Unleash AI Governance

FROM GATEKEEPER TO GROWTH DRIVER

AI+IM GLOBAL SUMMIT

Susan Gleason, AIGP, CIP, CRM/CIGO, IGP

Doron Goldstein, AIGP, CIPM, CIPP/E, CIPP/US, FIP, PLS

AI+IM GLOBAL SUMMIT

Amara's Law:

"We tend to overestimate the effect of a technology in the short run and underestimate the effect in the long run."

- Futurist Roy Amara

AI+IM GLOBAL SUMMIT

What is AI?

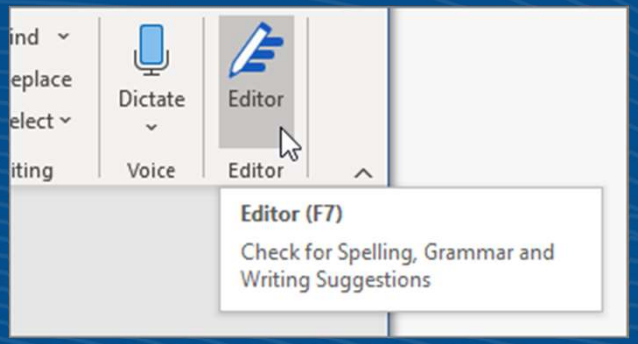
- A Machine or system that performs tasks that are normally considered to require human intelligence, or that behaves (or appears to behave) intelligently/ performs tasks that were assumed to be things only people (or other intelligent beings) could perform
- Turing Test: produces responses to a human interviewer that can fool the interviewer into thinking that they are human.
- Expectations of what AI is have changed (and will continue to change) over time.

Types of AI

- Artificial Narrow Intelligence (ANI) – Single task (e.g., play chess); automates repetitive tasks
- Broad AI – Multiple tasks, replying on multiple ANIs (e.g., self-driving cars)
- Artificial General Intelligence (or Full/Deep AI) – Closely resembles human intelligence; can think and learn unrelated tasks
- Artificial Super Intelligence (HAL 9000….) – Can perform a broad range of tasks better than humans

AI before ChatGPT

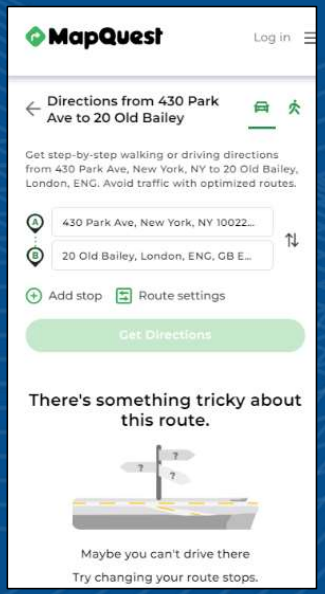
Chess Challenger (1977)



Microsoft Word Grammar Checker (1992)

Google Translate (2006)

Apple Siri (2011)



