, ISO 42001
Ethical & Compliance Risk	Bias, harm prevention, transparency	Bias test reports, transparency docs	OECD, IEEE 7000
Vendor and 3rd-Party Governance	Transparency, assurances, contracts	SOC2, model cards, SLAs	EU AI Act, ISO 42001

A	**Escalation and Human Intervention Protocols**	Every AI system should define: • When a human must intervene • How exceptions are routed • Who is authorized to override AI decisions • What risk thresholds require escalation • What scenarios trigger shutdown or fallback	Internal audit should confirm: • Escalation paths are documented and tested • Staff are trained on intervention criteria • Oversight responsibilities are clearly assigned
B	**Control Mapping: Human vs. AI Responsibilities**	AI governance requires clarity about: • What the AI system is allowed to do • What decisions require a human • How tasks shift between automation and manual work • How control activities change in mixed human-AI environments	IA should verify: • Updated RACI charts • Clear human-in-the-loop or human-on-the-loop expectations • Control redesign where AI replaces or augments tasks

Let the AI Audit Games Begin!

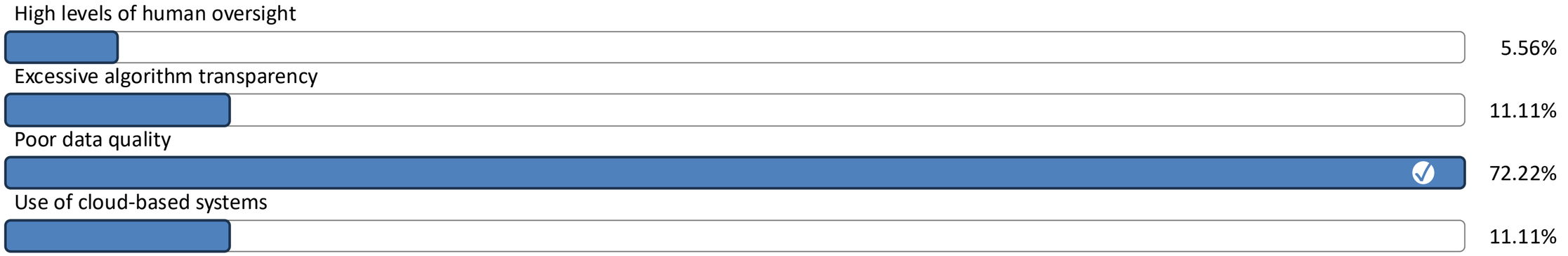
Get ready for 15 fast-paced questions to test your knowledge of AI, risk, governance, and cyber threats.

- One correct answer per question
- Some answers look right but aren't (trick questions!)
- Answer fast — scoring is based on speed
- Be ready… the leaderboard is watching 👀

ARC Hybrid

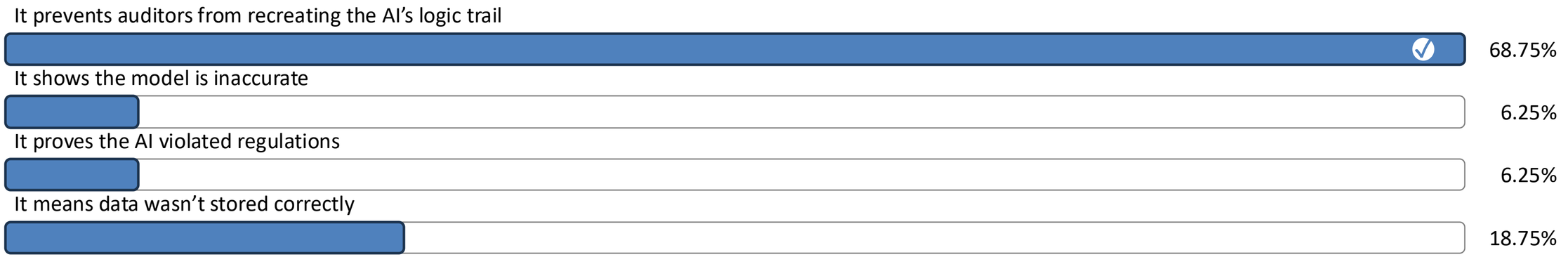
“Hallucination or Just Bad Data?”

