



FROM HYPE TO CONTROLS: The Cloud, Regulation, and AI in the Internal Auditor's Crosshairs

IIA ATLANTA CONFERENCE

SIKICH.COM



The Institute of
**Internal
Auditors**

SEPTEMBER 25, 2025



JAMEY LOUPE

Principal
Practice Lead - Risk

Jamey is the Risk practice leader with more than 20 years of progressive experience leading and organizing IT audit and IT Security teams and projects. He has provided IT audit and advisory services to various Fortune 500 and mid-size multinational companies in multiple industries. Jamey has further experience in Information Technology Standards & Governance, IT Risk Assessments, Cloud Security and Governance, and Disaster Recover Planning. He has been actively involved in ISACA, ISC2, IIA, CSA and MCA&F for over 20 years.



SARGON YOUNMARA

Principal
GRC

Sargon is a partner with over 30 years of extensive experience in audit and management services. Sargon has a deep understanding of financial reporting, project management, business process improvement and risk management. A trusted advisor, he provides expertise leading Sarbanes-Oxley compliance initiatives, including the requirements of the Public Company Accounting Oversight Board (PCAOB), the Securities and Exchange Commission (SEC) and the Committee of Sponsoring Organizations (COSO).

OBJECTIVES

- Identify and understand the pivotal *cloud, regulatory, and AI* inflection points from 2005 to 2025.
- Understand how each “Megatrend” changed attack surfaces, compliance obligations, and control expectations.
- Discuss practical techniques to identifying and mitigating risks.
- Understand how to incorporate these “Megatrends” into your own risk assessment and internal audit program.

AGENDA

- EVOLUTION OF RISK LANDSCAPE
- CLOUD ERA
- REGULATION TAKES CENTER STAGE
- EMERGENCE OF AI
- AI GOVERNANCE
- FORWARD LOOKING HOLISTIC INTERNAL AUDIT STRATEGY
- CLOSING AND QUESTIONS

A blurred photograph of a crowd of people walking through a modern, brightly lit hallway with a grid-patterned wall and a reflective floor. The image is split vertically into a blue-tinted left half and a white-tinted right half. The text 'EVOLUTION OF RISK LANDSCAPE' is overlaid in white on the blue section.

EVOLUTION OF **RISK LANDSCAPE**

EVOLUTION & **EMERGING RISK**

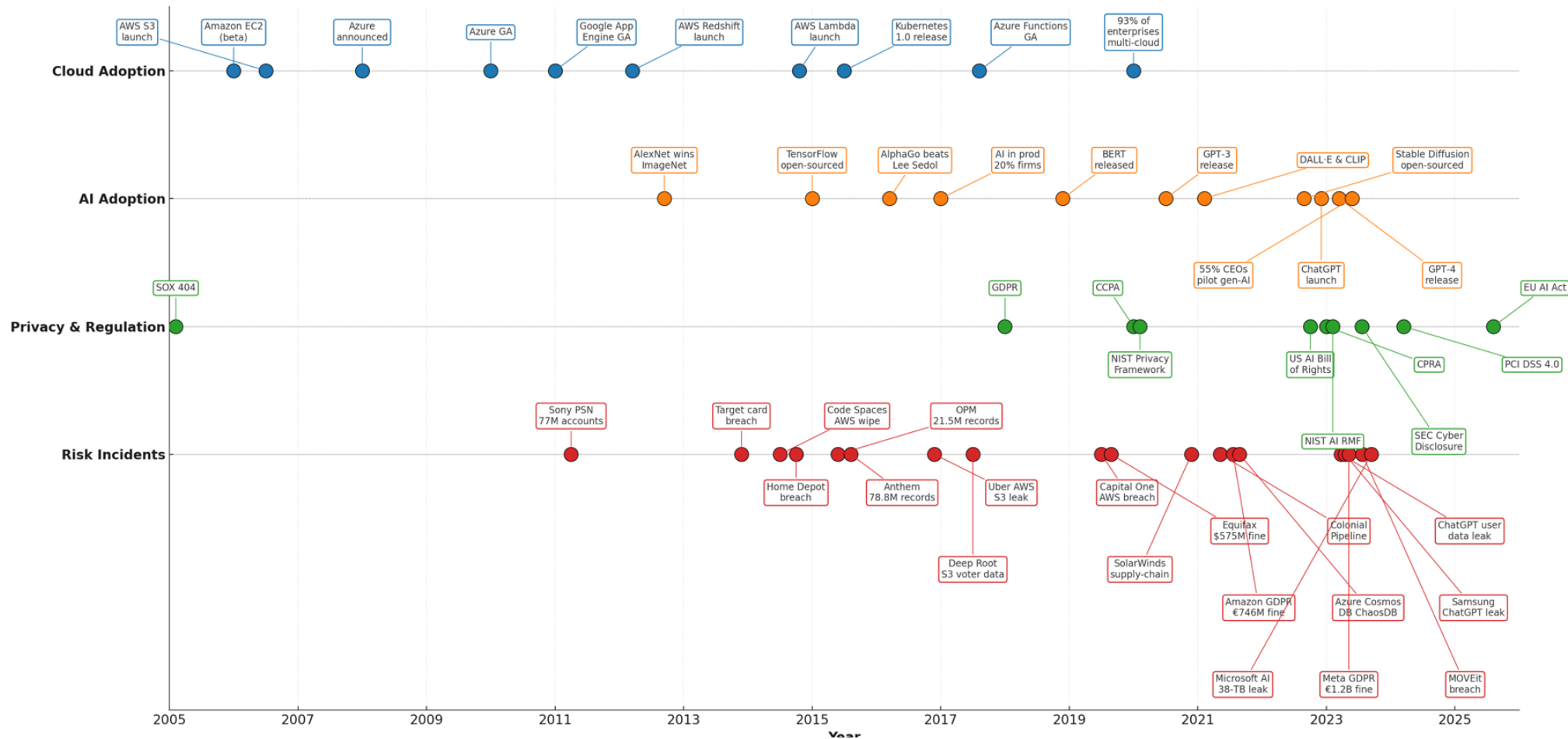
The last 20 years have reshaped the risk landscape faster than any previous era.

Three “Megatrends” that had the most impact in technology and the risk landscape:

1. Cloud adoption →
2. Regulation boom →
3. AI Expansion.

What does the Board and the Audit Committee expect of Internal Audit today?

CLOUD, PRIVACY/REGULATORY, & AI RISKS 2005 - 2025



EVOLUTION & EMERGING RISK

RISK CATEGORY	DESCRIPTION & AUDIT FOCUS
Data Privacy & Jurisdiction	Cloud storage often spans regions; data moves dynamically. Risks around privacy laws, cross-border data flows, and CSP access to data must be assessed.
AI-Specific Risks	Algorithmic bias, inaccuracy, accountability gaps, and model validation shortcomings can lead to flawed decisions. Auditors must validate model governance.
Cloud Configuration & Isolation Weaknesses	Multi-tenant environments, weak access controls, and insider threats heighten risks. Internal audit should evaluate segregation and monitoring controls.
Governance & Oversight	AI embedded without oversight poses data integrity and compliance risks. Embedding audit throughout AI lifecycle ensures accountability.
Talent & Readiness Gaps	Many audit teams lack AI/cloud expertise, hampering control assessments. Readiness maturity varies widely.
Dynamic Attack Surfaces	AI in cloud creates new, evolving threats—traditional periodic reviews aren't enough. Risk models must adapt.
External Expectations & Regulation	Regulators and DOJ increasingly push for AI risk review in compliance programs. Independent auditing of AI systems is a growing focus.