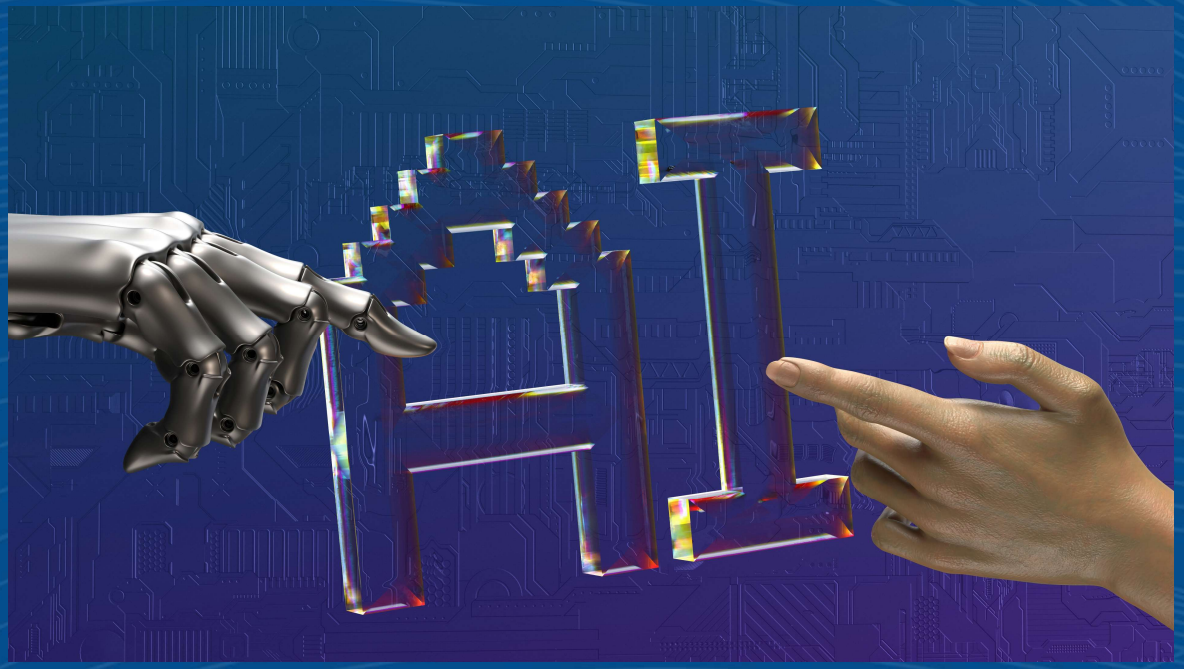
MapQuest (1996)

AI+IM GLOBAL SUMMIT

AI is Everywhere

- AI is now included (and often touted) in many software products
- Some are narrow, some more broad (not including GenAI)
  - **Salesforce Sales Cloud (with Einstein AI)** – Predictive lead scoring, opportunity insights, sales performance intelligence.
  - **Workday ERP** – Uses machine learning for anomaly detection, forecasting, and HR analytics (esp. in finance/workforce).
  - **Mimecast** – Embeds AI and machine learning, including for threat detection & anomaly analysis, natural language processing (NLP), machine learning & behavioral analytics, and AI security.
  - **Oracle Fusion Cloud** (vs. Oracle GenAI functions) – AI for financials, supply chain insights, and operational data analysis.
  - Shadow AI in Organizations

How to approach AI Governance



AI+IM GLOBAL SUMMIT

Generally Accepted Record Keeping Principles (aka "The Principles")

Accountability Principle of Transparency Principle of Integrity Principle of Protection	•Principle of Compliance •Principle of Availability •Principle of Retention •Principle of Disposition

AI+IM GLOBAL SUMMIT

Guidelines for AI Governance

- Transparency
- Accountability
- Bias Mitigation and Fairness
- Safety and Reliability
- Privacy and Data Security
- Compliance with Regulations
- Inclusiveness and Sustainable Innovation
- Data Governance
- Audits and Monitoring
- Human-Centricity

GARP

- **Principle of Accountability**
- **Principle of Transparency**
- **Principle of Integrity**
- **Principle of Protection**
- **Principle of Compliance**
- **Principle of Availability**
- **Principle of Retention**
- **Principle of Disposition**

AI

- Transparency
- Accountability
- Bias Mitigation and Fairness
- Safety and Reliability
- Privacy and Data Security
- Human-Centricity
- Inclusiveness and Sustainable Innovation
- Data Governance
- Audits and Monitoring
- Compliance with Regulations

AI Model Lifecycle

1. Development
2. Training operationalization
3. Model deployment
4. Prediction serving
5. Monitoring
6. Retirement

Data Inventory, Ownership and Segregation

AI+IM GLOBAL SUMMIT

Data Mapping

- Why Map?
  - Basic source of information and foundational building block for compliance and operations
  - Identification of both operational and regulatory risk
  - Implementation of controls and processes
  - Necessary for incident response
  - Allows AI systems to know what they are touching

Data Mapping (cont.)