Q: What is the *primary* cause of many AI hallucinations in audit contexts?



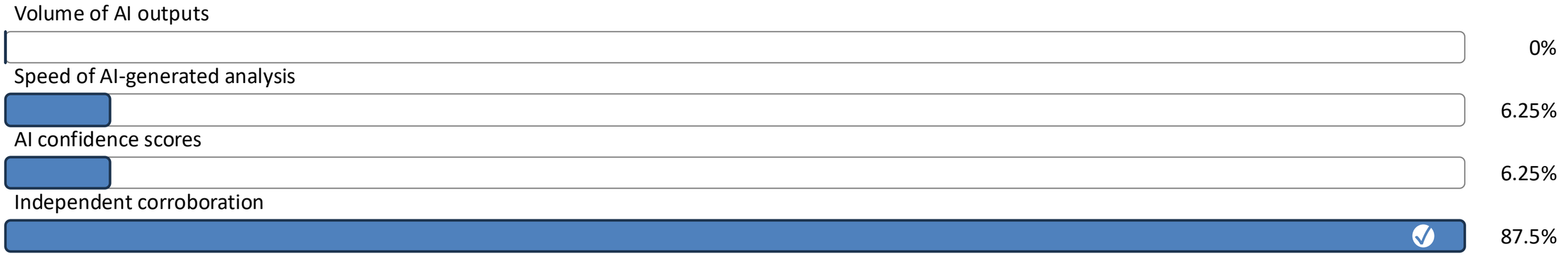
“Black Box Blues”

Q: Why is the Black Box Problem a *material* audit risk?



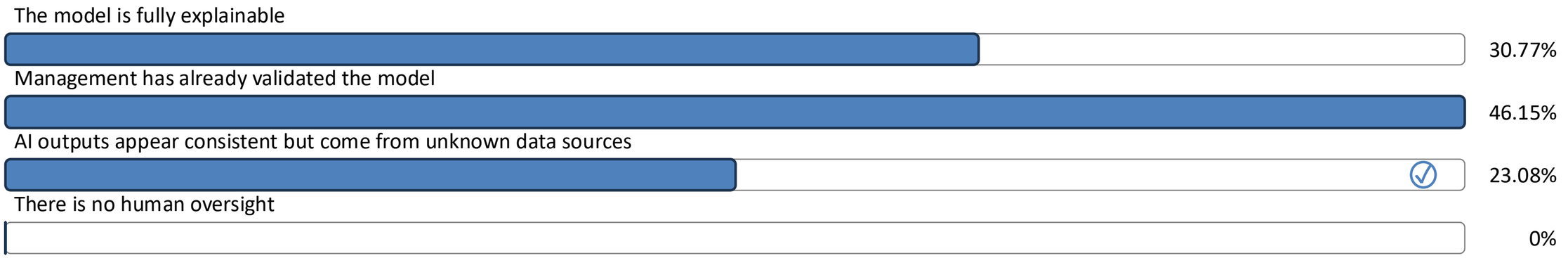
“Good Enough Evidence?”

Q: When determining if AI-generated evidence is acceptable, what must the auditor rely on MOST?



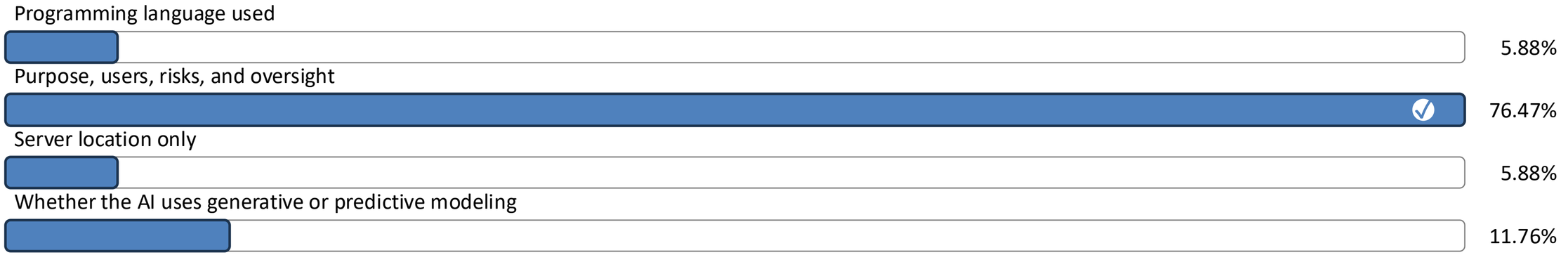
“Reasonableness Test 2.0”