NEXT FIVE YEARS OF **RISK LANDSCAPE**

RISK THEME	WHY IT'S RISING	AUDIT EARLY WARNING SIGNAL
AI Supply-Chain Poisoning	Tampered model weights compromise downstream AI apps	Missing checksum / SBOM check
Synthetic Fraud & Deepfake Extortion	GPT-v5 multimodal + real-time voice cloning enables hyper-real scams	Spike in MFA resets or odd wire approvals
Cloud-Concentration Outage	3 hyperscalers host > 80% workloads; region failure = systemic impact	BCP tests skip region-wide failover
Quantum-Ready Encryption Gap	Post-quantum window ~4-6 years; legacy data at risk of 'steal-now-decrypt-later'	No crypto-asset register or quantum migration plan
RegTech Fatigue	Controls balloon (DORA, ISO 42001, ESG); owners face audit fatigue	More open remediation items; SOX testing slippage

NEXT FIVE TO 10 YEARS

Cybersecurity & Technology Risks

- AI-enabled attacks (adaptive phishing, botnets)
- Expanding IoT attack surface
- Quantum threats to encryption
- Governance gap – tech > regulation

Ethical & Societal Dilemmas

- Algorithmic bias in decisions
- Data privacy & misuse risks
- Weaponized AI & disinformation
- Job displacement & reskilling gap

Future of Risk

Geopolitical & Economic Instability

- Tech supremacy competition
- Cascading global cyber risks
- Adoption pressure vs. risk

Emerging Science & Clean Energy

- AI-driven biotechnology advances
- Clean energy & demands
- Quantum breakthroughs in science

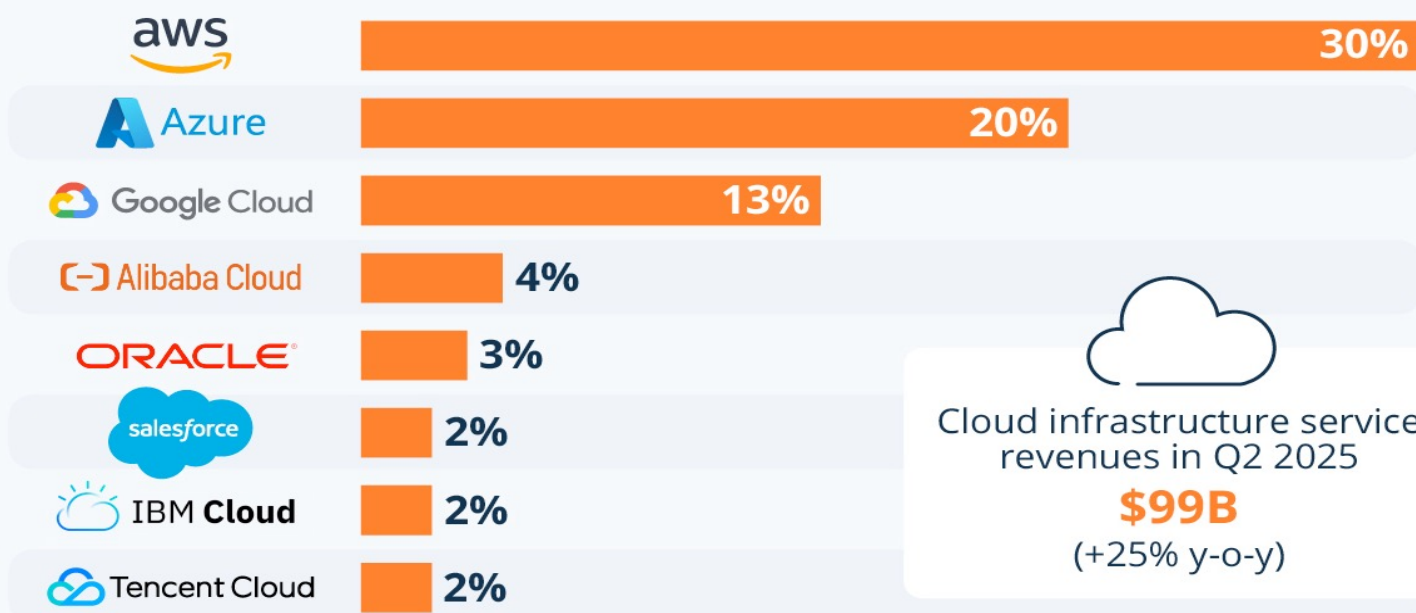
A blurred photograph of a crowd of people walking through a modern, brightly lit hallway with a grid-patterned ceiling and reflective floor. The image is split vertically into a blue-tinted left half and a white-tinted right half. The text 'CLOUD ERA' is overlaid on the left side in white.

CLOUD ERA

CLOUD ADOPTION

THEME	LATEST NUMBERS
Ubiquity	94 % of enterprise-size organizations (1 000+ employees) now run at least some production workloads in the cloud.
Workload Penetration	Over 50 % of all enterprise + SMB workloads—and data—are already in public clouds.
Multi-Cloud Normal	89 % of organizations report using two or more public clouds (up from 87 % the prior year).
Provider Split (enterprises)	AWS 30 % • Azure 20 % • GCP 13 % host “significant workloads.”
Cost Gravity	33 % of enterprises spend > \$12 M a year on public-cloud services; 11 % exceed \$60 M .
Top Challenge	84 % say managing cloud spend is harder than security; budgets expected to rise another 28 % in 2025.
Security & Governance	61 % of large enterprises now deploy multi-cloud security tooling; 57 % use multi-cloud FinOps tools to rein in costs.

Worldwide market share of leading cloud infrastructure service providers in Q2 2025*



* Includes platform as a service (PaaS) and infrastructure as a service (IaaS) as well as hosted private cloud services

Source: Synergy Research Group

RISKS OF CLOUD **ADOPTION**

- **Data Security & Privacy** – Risk of breaches, unauthorized access, data residency issues.
- **Regulatory Compliance** – GDPR, HIPAA, SEC, and sector-specific obligations.
- **Shared Responsibility Gaps** – Misunderstanding of what provider vs. customer secures.
- **Vendor Lock-In** – Difficulty migrating or multi-cloud strategy challenges.
- **Service Availability & Resilience** – Outages or disruptions affecting critical operations.
- **Configuration Errors** – Misconfigured storage buckets, IAM roles, or network settings.
- **Cost Overruns** – Poor visibility/controls over usage leading to unexpected expenses.

A blurred photograph of a crowd of people walking through a modern, brightly lit hallway with a grid-patterned wall and a reflective floor. The image is split vertically into a blue-tinted left half and a white-tinted right half. The text 'REGULATION TAKES CENTER STAGE' is overlaid in white on the blue section.

REGULATION TAKES **CENTER STAGE**

REGULATORY **TIMELINE**

Regulatory initiatives have started around the world and now technology risk is synonymous with regulatory risk!



Technology risk is now regulatory risk.

YEAR / REGULATION	KEY INTERNAL AUDIT IMPLEMENTATION
2010 – HIPAA / HITECH	Audit PHI safeguards; review access controls; test breach notification processes.
2016 – EU-US Privacy Shield	Audit cross-border transfers; validate contractual clauses; assess third-party compliance.
2018 – GDPR	Verify lawful basis for processing; review DPIAs; test subject rights (access/deletion); records of processing.
2020–2025 – U.S. State Privacy Laws	Test opt-out mechanisms; validate “Do Not Sell/Share” compliance; audit data retention and consent processes.
2023 – SEC Cybersecurity Disclosure Rule	Review incident response escalation and disclosure controls; validate Board reporting; test 10-K/8-K accuracy.
2023 – EU NIS2 Directive	Audit cyber resilience for critical infrastructure; test incident reporting obligations; review supply chain risk.
2024 – EU AI Act (phased 2025–2027)	Map AI systems to “high-risk”; review governance roles; audit model documentation and risk management system readiness.

