weaver

Assurance • Tax • Advisory

AI Vendor Management
A Continuous Journey

Presenters

Lulu Walker

CISA

GRC Senior Manager

Eric Peeters

CISA, CCSK

ISO 27001 Lead Auditor

GRC Senior Manager

Case Study: Business Impact of AI

Canadian Airline

- Airline required to implement chat bot instructions to a passenger
- Chat bot information was "reasonable"
- AI users should not be required to "double check" from another source

Online Education Vendor

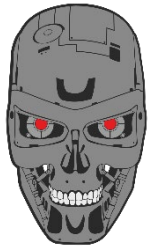
- Consent decree with EEOC over age and gender discrimination in contractors
- Vendor used AI to filter out certain ages without using date of birth
- AI-based discrimination applicable to independent contractors

Existing legal and regulatory framework applied to Artificial Intellignce

AI Deployment Models and AI Risks

Evaluation of AI

- Reactive AI
- Artificial Narrow Intelligence
- Generative AI
- Artificial General Intelligence
- Self-Aware AI

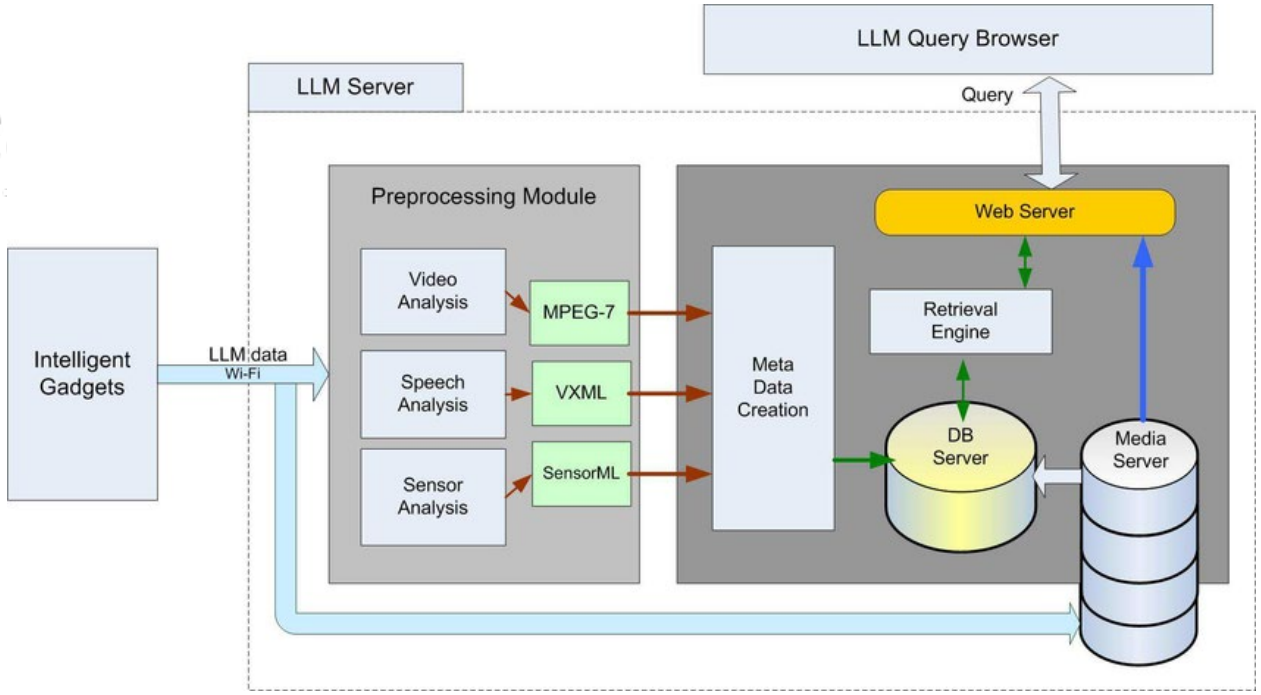


- ❑Data Security
- ❑Transparency
- ❑Data Manipulation
- ❑Bias and Discrimination
- ❑Prompt Engineering
- ❑Evasion Attack
- ❑Abuse Attack
- ❑Hallucination