Q: The reasonableness test is MOST useful when:



“Inventory Detective Work”

Q: A complete AI inventory MUST include which of the following?



“AI-Powered Chaos”

Q: Why do AI-generated phishing attacks dramatically increase risk?

They are hyper-personalized at scale — 100%

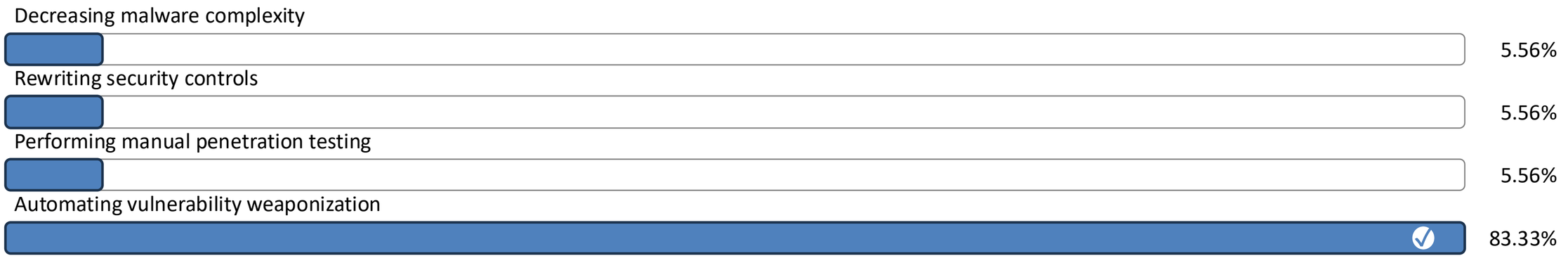
They are easier to detect — 0%

They only target system administrators — 0%

They require deepfake video to be effective — 0%

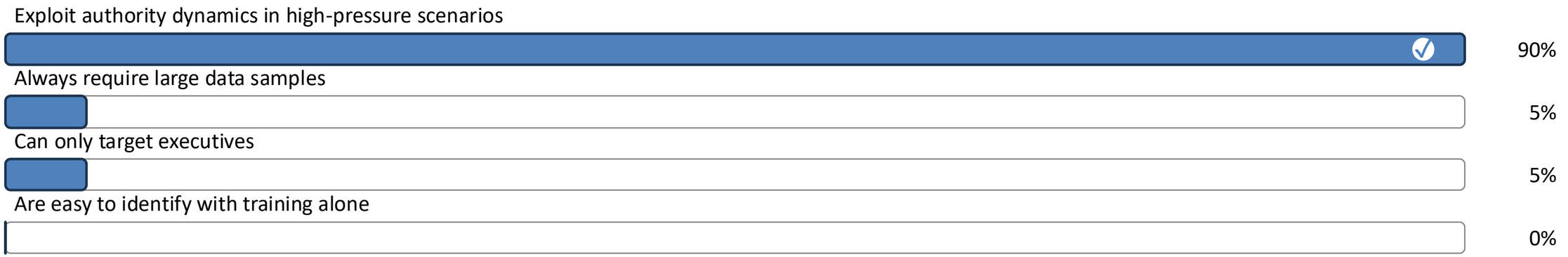
“Speed Kills… Systems”

Q: AI accelerates exploitation primarily by:



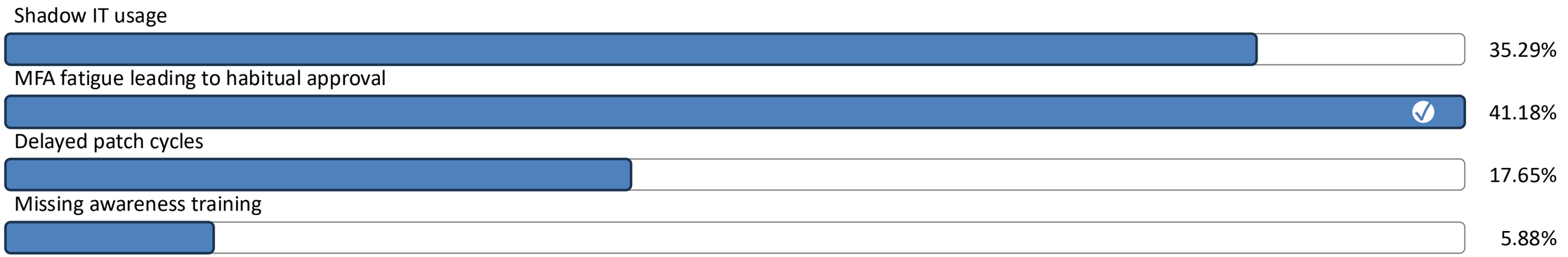
“Deepfake Disaster”

Q: Deepfake attacks are especially dangerous because they:



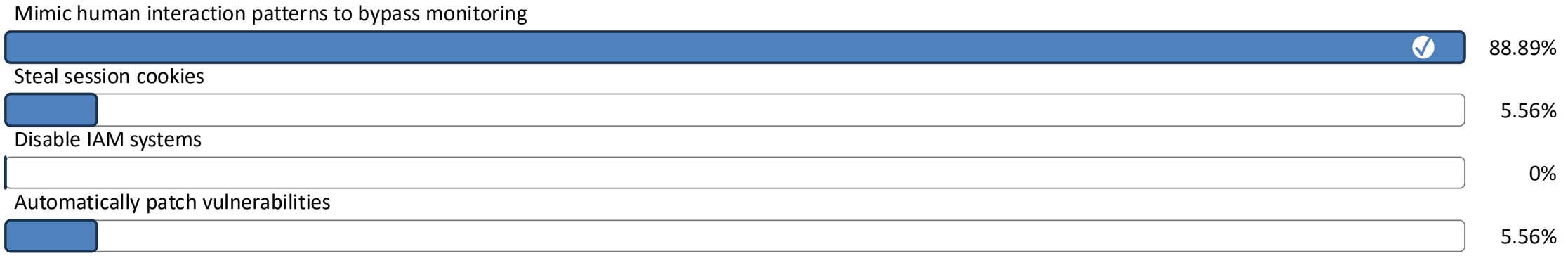
“Human Firewall Failure Points”

Q: Which issue MOST undermines MFA protection?



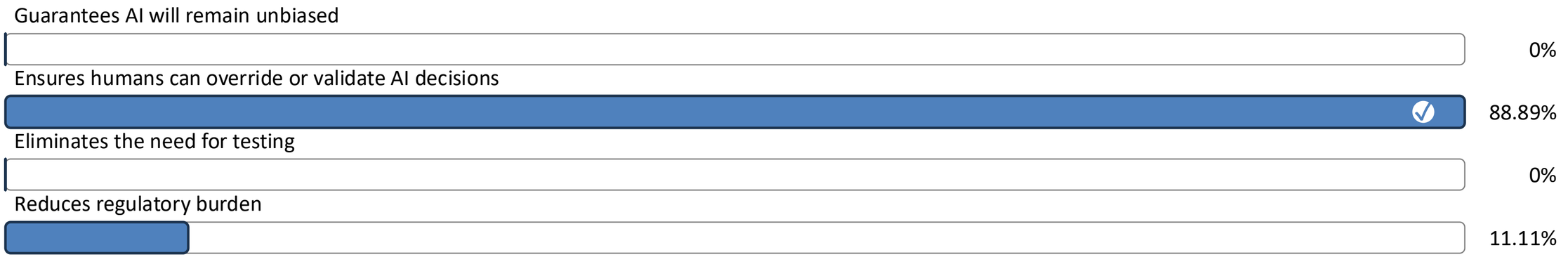
“Inside Job… or Just AI?”