KEY SHIFTS IN REGULATORY ENVIRONMENT: **THEN AND NOW**

What changed? Maturity and evolution in processes.

Regulators moved from policies on paper to proof of operating effectiveness.

THEN (2010'S)

- Privacy compliance = policy checklists, minimal enforcement
- Cyber disclosures = voluntary, often buried in risk factors
- Cloud risk = handled through SOC 2 reports from providers
- Regulators focused mainly on financial reporting (SOX) and sector-specific laws
- Internal Audit role = confirm policies exist and basic controls are documented







NOW (2020'S)

- Privacy = operational evidence required (GDPR DPIAs, DSAR SLA reporting, CPRA opt-out signals)
- Cyber = mandatory disclosure rules (SEC 8-K/10-K, NIS2 obligations)
- AI = new governance expectations (EU AI Act classification, monitoring transparency)
- Internal Audit role = confirm controls are operating and evidence can be produced under regulator scrutiny

REGULATIONS ON THE **HORIZON**

DOMAIN	UPCOMING REGULATIONS
AI Regulations	<ul style="list-style-type: none">▪ EU AI Act (2024): Phased rollout 2025–2027; classifies AI by risk (Prohibited, High-Risk, Limited, Minimal). High-risk systems (HR, credit, healthcare) require documentation, testing, and human oversight.▪ US: No federal AI law; NIST AI Risk Management Framework (2023) emerging as de facto standard. FTC actively policing deceptive or biased AI.▪ Global: UK, Canada, China drafting sector-specific AI rules.
Cloud Regulations	<ul style="list-style-type: none">▪ EU NIS2 Directive (2023): Effective 2024–25; expands incident reporting and supply chain oversight obligations for digital service providers (including cloud).▪ US SEC Cyber Rule (2023): Requires cyber governance disclosures in annual reports and timely reporting of material incidents (8-K within 4 business days).▪ Shared Responsibility Enforcement: Regulators increasingly scrutinize customer-side controls (e.g., IAM, misconfigurations).
Data Privacy Regulations	<ul style="list-style-type: none">▪ US State Privacy Laws: Over 20 states by 2025; obligations for opt-out, consent, sensitive data, and retention.▪ Cross-Border Transfers: Schrems II → Standard Contractual Clauses (SCCs) + Transfer Impact Assessments (TIAs). New EU–US Data Privacy Framework (2023) under legal challenge.▪ Sectoral Updates: Healthcare (HIPAA updates), financial services (Basel/AI guidance).

AI REGULATORY INITIATIVES **AROUND THE WORLD**

Characteristics	European Union 	United States 	United Kingdom 	China 	Canada 	Australia 
Regulatory Approach	Risk and Rights-Based	Market-Driven	Context and Market-Driven	State-Driven	Risk and Rights-Based	Risk and Rights-Based
AI Regulations / Initiatives	<p>EU AI Act</p> <p>General Data Protection Regulation</p> <p>Product Liability Directive</p> <p>EU Data, Digital Services, Digital Markets, Data Governance Act</p>	<p>Executive Order 14179: Removing Barriers to American Leadership in Artificial Intelligence</p> <p>Executive Order 14141: Advancing United States Leadership in Artificial Intelligence Infrastructure</p>	<p>Context and principle-based framework</p> <p>UK Online Safety Act</p> <p>UK Data Protection Framework and Digital Information Bill</p>	<p>Generative AI Regulation</p> <p>Personal Information Protection Law</p> <p>Deep Synthesis Regulation</p> <p>Algorithm Recommendation Regulation</p>	<p>AI and Data Act (proposed, part of Bill C-27, the Digital Charter Implementation Act), focused on responsible AI guidelines for development/deployment</p>	<p>AI Ethics Principles (voluntary guidelines)</p> <p>Roadmap for Developing a National AI Strategy</p>
Enforcement	<p>European AI Office</p> <p>National Data Protection Authorities</p>	<p>Office of Management and Budget (OMB) communicates to federal agencies how to comply with executive order (M-25-21, M-25-22)</p>	<p>Information Commissioner's Office</p> <p>Competition and Markets Authority</p> <p>Department for Science, Innovation, and Technology</p> <p>Sector-specific regulators</p>	<p>Ministry of Science and Technology</p> <p>National Development and Reform Commission</p> <p>Sector-specific regulators</p>	<p>Innovation, Science, and Economic Development Canada (ISED)</p> <p>Sector-specific regulators</p>	<p>Office of the Australian Information Commissioner (OAIC)</p> <p>Australian Competition and Consumer Commission (ACCC)</p>

ENFORCEMENT **TRENDS**

- **GDPR**
 - Meta (2023): €1.2B fine for unlawful EU-US data transfers.
 - Amazon (2021): €746M fine for advertising/data processing violations.
- **California Consumer Protection Act / California Privacy Rights Act**
 - Sephora (2022): \$1.2M fine for failure to honor opt-out requests.
- **SEC Cyber Rule / Cyber Disclosures**
 - SolarWinds executives (2023): SEC charges for alleged misstatements on cyber risk disclosures.
- **AI / FTC Enforcement**
 - FTC actions (2023–24): against AI vendors for deceptive claims and biased outcomes.

INTERNAL AUDIT'S ROLE IN **REGULATORY ERA**

ACTIVITY	WHAT IT MEANS	WHY IMPORTANT	IA'S ROLE
1. MAINTAIN A REGULATORY APPLICABILITY MAP	A simple matrix showing which regulations apply to which systems, data, or processes.	Overlapping laws (GDPR, CPRA, SEC Cyber, EU AI Act) create gaps if not tracked.	Check if management has a current map; e.g., which apps store EU data (GDPR), use AI (AI Act), or fall under HIPAA/NIS2.
2. VERIFY EVIDENCE EXIST AND IS CURRENT	Regulators want evidence, not just policies (DPIAs, SCCs/TIAs, SEC disclosure playbooks, AI model cards).	Companies often fail on producing artifacts quickly, not on having policies.	Sample-check that documents exist, are up-to-date, and align to actual practices.
3. TEST OPERATING EFFECTIVENESS	Go beyond "is there a process" to "does it work?" (mock DSAR, review last cyber incident, inspect configs).	Regulators expect proof processes work in practice, not just on paper.	Test outcomes: response times, documented decisions, correct configurations.
4. FACILITATE HORIZON SCANNING	Identify upcoming regulations before they take effect (EU AI Act 2025–27, new state privacy laws, sectoral updates).	Audit can be a trusted advisor by alerting leadership before obligations hit.	Brief leadership annually on regulatory changes that may alter controls.
5. COMMUNICATE READINESS TO AUDIT COMMITTEE & MANAGEMENT	Translate compliance into simple dashboards/readiness reports (e.g., % systems with DPIAs, AI gaps).	Boards face personal liability (SEC, EU). They need clear, concise visibility.	Provide assurance, highlight gaps, and outline remediation paths.

A blurred photograph of a crowd of people walking through a modern, brightly lit hallway with a grid-patterned ceiling and reflective floor. The image is split vertically into a blue-tinted left half and a white-tinted right half. The text 'EMERGENCE OF ARTIFICIAL INTELLIGENCE' is overlaid in white, bold, sans-serif capital letters across the center.