AI Architecture

Components Of An AI Tool

- Complex supply chain
- Vendor on top of Large Language Model
- Suppliers of training data and source data
- Designer of system inputs
- Infrastructure provider



Source: Sang Chul Ahn, Korea Institute of Science and Technology

AI Risk Ownership

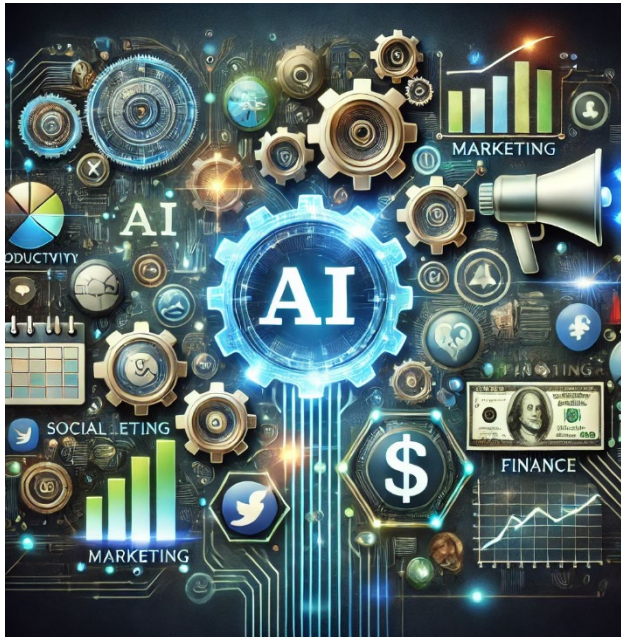
AI impacts every function

- Marketing
- Finance
- IT
- Customer Service
- Manufacturing
- Procurement

Risk posture is important

- Centralized vs decentralized management
- Proactive vs reactive
- Risk ownership vs risk acceptance

The owner of AI risk will define the AI governance and compliance posture



Your Governance Journey

Define the AI environment

- What policy do you have? Is it granular?
- How do you leverage AI today? The answer is not “we don’t”
- How do your vendors leverage AI? Focus on SaaS
- How does your competition use AI?

Legacy Risks in AI Era

Availability

DevSecOps

Data Quality

- Bad Data = Bad AI
- Data Cleaning, Imputation, Normalization, Archiving
- Master Data Management Program