Q: Behavioral spoofing allows attackers to:



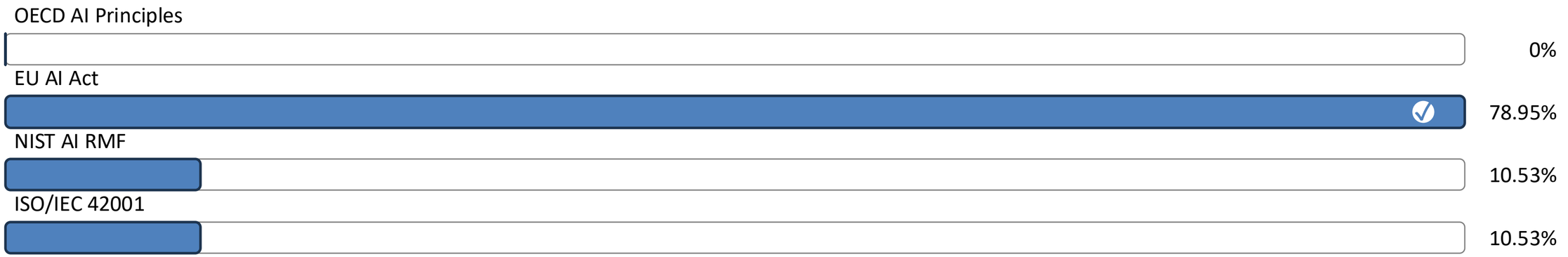
“HITL vs HOTL”

Q: Why is HITL essential for high-risk AI systems?



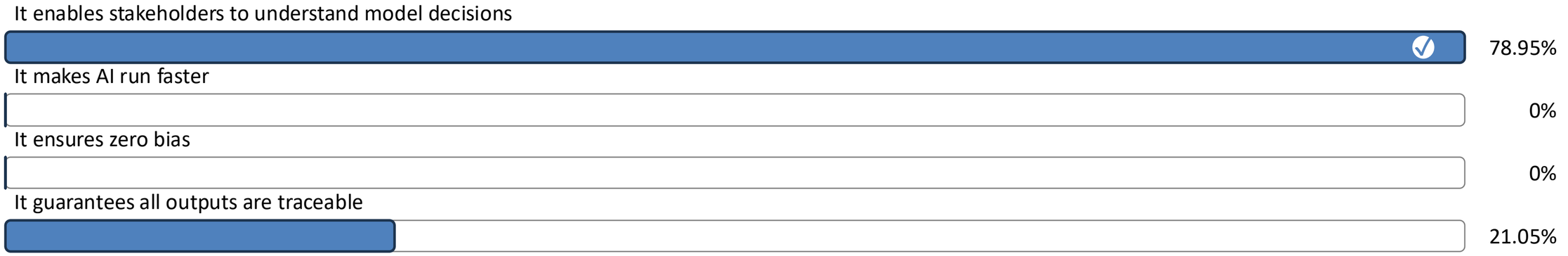
“Framework Face-Off”

Q: Which framework is *legally binding* and imposes enforceable requirements?



“Explainability: More Than a Buzzword”

Q: Why is explainability a core governance principle?