EMERGENCE OF **ARTIFICIAL INTELLIGENCE**

ARTIFICIAL INTELLIGENCE IN **ACTION**

There are many ways in which we can break down AI, including the following commonly known subsets.

Machine Learning (ML)

ML uses algorithms and data to assist computers in learning tasks or performing functions, without necessitating specific programming parameters. It includes supervised, unsupervised, reinforced, and deep learning.

Natural Language Processing (NLP)

NLP focuses on the study and analysis of linguistics as well as other principles of AI to create an effective method of communication between humans and machines or computers.

Robotic Process Automation (RPA)

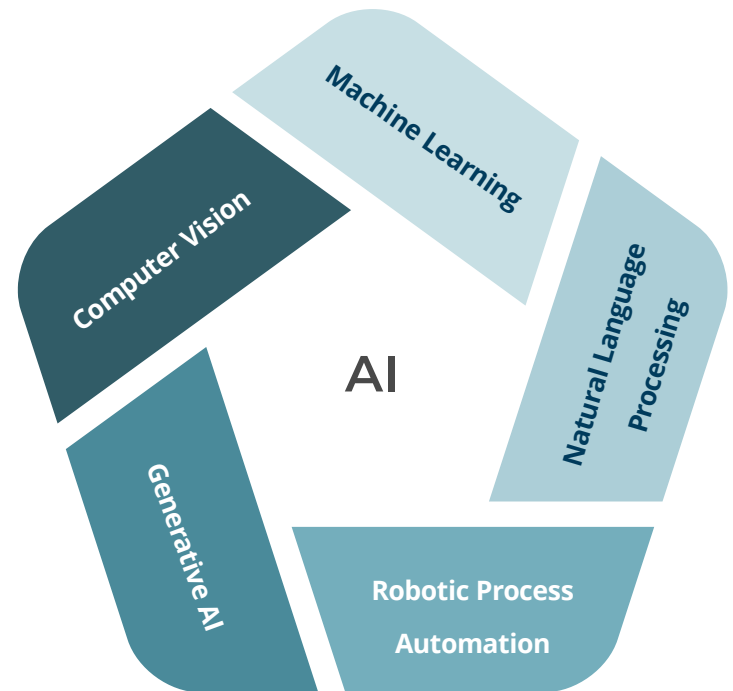
The focus of RPA is to drive business efficiency through automation of low-skills, tedious operational tasks, enabling focus to high-skills tasks, while reducing human errors.

Generative AI (Gen AI)

This subset of AI is focused on generating text, images, music, or even entire human-like conversations. These are designed to produce new, original data by learning patterns from existing datasets.

Computer Vision

Computer vision moves beyond simply translating a group of pixels into a corresponding image. It incorporates classification and segmentation of images.



AI ADOPTION TIMELINE

YEAR	MILESTONE	AUDIT & ORGANIZATION LEVEL RISK
2017	Only around 20 % of enterprises had any AI in production.	AI risks mostly theoretical; few IA programs address them.
2018	Adoption <i>doubles</i> in one year.	Enterprises start considering AI risk
Nov. 2022	ChatGPT launch ignites gen-AI craze.	Shadow-AI & data-exposure risk explode overnight.
2023	55 % of CEOs already piloting or deploying gen-AI.	Boards expect assurance on speed-to-value <i>and</i> control.
2025	78 % of firms use AI; 71 % use gen-AI in ≥ 1 function.	Continuous AI-control testing moves from “nice” to “necessary.”

AI RISK CATEGORIES FOR THE ORGANIZATION

Validity and Reliability

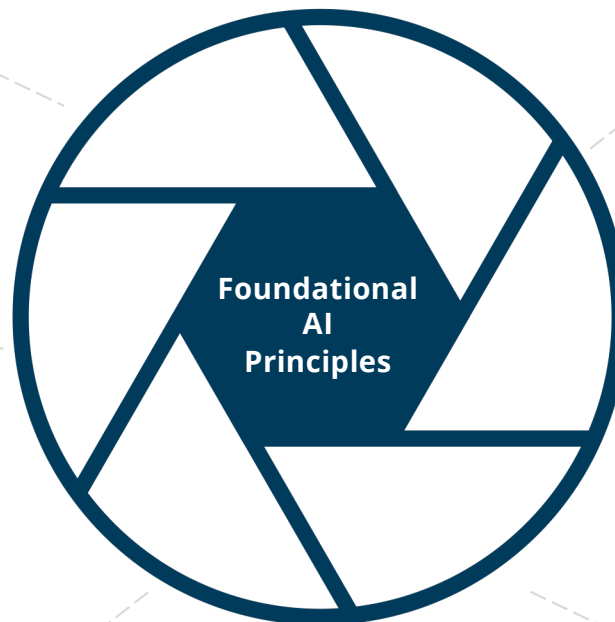
- Hallucinations
- Misinformation
- Deepfakes

Accountability

- Human-AI Configuration
- Environmental
- Lack of Human Oversight

Fairness and Bias

- Data Bias
- Algorithmic Bias
- Nonrepresentative Data



Safety and Security

- Harmful Responses
- Adversarial Attacks
- Data Poisoning

Data Privacy

- Intellectual Property
- Data Breaches
- Misuse of Data

Explainability and Transparency

- Reasoning Methodology
- Training Data
- Model Weights

THIRD PARTY VENDOR **AI RISKS**

- Lack of transparency and explainability.
- Intellectual property (IP) ownership.
- Model performance and maintenance.
- Vendor lock-in.
- Business continuity and exit strategy.
- Regulatory compliance.



ARTIFICIAL INTELLIGENCE FAILURES IN THE NEWS

TastingTable.

McDonald's Is Removing Its Current AI Technology From More Than 100 Drive-Thrus

March 2024

Copilot goes into autopilot, starts breaking rules

August 2023

Pregnant woman sues after AI accuses her of carjacking

April 2024

X's chatbot Grok accuses NBA player of going on vandalism spree after it misinterprets tweets about game

September 2023

AI-generated song submitted to the Grammys

June 2024

Microsoft Recalls CoPilot+

Rite Aid Banned from Using AI Facial Recognition After FTC Says Retailer Deployed Technology without Reasonable Safeguards

SECRET AI AGENTS

The next step on the AI journey

WHAT ARE THEY?