The New Era – *T R U S T ! !*

Bias and Ethics

Hallucination

Prompt Engineering

Source Data Manipulation

The New Era – *RELIABILITY?*

Intellectual property rights

- Third-party training data
- Outputs

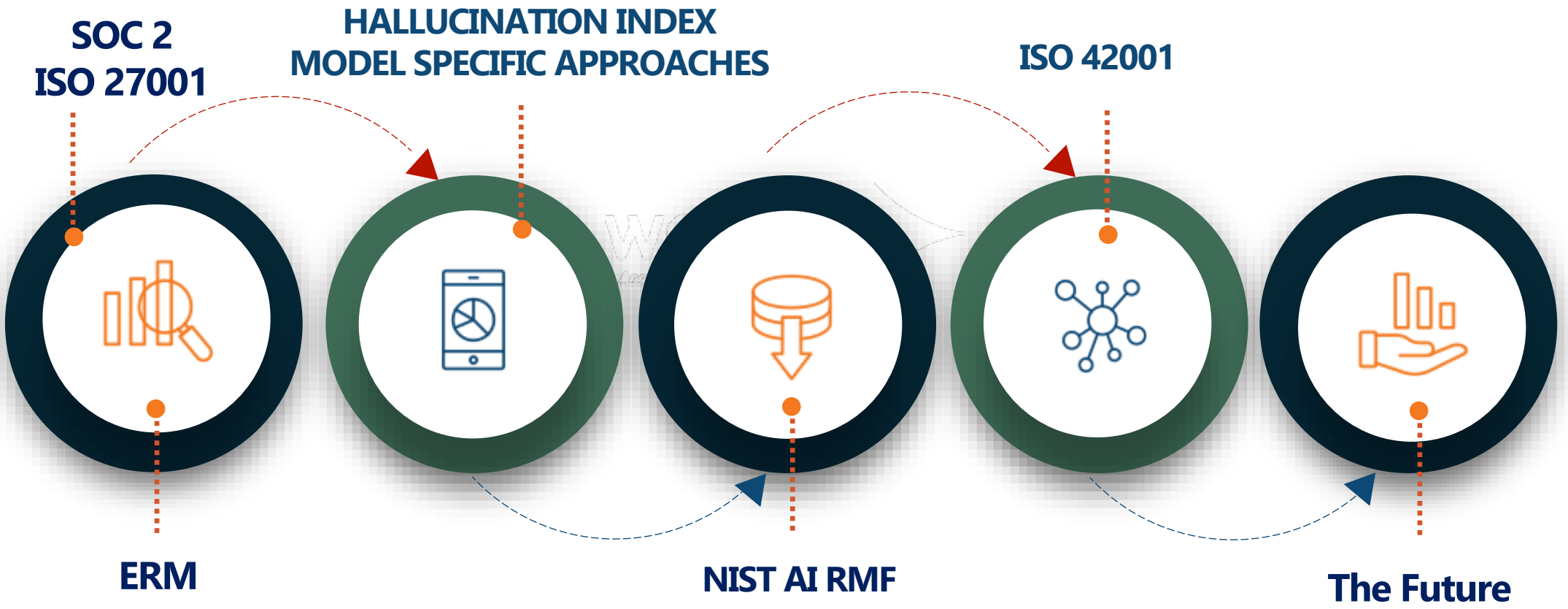
Fast-changing regulatory space

- State regulations
- Industry mandates

Dynamic vendor environment

- Loss of funding
- Change of trajectory

Plan an AI Governance Maturity Path



What Governance Framework?

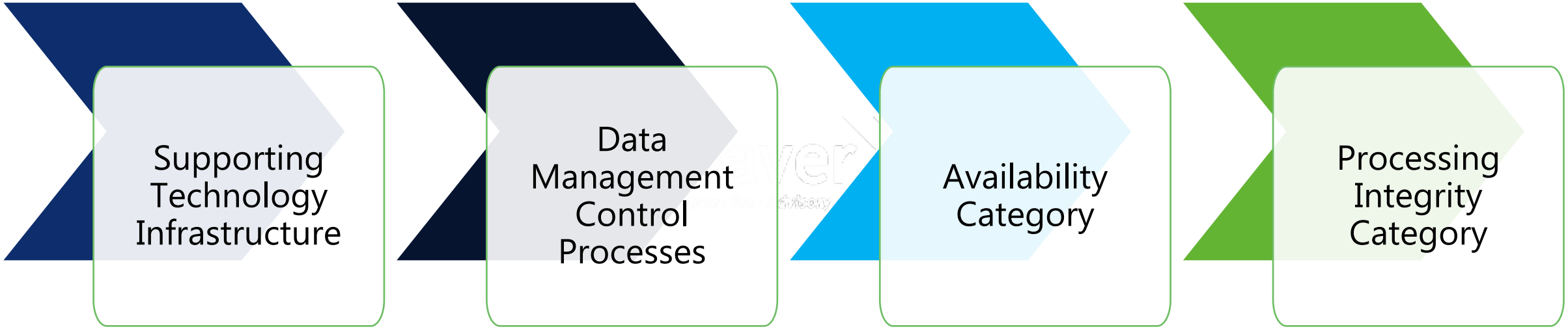
LACK OF AI FOCUS

- ISO 27001
- NIST 800-53
- CIS CSC 8
- COBIT 2019
- SOC 2

SLOW PACE OF CHANGE

- Years, if not decades, in between updates
- ISO: 2013 – 2022
- COBIT: 2012 – 2019
- Can existing frameworks be adapted
- Are new frameworks needed