- Building the Data Map
  - Scope and process owner(s)
  - Discover locations and sources
  - Classify the data
  - Document data flows and access/roles
  - Validate, maintain and update

Data Ownership and Control

- Who owns each data type (and who has rights)
  - Disgorgement?
- Is the data subject to any other regulatory or legal requirements (e.g., SEC, privilege)?
- Data lifecycle details, such as creation, retention, archiving, disposal
- Key uses, sharing and access permissions

ROT

- 81% of AI investments are using flawed data
- 90% of AI Leaders believe leadership is failing to focus on it.
- 77% of companies with $5B+ in revenue expect poor data quality to cause a major crisis
- 65% of the above still believe their AI strategy is on the right path

Qlik Research, 3/5/25

Context ROT

- AI Conversations can gradually lose accuracy and reliability over time.
- An uncontrolled stream of information can lead to inaccuracy in the agent

AI+IM GLOBAL SUMMIT

How do we improve the data quality?

AI+IM GLOBAL SUMMIT

How do we improve data quality?

- Define AI-ready data standards for accuracy, completeness, consistency, timeliness and bias
- Valid data before use (automated checks for required fields, formats)
- Clean and standardize existing data (de-dup, update stale records, apply retention)
- Keep humans in the loop (data stewards and business users should review data)

AI Committee

AI+IM GLOBAL SUMMIT

Privacy and AI Legal / Regulatory Compliance

- Is there any personal data (and the definitions can be broad and differ)?
- Is the data subject to any other regulatory or legal requirements (e.g., SEC, privilege)?
- Might there be export control or sanction issues?

Current AI-specific Laws (examples)

- Internationally: EU AI Act; China (multiple laws and regulations)
- US: No federal law (Executive Orders); Multiple State Laws; Municipalities (e.g., NYC AI in Employment)
- Laws may apply at different levels, based on role (developer/deployer), model size ("frontier models") and/or purpose (employment, chats).

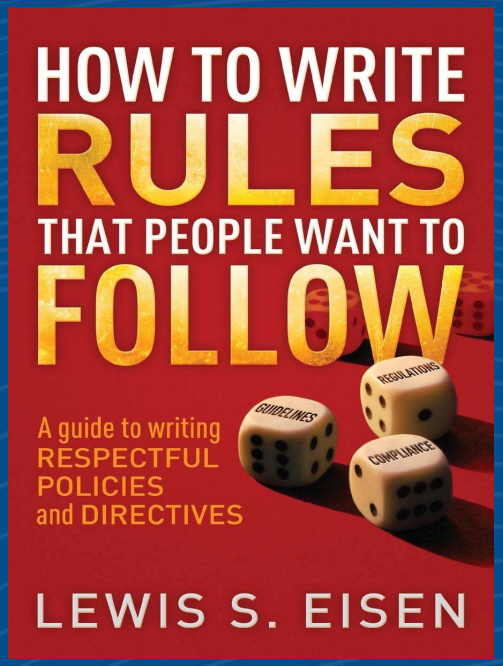
Current Key Frameworks (examples)

- NIST AI Risk Management Framework (RMF)
  https://airc.nist.gov/airmf-resources/playbook/
- ISO/IEC 42001
- OECD AI Principles
- IEEE 7000-2021

Framework Comparison

Dimension	IEEE 7000-2021	OECD AI Principles	EU AI Act	NIST AI RMF
Scope	System design ethics	Full AI value chain	Risk-based classification	Organizational Risk Management
Enforcement	Voluntary	Softlaw principles	Legally binding	Voluntary
Accountability	Design-stage value alignment	Proportional answerability	Provider / deployer obligations	Govern function roles
Strength	Engineering integration	International Consensus	Legal enforceability	Operational practicality
Certification	No	No	Compliance Required	No, but pairs with ISO/IEC 42001

AI Policies



VS

AI+IM
GLOBAL SUMMIT

AI Policies

- Governance = “How we can” instead of “Why we Can’t”
- The expansion of information governance → AI governance
- Governance as Growth—how guardrails create speed while reducing/mitigating risks.