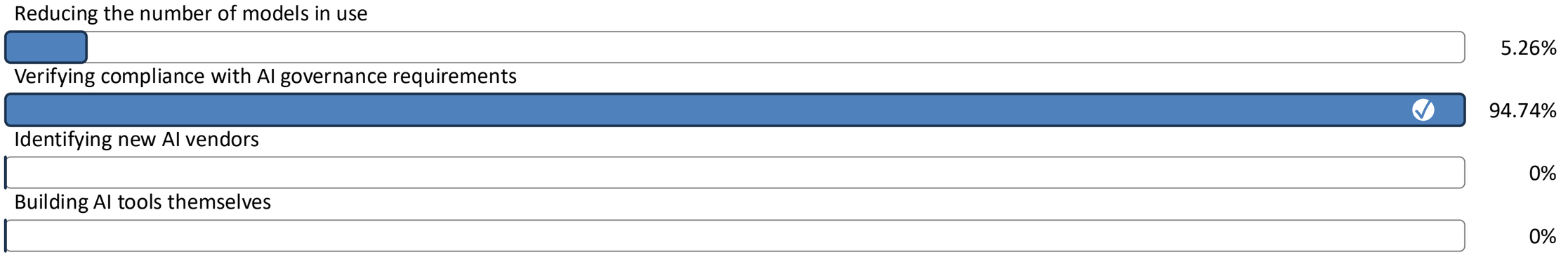


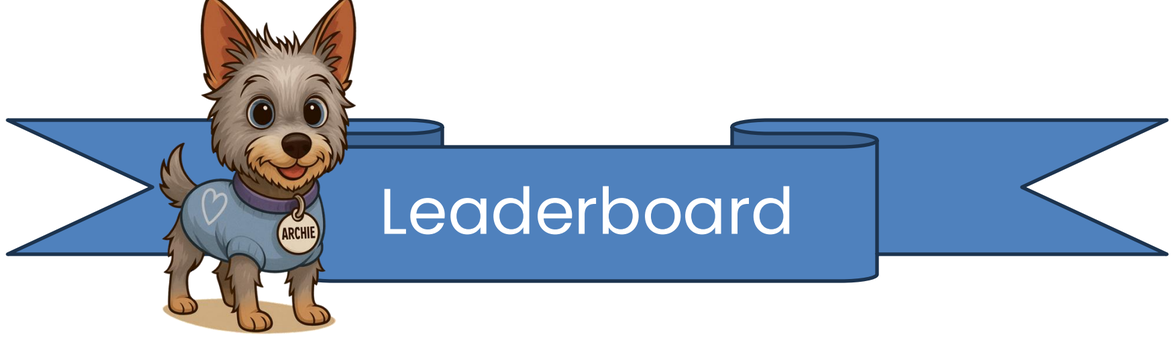
“High-Risk… or Just High Profile?”

Q: What distinguishes a *high-risk* AI system under governance models?

“New Audit Reality”

Q: What must internal audits increasingly focus on?





Leaderboard

Position	Participants	Score
🏆=1st	Devon Reddingius, Doug Lamb	14 / 15
=3rd	Bill MacKeeman, Heidi Pinner, Karel Johnson, Sheila Aquino	12 / 15
=7th	Mark Breslow, Shane	11 / 15
=9th	Ana Rodgers, Carly Burns, Joe Htin, Jose Abadal, Matthew Demler	10 / 15
=14th	Darcy Eckert, Mary B, Michael A	9 / 15

Total participants: 20

Average Score: 9.8 / 15

Four AI Imperatives for Internal Audit

1

Re-evaluate Core IT Audits for AI-Speed Threats

2

Launch a 'Human Firewall' Audit Program

3

Mandate 'Trust but Verify' for Internal AI Tools

4

Integrate AI Governance into Enterprise Risk Universe

ARC Hybrid

Sharing Wisdom Together

QUESTIONS

60:00

Audit in Motion

SCOTT MADENBURG

AUDIT, RISK, COMPLIANCE
ADVISOR | TRAINER | SPEAKER

Let's Connect

- Founder of ARC*Hybrid*
- 20+ Years of Industry Experience
- CIA, CISA, and CRMA
- Transformative Leader and Market Advisor
- Trainer and Coach
- Recognized Speaker and Author
- Go-To-Market and Product Strategy Advisor

Empower your teams and elevate your impact with Scott:

- *Internal audit, risk, and compliance consulting*
- *Group training for internal audit and risk management*
- *Training for Boards and Committees*
- *Team-building workshops*
- *Career coaching sessions*
- *Inspiring keynote presentations*

ARC Hybrid

smadenburg@thearchybrid.com