Autonomous systems that:

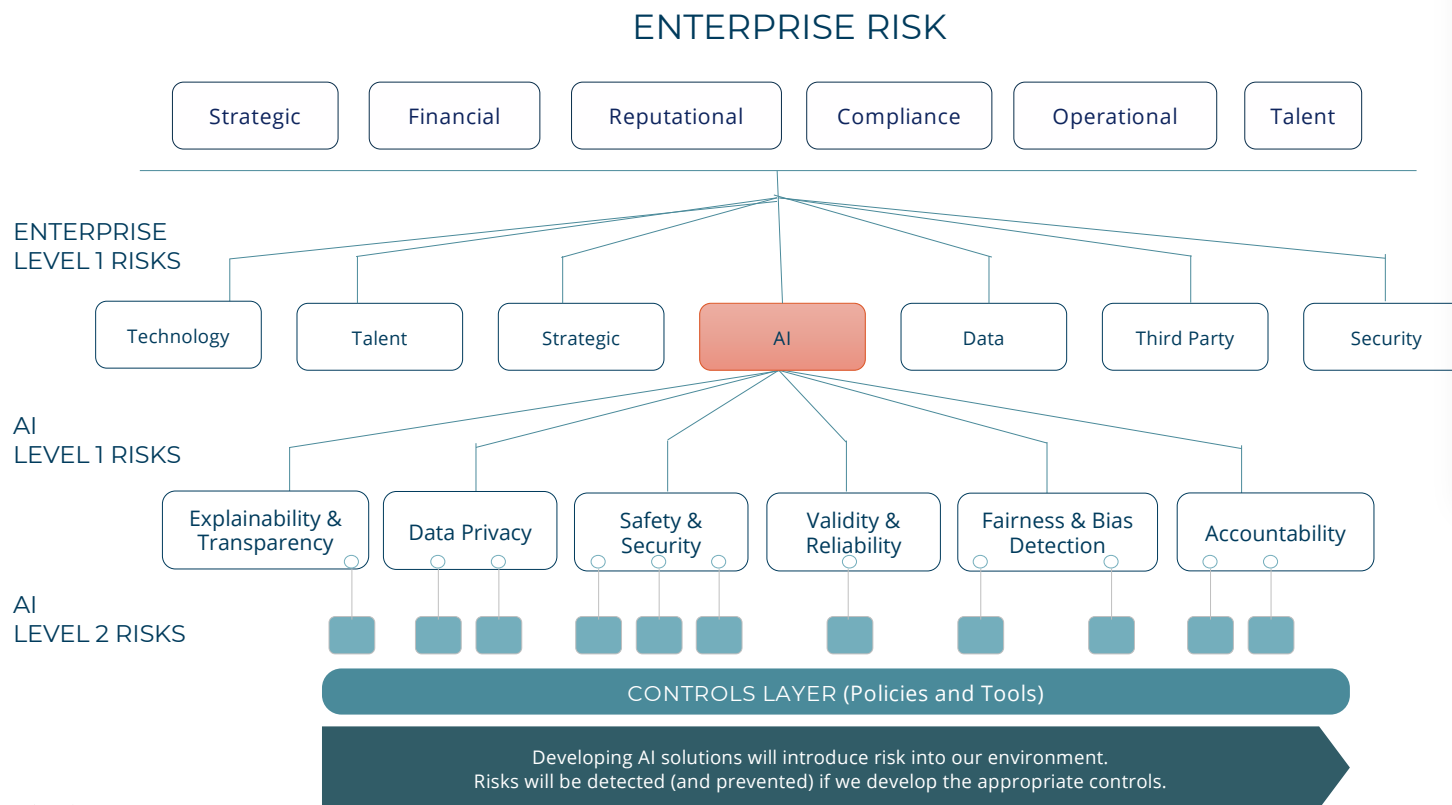
- Perceive their environment.
- Make decisions.
- Take actions to achieve goals.
- Learn from interactions.

WHY SHOULD YOU CARE?

- Autonomy is harder to monitor.
- Proactive actions by a machine are hard to regulate/control.
- Transparency can be obfuscated by the sheer number of actions and interactions.

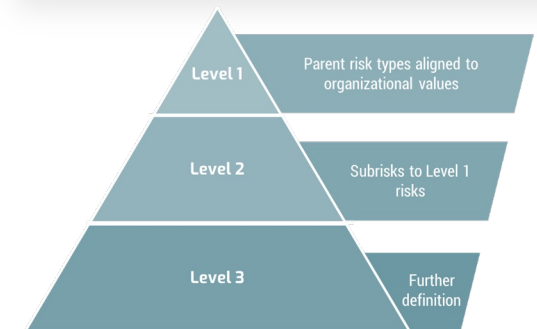
ALIGN YOUR AI RISK TAXONOMY

A risk taxonomy provides a common classification of risks that allows them to roll up systematically to enterprise risk, enabling more effective risk responses and more informed decision-making.



BEST PRACTICES

- Ensure your organization's values are embedded into the risk types.
- Design your taxonomy to be forward looking and risk based.
- Make Level 1 risk types generic so they can be used across the organization.
- Ensure each risk has its own attributes and belongs to only one risk type.
- Collaborate on and communicate your taxonomy throughout organization.



AI INNOVATION SHOULD BE **BALANCED WITH SAFETY**

SAFETY

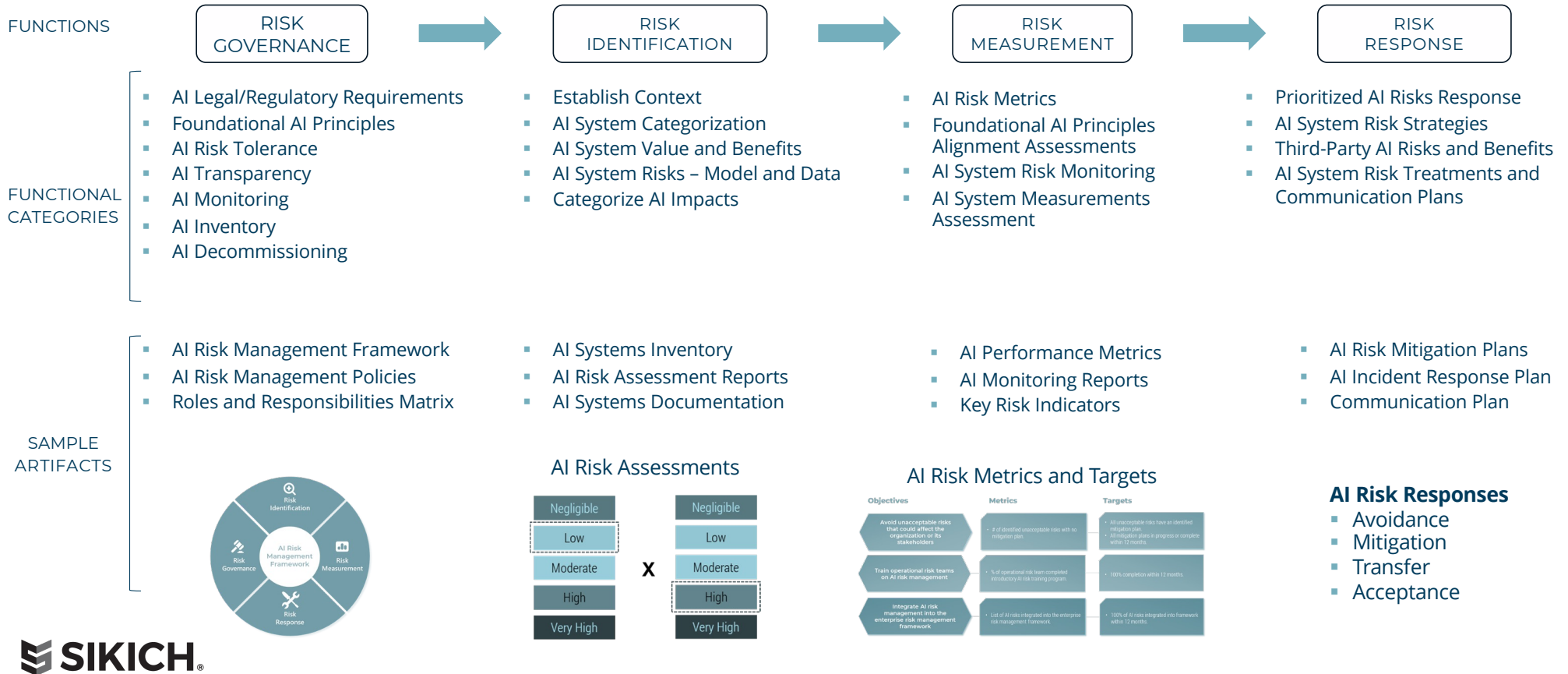
- Protect users/citizens from unintended consequences of AI applications.
- Establish organizations to be responsible and accountable for the use of their AI applications.
- Deliver a framework in which users/citizens have the right to file complaints against AI providers and compensation can be enforced.