The Gatekeeper Model is failing

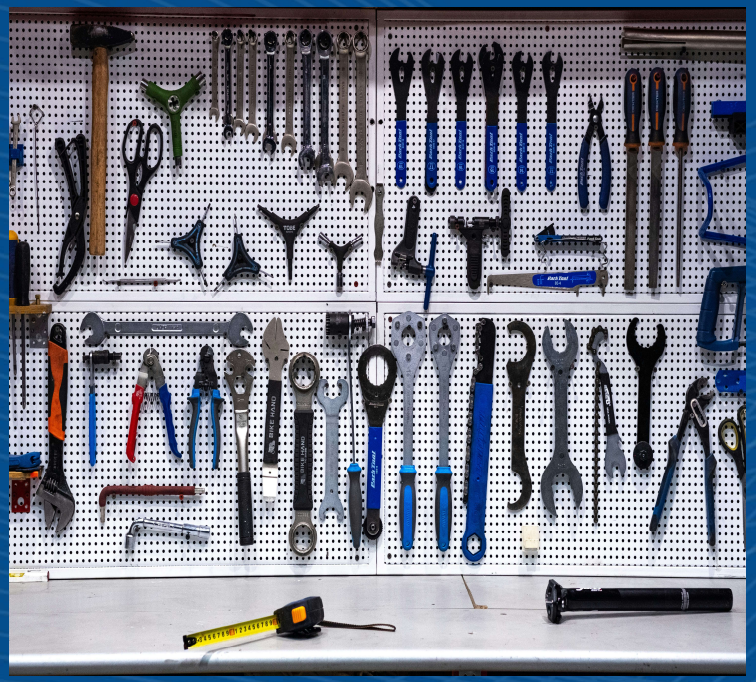
- Innovation Lag
- Trust Erosion
- Process Silos
- Shadow AI Usage

Changing the mindset

Attribute	The Old Gatekeeper	The New Growth Driver
Primary Goal	Risk Avoidance	Trusted Innovation
Involvement	End-of-lifecycle review	Embed in the lifecycle
Focus	What we can't do	How we do it safely
Success Metric	Compliance Audits	User adoption
Mindset	Defensive / Protective	Strategic / Enabling

AI+IM GLOBAL SUMMIT

AI Tool Diligence



AI+IM GLOBAL SUMMIT

AI Tool Diligence

- Key part of understanding and doing AI risk/benefit analysis and implementing appropriate controls.
- There are no industry standards on fundamental issues like ingestion and training, retention/deletion, security, breach or fail notification.
- Requires legal/compliance, data/governance, business/operational, IT/technical and security review of the tool and documentation

AI Tool Diligence (cont.)

- Process:
  - Inventory and classification of tools (based on function, risk, etc.)
  - Vendor risk assessment – both of the tool and the vendor itself
  - Compliance and security review
  - Legal and contractual review
  - Approval (and conditions/controls/exceptions)
  - Monitoring, auditing and reassessing

AI Tool Pilot

AI+IM
GLOBAL SUMMIT

AI Tool Piloting

- Buying AI quickly without considering impact and where it fits in the puzzle
  - The gold rush encouraged fast decisions without considering strategy and integration.
  - AI as a solution to an undefined problem, rather than examining the problem and determining if/what tools (AI or otherwise) can be used to resolve/mitigate it.
  - Ensuring correct people are involved in the pilot
  - 90%+ of AI projects fail

AI Tool Piloting (cont.)

- Why pilot before deploying?
- *AI tools carry real governance risk – piloting can help surface risks/issues early*
  - *Data exposure – what data enters, is retained, is used for training, etc.*
  - *Use cases – what is it good/bad for; who can use it; how are controls implemented, etc.*
  - *Value analysis – does it actually solve the particular problem(s)*
  - *Shadow AI controls – without pilots, personnel will experiment anyways*

AI Tool Piloting (cont.)

- Pilot Process
  - *Define scope and risk*
  - *Initial vendor due diligence*
  - *Implement controlled/limited pilot, and perhaps expand after initial stage*
  - *Evaluate and decide on implementations*

AI Impact Assessment

AI+IM GLOBAL SUMMIT

AI Impact Assessment

- An AIIA is a structured process to identify, document, and mitigate the risks an AI system poses before and during deployment
  - Invisible Harms: AI systems can discriminate, leak sensitive data, and produce unreliable outputs — are better surfaced through deliberate assessment, rather than accidentally through use.
  - Increased Regulation
  - Identifies Governance Gaps

AI Impact Assessment (cont.)