Components in a SOC 2 for AI



Available in ISO 27001 and other frameworks

AI Tool Third Party Results Assessment Considerations

weaver
Assurance · Tax · Advisory

- Security & Compliance
- Data Management
- Bias and Fairness
- Security and Incident Response
- Governance and Accountability
- Continuous Improvement

If All You Have Is a SOC 2

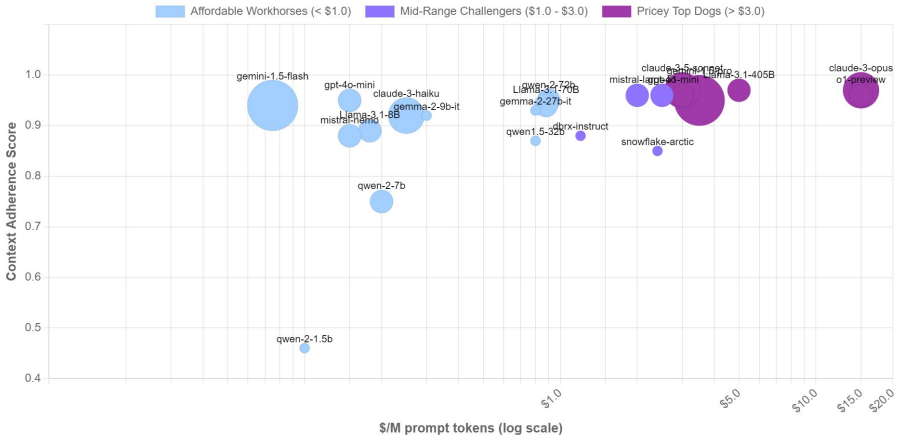
- Understand the Scope and Boundaries
- Define Your Expectations
- … Do the Controls Meet Them?
- Review the Test Procedures
- Inquiry vs Sampling
- Question the Absence of Availability and Processing Integrity

A SOC 2 with only Security tells you the AI dev environment is secure… maybe

Hallucination Index & Model Approaches

Hallucination Index by Galileo

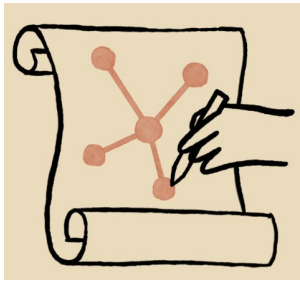
- Ranking and evaluation framework for hallucination
- 22 open and closed source models
- Focused on Retrieval-Augmented Generation (RAG)
- System prompts affect results
- Solutions built on open-source model can update weights

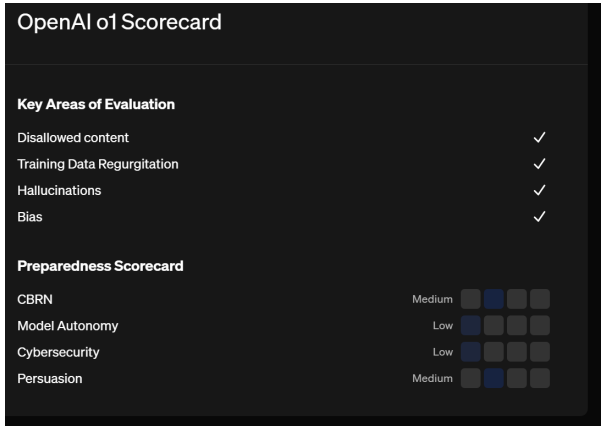


Model-Specific Approaches

- Limited visibility into methodology
- Self-review bias
- Detailed technical reports
- Not suited for comparison across LLMs
- Source of risks to be discussed with vendor