INNOVATION

- Promote and enable the rapid and agile development and deployment of AI applications.
- Minimize bureaucratic oversight and compliance costs.
- Deliver an AI ecosystem/framework that promotes innovation and competition.

AI RISK MANAGEMENT FRAMEWORK **OVERVIEW**

CORE FUNCTIONS, FUNCTIONAL CATEGORIES, AND SAMPLE ARTIFACTS

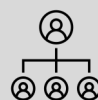


IIA AI AUDITING **FRAMEWORK**



Governance (Board / Audit Committee)

- Define AI vision, strategy, values, and risk appetite.
- Oversee accountability and ethics alignment.
- Monitor organizational readiness and oversight.



Management (1st & 2nd Lines)

- Establish AI policies, controls, acceptable use.
- Manage data integrity, cybersecurity, third parties.
- Execute AI with transparency, explainability, auditability.



Internal Audit (3rd Line)

- **Advisory:** Support AI strategy, governance, & leadership teams.
- **Assurance:** Test AI governance, controls, compliance.
- Evaluate AI risk inventory, lifecycle, and regulations.

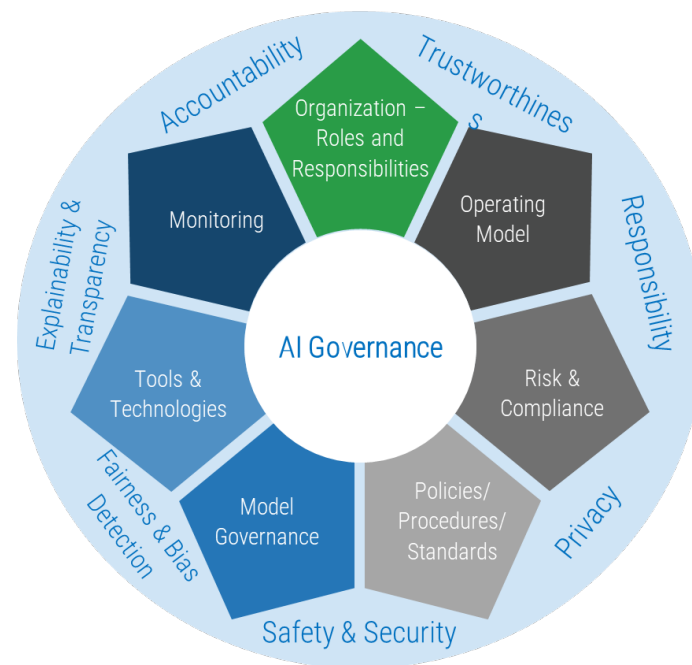
A blurred photograph of a crowd of people walking through a modern, brightly lit hallway with a grid-patterned ceiling and reflective floor. The image is split vertically into a blue-tinted left half and a white-tinted right half. The text 'GOVERNANCE OF ARTIFICIAL INTELLIGENCE' is centered across the middle in white capital letters.

GOVERNANCE OF **ARTIFICIAL INTELLIGENCE**

WHAT IS **AI GOVERNANCE**?

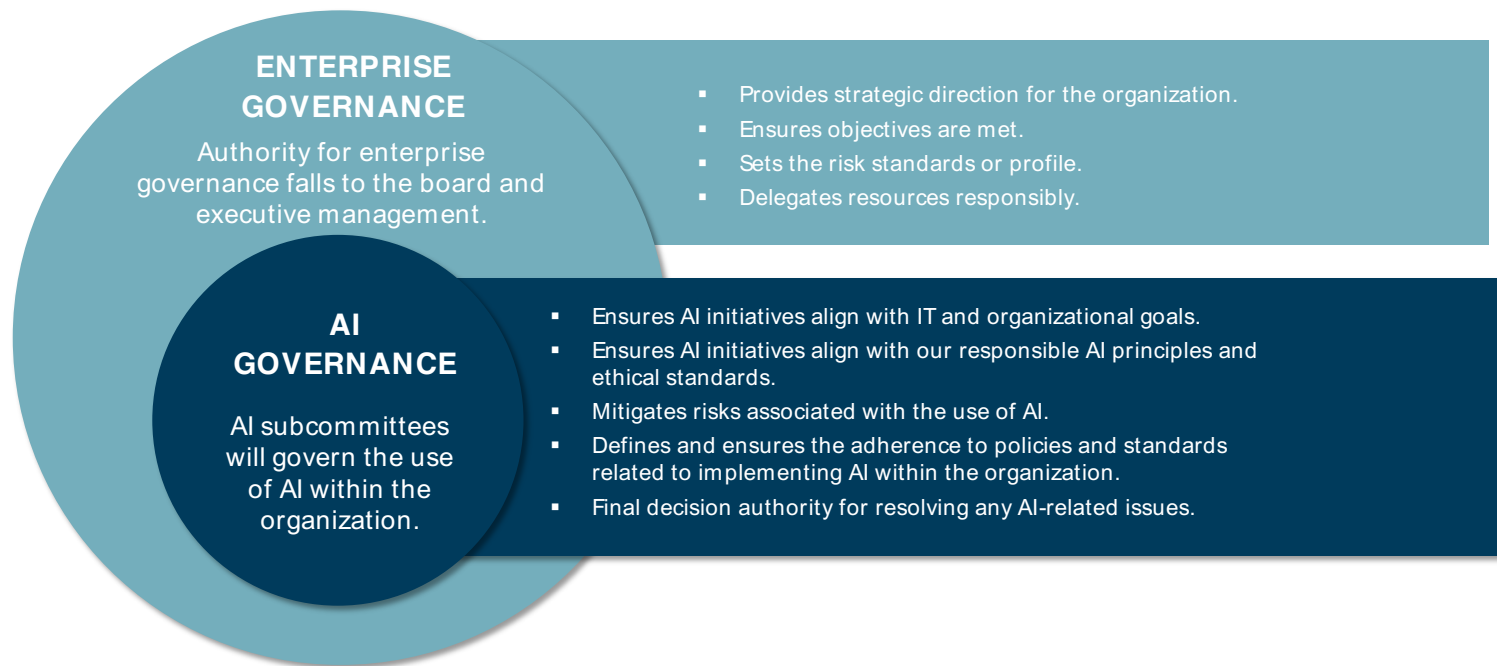
AI governance is a set of practices and structures that ensure investments, resources, and risks are aligned in the best interests of the organization and produce business value. AI governance is the extension of corporate governance to AI investments, resources, and risks.

- Extends **corporate governance** to AI investments, risks and resources.
- Align AI governance with **enterprise values and long-term strategy**
- Implements **responsible AI principles** (fairness, transparency, and accountability)
- Ensures AI is governed **across its lifecycle** (design → deployment → monitoring)



ALIGNING AI WITH **CORPORATE GOVERNANCE**

Corporate Governance is a system of rules, practices and processes by which an organization is directed and controlled set by the board and executives. AI Governance is no different.



FOUNDATIONAL **RESPONSIBLE AI PRINCIPLES**

Leveraging industry best practices and practitioner insights, we have identified the six foundational AI principles below:

DATA PRIVACY

Privacy values such as anonymity, confidentiality, and control will guide our choices for AI model/system design.