- Key Domains:
  - Purpose and Risk
  - Data Lineage/Retention
  - Privacy and Security
  - Legal Basis and Regulatory Requirements
  - Bias and Disparate Impact
  - Human Oversight and Accountability
  - Vendor and Contractual Controls

Training

AI+IM GLOBAL SUMMIT

Training

- Necessary to address legal, operational and reputational risk.
- Compliance Risk Without Training
  - Sensitive data exposure, improper use for regulated purposes, etc.s
- AI Doesn't Behave Like Other Software
  - Personnel must understand how specific tools/models work, what the use cases are for each, and how to evaluate prompts and outputs
- Training is Required by Governance Frameworks
  - Lack of training is a gap in compliance with various frameworks

Training (cont.)

- General Training (all personnel)
  - What AI can and cannot do — address over-trust and under-trust
  - Data input and output rules and limitations
  - Approved tools vs. shadow AI — your organization's permitted list
  - Incident reporting: what to do when AI produces problematic output
- Role-Based Trainings (targeted by function & risk)
  - Certain roles (based on access to sensitive data, use cases for outputs, etc.

Model Cards

AI+IM GLOBAL SUMMIT

Model Cards

- A standardized disclosure document that tells you what an AI model does, how it was built, and where it falls short.
- Governance artifacts — allow accountability, enable oversight, and support compliance.
- Like a nutrition label for an AI model. Just as a nutrition label tells you what's in your food — calories, allergens, ingredients — a model card tells you what's in your AI
- Developed by developers (vendors) or deployers

Model Cards (cont.)

- Intended Use
  - What is the model is designed to do — and what it is not.
- Training Data
  - The data nature and source(s), and how was it processed/integrated
- Performance Metrics
  - Accuracy and test results across different processes and functions
- Limitations and Risks
  - Known failures, biases, and out-of-scope uses

Why Model Cards Matter for IG

- Risk & Compliance
  - Documents fitness for purpose and issues; creates audit trail for model selection decisions
- Records & Accountability
  - Defines data lineage; captures change history; identifies responsible parties; provides retention and disposition context
- Vendor management
  - Vendor transparency; will be key for tool diligence; indicates gaps/risk

Ongoing analysis

AI+IM GLOBAL SUMMIT

Ongoing Analysis / Continuous Monitoring

- Set up automated pipelines with alerts for data drift, schema violations, and quality drops post-ingestion.
- Combine rules-based checks with machine learning for predictive degradation detection, reviewing after each milestone.
- Maintain human oversight via dashboards showing KPIs like completeness and freshness.

Governance and Prevention

AI+IM GLOBAL SUMMIT

Build Governance and Prevention

- Enforce validation at the source (schemas, blocking bad data) and promote cross-team ownership with shared metrics.
- For enterprises, break silos using AI-driven mapping and harmonization across systems.
- Start small: focus on high-impact datasets for your pilots, then scale practices.

Exercise: Applying AI Governance

AI+IM GLOBAL SUMMIT

Exercise: Applying AI Governance

- You are given 100 potential points to allocate across resources for developing an AI Governance Program at your organization.
- Discuss and allocate the resources so that the sum equals 100 points. The points should be allocated by priority, not time or money
- Provide a brief explanation and rationale for your decisions.

AI Action plan

AI+IM GLOBAL SUMMIT

Initial step: Strategy, Readiness, Governance

- Establish AI Leadership and operating model
- Mapping and Data Posture
- Define AI vision, success matrix, and guardrails
- Run AI Readiness and data / infrastructure assessment
- Outline initial AI governance and policy considerations
- Identify and prioritize 3-5 high value pilot use cases
- Prepare people and skills

AI+IM GLOBAL SUMMIT

Key Deliverables

- Documented AI vision, success metrics, and prioritized pilot list.
- Initial AI governance framework and policies.
- Baseline measurements and a ready pilot team with training.