ANTHROP\C





From NIST AI RMF To ISO 42001

NIST AI Risk Management Framework

- Risk-based approach to assessing AI solutions
- Focus on developing and implementing "trustworthy" AI
- Collection of desirable outcomes across four functions: Govern, Map, Measure, Manage
- Playbook and Profile to support implementation

How does ISO 42001 enhance maturity versus NIST AI RMF

Greater consistency and predictability in the AI management practices implemented

Certifiable standard by an independent third-party

Controls set can be used as basis for Internal Audit over AI

Recognized practices vs "choose your own adventure" approach

ISO 42001 For an AI Management System

- 38 controls grouped in 10 control objectives
- Prescriptive control objectives and controls supported by extensive implementation guidance
- Strong ISO governance practices
- Focus on AI management, allocation of resources, AI impact, life cycle and data management

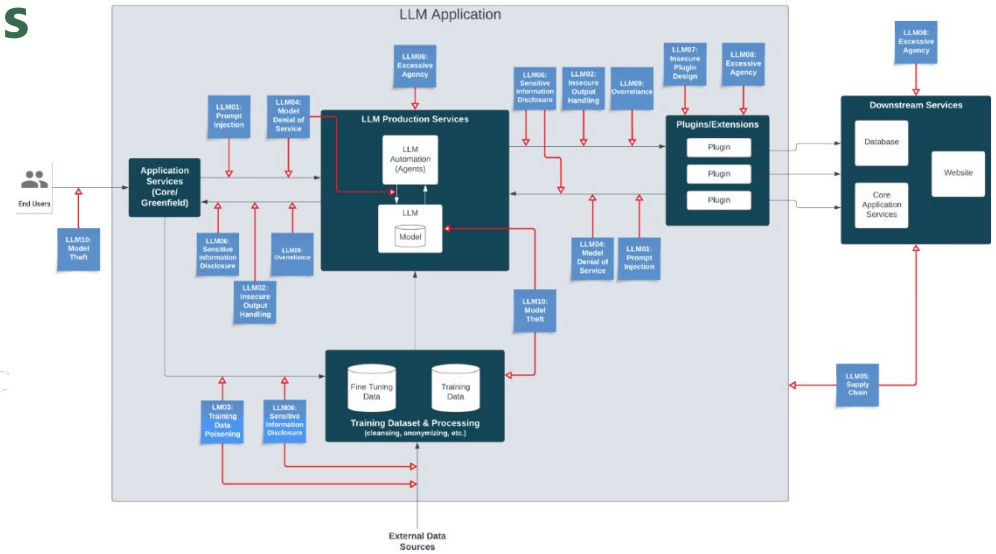
In Summary

You build		You Ask
AI-Aware ERM	1	**SOC 2 and/or ISO 27001**
A high-level review of the NIST AI RMF is a good start to an AI-aware ERM	2	**Hallucination Index** **Model-Specific Approaches**
NIST AI Risk Management Framework	3	
ISO 42001	4	**ISO 42001**

When There Is Nothing Else…

OWASP Top 10 for LLM Applications

- Industry-recognized source of threats
- Catalog of 10 most common threats against LLM
- Focus: Security risks to your AI environment



SIG Questionnaire

- Common alternative to third-party audits
- Mapping to multiple frameworks
- Focus: Substitute to a third-party attestation report

AI Model Risk Management Framework

- Risk identification and communication with internal and external stakeholders
- Flexible: for AI developers and users alike
- Focus: Custom AI risk assessment

Consider The AI Model Risk Management Framework To Mature Your AI-Aware ERM

Key Takeaways

1. Understand the Usage of AI at Your Organization
2. Identify The Owner of AI at Your Organization
3. Move Governance Forward Despite The Uncertainties
4. Evaluate the Reliance on Your Vendors

weaver

Assurance • Tax • Advisory

Lulu Walker

CISA

lulu.walker@weaver.com

Eric Peeters

CISA, CCSK, ISO 27001 Lead Auditor

eric.peeters@weaver.com