FAIRNESS AND BIAS DETECTION

We will endeavor to ensure any models/systems are fair and free from harmful bias.

EXPLAINABILITY AND TRANSPARENCY

AI actors will be accountable for the functioning of AI systems.

SECURITY AND SAFETY

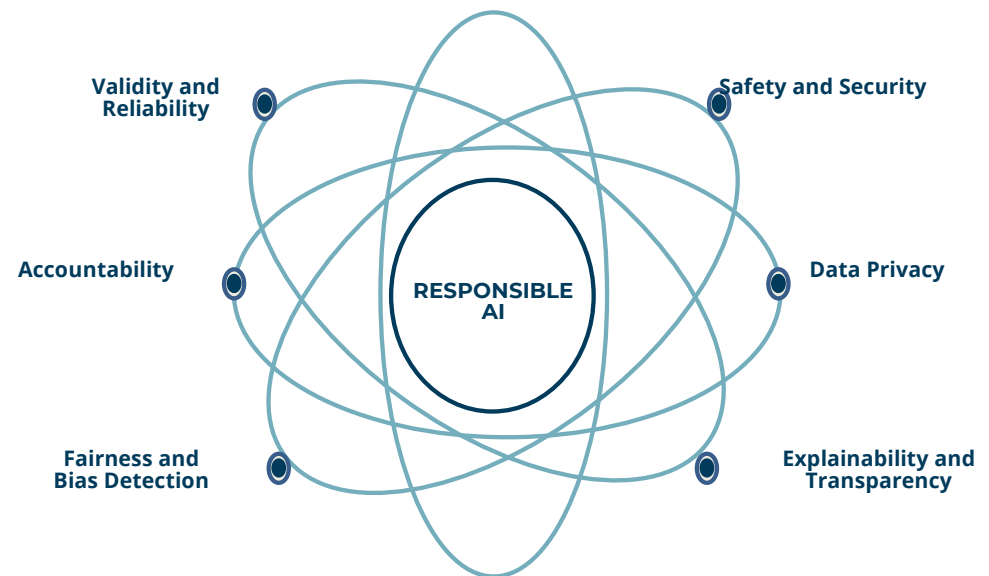
AI model/systems should be resilient, secure, and safe throughout their entire lifecycle

VALIDITY AND RELIABILITY

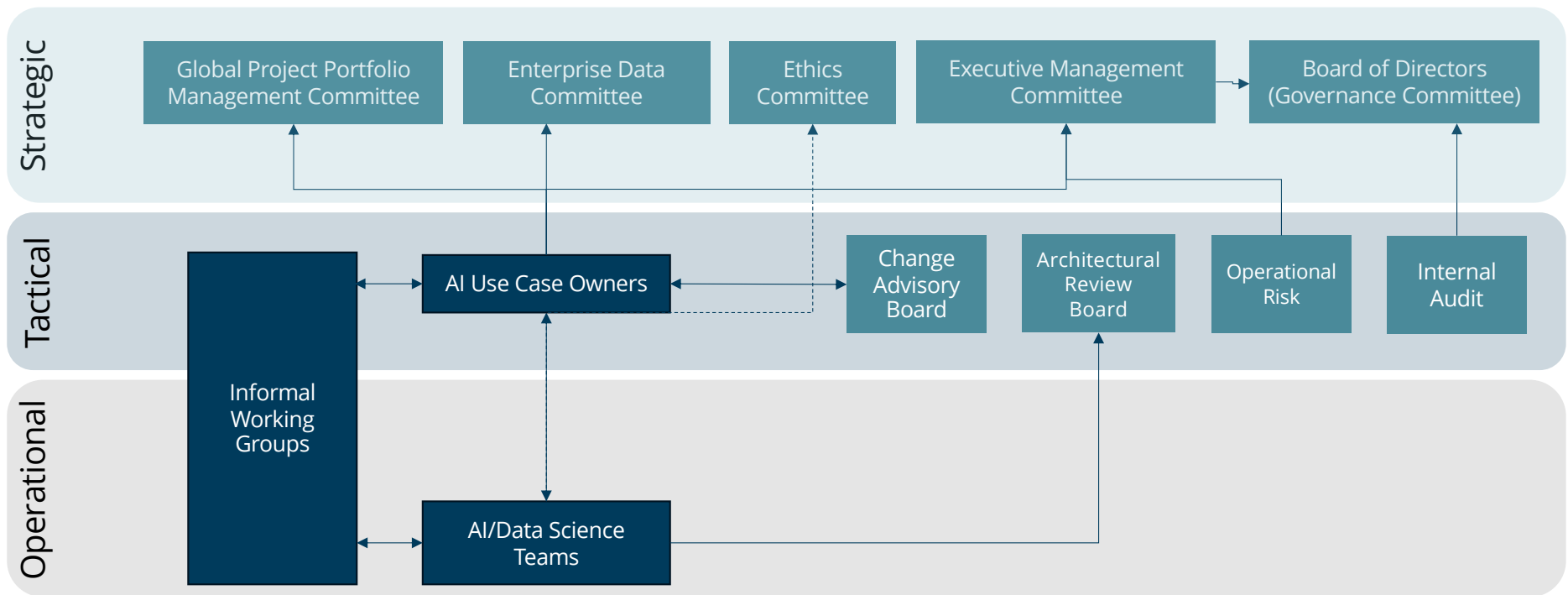
AI systems should perform reliability and as expected.

ACCOUNTABILITY

AI actors will be accountable for the functioning of AI systems.



Example AN ORGANIZATION'S GOVERNANCE STRUCTURE



WHY **AI GOVERNANCE** IS CRITICAL (IBM)?

AI governance is a set of practices and structures that ensure investments, resources, and risks are aligned in the best interests of the organization.

FINDING	STATISTIC	INTERPRETATION / WHY IT'S IMPORTANT
Dependence on people vs. technology	64% of CEOs say success with Gen AI depends more on people's adoption than the technology itself. (IBM Newsroom)	Technology alone isn't enough — culture, change management, training, and workforce readiness are critical. Without adoption, even excellent tools may underperform.
Governance recognition vs implementation	75% of CEOs say “trusted AI is impossible without effective AI governance”; only 39% believe they have good generative AI governance in place today. (IBM Newsroom)	There is a big gap: many leaders believe governance is necessary, but few think their organizations have matured to that point. Huge opportunity for audit oversight.
Speed vs comfort / risk	61% say the organization is pushing generative AI adoption more quickly than some employees are comfortable with. (PR Newswire)	Rushing ahead can trigger risks: poorly controlled systems, backlash, mistakes. Suggests need for balance.
Workforce impact	63% say their teams have the skills/knowledge to incorporate Gen AI. (IBM Newsroom) • 56% have not yet assessed the impact of generative AI on their employees. (PR Newswire) • 51% are hiring AI roles that didn't exist last year; 47% expect workforce reduction or redeployment in next 12 months. (PR Newswire)	Shows both opportunity (new roles, new skills) and risk (disruption, retraining, potential job shifts). Auditors should check whether workforce and HR risk are being managed.
Cultural & collaboration challenges	65% say success depends on collaboration between finance & tech; but 48% say internal competition among C-Suite hinders collaboration. (PR Newswire)	Governance isn't just structure; culture matters. Silos and internal friction undermine governance and risk management.

AI RISK MANAGEMENT FRAMEWORK – WHAT **INTERNAL AUDIT** TESTS?