Pilot, Build, Integrate & Launch

- Technical design and environment set up
- Build and configure pilot solutions
- Internal testing and risk checks
- Soft launch to controlled user groups
- Measure usage

Key deliverables

- 2–3 AI pilots live with real users under governance.
- Dashboards and weekly review forums in place.
- First set of documented improvements and lessons learned.

Prove Value, Standardize, Plan Scale

- Deep-dive on pilot performance and ROI (Week 9–10)
- Decide scale-up, pivot, or stop for each pilot
- Institutionalize governance and operating practices
- Build the next-phase AI roadmap
- Scale change-management and communications

Key deliverables

- Measured ROI and qualitative impact story for each pilot.
- Formalized AI governance and operating model.
- Approved 6–12 month AI roadmap and scale-out plan.

Questions?

AI+IM GLOBAL SUMMIT

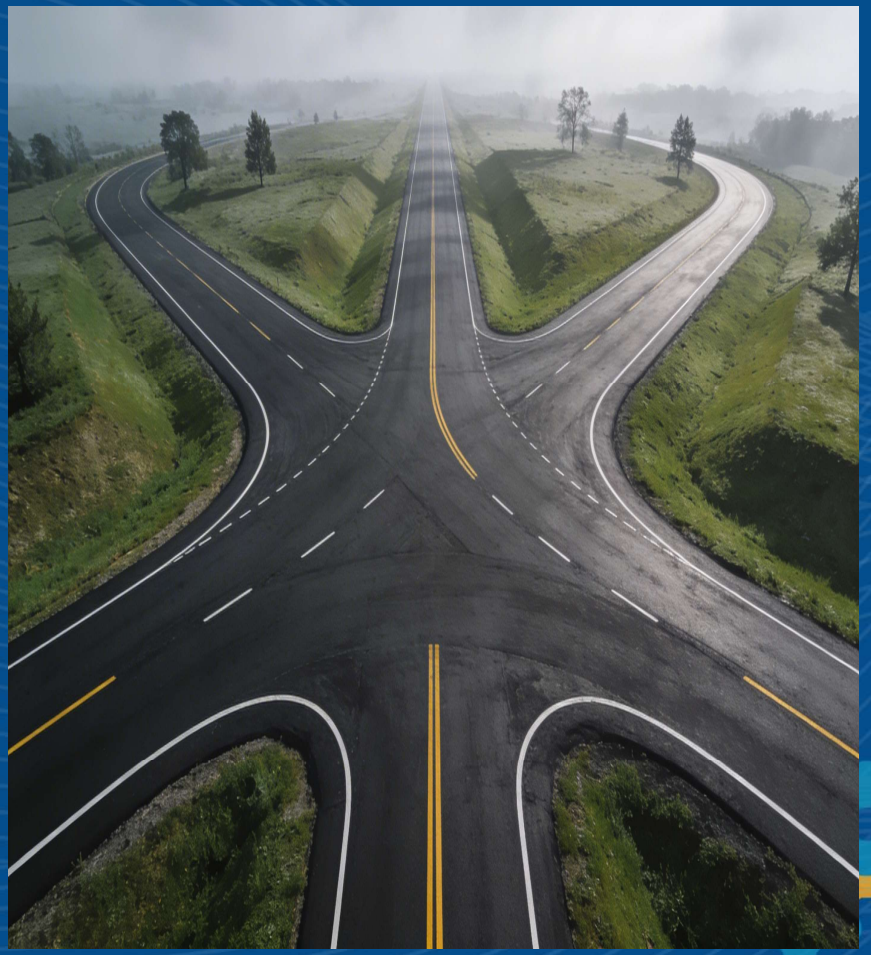
THANK YOU!

Susan Gleason, AIGP, CIP, CRM/CIGO, IGP

Doron Goldstein, AIGP, CIPM, CIPP/E, CIPP/US, FIP, PLS

AI+IM GLOBAL SUMMIT

Your competitive advantage in the modern enterprise lies in the crucial intersection of Trust, AI Governance and Scale



AI+IM GLOBAL SUMMIT