AI governance follows the same cycle as enterprise risk management — governance, identification, measurement, and response. Internal Audit's role is to verify that each step is operating effectively across the AI lifecycle.

FRAMEWORK STEP	WHAT MANAGEMENT DOES	INTERNAL AUDITOR'S RESPONSIBILITIES	EVIDENCE TO TEST
Governance	Define AI policies, assign roles & accountability.	Assess clarity of governance, check Board oversight, evaluate committee structure.	AI governance policy, RACI chart, Board minutes, committee charters.
Identification	Maintain AI system inventory, classify risk levels (E.g., prohibited, high risk, low risk).	Verify inventory completeness, test classification criteria.	AI system inventory, risk categorization matrix, project register.
Measurement	Monitor model performance, track bias, set KRIs; validate explainability.	Evaluate monitoring process, sample metrics, check bias testing.	Model cards, validation results, bias testing reports, monitoring dashboards.
Response	Apply controls (avoid, mitigate, transfer, accept); conduct incident response.	Review mitigation actions, test incident response & remediation.	Risk assessments, mitigation plans, AI incident logs, remediation reports.

AI RISK MANAGEMENT FRAMEWORK – WHAT **INTERNAL AUDIT** TESTS?

AI governance follows the same cycle as enterprise risk management — governance, identification, measurement, and response. Internal Audit's role is to verify that each step is operating effectively across the AI lifecycle.

FRAMEWORK STEP	WHAT MANAGEMENT DOES	INTERNAL AUDITOR'S RESPONSIBILITIES	EVIDENCE TO TEST
Governance	Define AI policies, assign roles & accountability.	Assess clarity of governance, check Board oversight, evaluate committee structure.	AI governance policy, RACI chart, Board minutes, committee charters.
Identification	Maintain AI system inventory, classify risk levels (E.g., prohibited, high risk, low risk).	Verify inventory completeness, test classification criteria.	AI system inventory, risk categorization matrix, project register.
Measurement	Monitor model performance, track bias, set KRIs; validate explainability.	Evaluate monitoring process, sample metrics, check bias testing.	Model cards, validation results, bias testing reports, monitoring dashboards.
Response	Apply controls (avoid, mitigate, transfer, accept); conduct incident response.	Review mitigation actions, test incident response & remediation.	Risk assessments, mitigation plans, AI incident logs, remediation reports.

INTERNAL AUDITOR'S ROLE IN AI GOVERNANCE

Internal Audit ensures that AI investments, resources, and risks are aligned with organizational objectives, laws, and ethical expectations. IA's role extends corporate governance to AI by providing **independent assurance and advisory support**.

- **Evaluate AI Governance Frameworks** – Review whether policies, committees, and accountability structures exist and are effective.
- **Assess AI Risk Management** – Test how AI risks are identified, categorized, monitored, and mitigated.
- **Review Data Governance & Integrity** – Validate data quality, lineage, access controls, and protection of sensitive data.
- **Audit Compliance with Regulations** – Ensure readiness for GDPR, CPRA, SEC Cyber, EU AI Act, and emerging AI/Privacy laws.
- **Ensure Transparency & Explainability** – Verify models can be explained to regulators, customers, and management.
- **Provide Assurance & Advisory** – Offer independent assurance to the Board, while advising management on emerging risks.
- **Monitor Third-Party AI Risks** – Evaluate reliance on vendors/SaaS providers embedding AI in tools; confirm contracts assign clear responsibility.
- **Facilitate Horizon Scanning** – Brief leadership on upcoming AI regulations and assess organizational readiness.

The image features the Kahoot! logo in a large, white, rounded font. The background is a stylized world map with four distinct color-coded quadrants: red for the top-left (North America and Europe), blue for the top-right (Europe and Asia), yellow for the bottom-left (South America and Africa), and green for the bottom-right (Africa and Asia).

Kahoot!

A blurred photograph of people walking in a modern, brightly lit hallway. The background features a wall with a grid pattern and circular ventilation holes. The floor is highly reflective. The image is split vertically into a blue-tinted left half and a white right half.

FORWARD LOOKING **INTERNAL AUDIT APPROACH**

KEY ACTIONS FOR **INTERNAL AUDITORS**

Internal Audit ensures that AI investments, resources, and risks are aligned with organizational objectives, laws, and ethical expectations. IA's role extends corporate governance to AI by providing **independent assurance and advisory support**.

- **People** – Upskilling and training.
- **Process** – Risk-based approach, collaboration and shared responsibility.
- **Tools** – Data lifecycle, privacy, documentation and continuous auditing.

FUTURE-READY **INTERNAL AUDIT**



1. **Upskill and Educate**

- Build knowledge of Cloud & AI (IaaS, PaaS, ML, NLP, Generative AI).
- Track evolving regulations (GDPR, CCPA, HIPPA, AI laws).
- Develop AI audit methodologies (bias, fairness, transparency, data provenance).



2. **Adopt a Risk-Based Approach**

- Prioritize audits on critical cloud/AI systems handling sensitive or high-risk data.
- Integrate cloud & AI risks into enterprise risk framework.



3. **Collaborate with Stakeholders**

- Partner with IT & Security to understand AI/cloud architectures and controls.
- Engage Legal & Compliance to ensure regulatory alignment.
- Communicate risks and recommendations clearly to leadership & audit.

FUTURE-READY INTERNAL AUDIT



4. Leverage Cloud-Native and AI-Powered Audit Tools

- **Cloud Security Posture Management (CSPM):** Utilize CSPM tools to continuously monitor cloud configurations and compliance deviations.
- **Cloud Access Security Brokers (CASB):** Employ CASB solutions to gain visibility and control over cloud usage, enforce security policies and detect threats.



5. Focus on the Shared Responsibility Model

- **Verify Client-Side Controls:** Ensure the organization is diligently fulfilling its responsibilities for security “in the cloud”, including access management, data encryption, network configuration, and application security.
- **Review Cloud Provider Attestations.**



6. Emphasize Data Lifecycle Management

- **Data Discovery and Classification:** Confirm that organization has a clear inventory of all data stored in the cloud, including access management and data encryption.
- **Data Minimization:** Assess the use of techniques to protect personal data is collected and retained analysis.

FUTURE-READY **INTERNAL AUDIT**



7. Promote a Culture of Privacy & Security

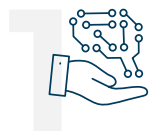
- **Advocate for Privacy by Design:** Encourage the integration of privacy principles into the design and development of all cloud-based systems and AI applications.
- **Continuous Improvement:** Foster a culture of continuous improvement in data privacy and security practices, driven by ongoing monitoring, regular audits, and lessons learned.



8. Document Everything

- **Maintain Comprehensive Documentation:** Document all audit findings, control recommendations, management responses, and remediation efforts related to cloud and AI data privacy.
- This is crucial for demonstrating due diligence and compliance.

KEY TAKEAWAYS



The risk landscape is rapidly changing, and the next five years will see more change.



Governance is essential for risk management and creating trust.



Effective oversight requires a combination of technical and procedural controls.



Internal Auditors play a crucial role in ensuring risk mitigation and the effectiveness of governance.



A risk-based approach that includes the key “megatrends” can help prioritize audit efforts and address emerging risks.



Documentation and transparency are foundational elements.

ANY QUESTIONS?



JAMEY LOUPE

JAMEY.LOUPPE@SIKICH.COM

Jamey's
LinkedIn
Profile



SARGON YUMARA

SARGON.YUMARA@SIKICH.COM

Sargon's
LinkedIn
Profile



THANK YOU

