AI Governance: Aligning Organizational Policies with Global Standards

Presented by: *Faisal Shafiullah*



PECB U.S Regional Webinar

September 30th 2025

PECB REGIONAL WEBINARS

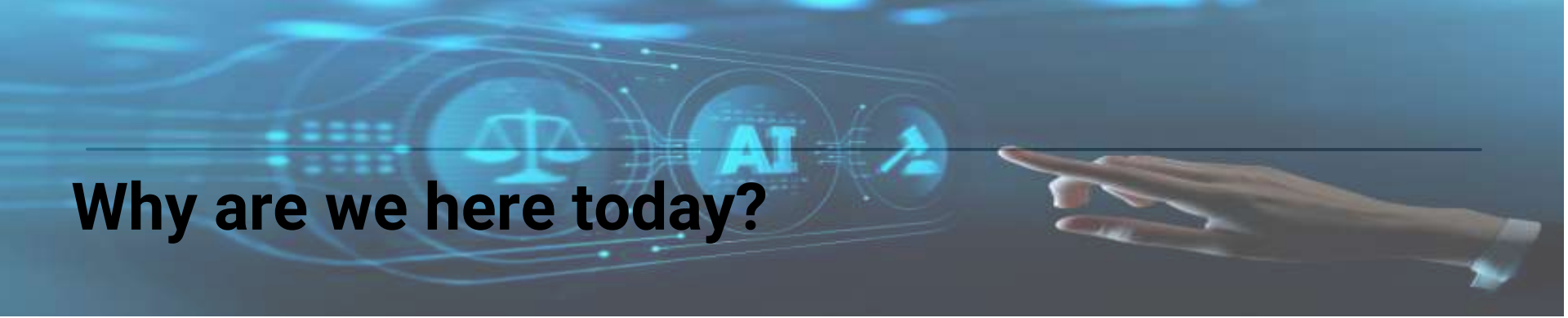


Faisal Shafiullah

Certifications: 🎓 (CISA), 🔐 (ISO/IEC 27001), (ISO/IEC 42001)

- Florida-based risk leader with 20+ years of experience in external audit, internal audit, and consulting.
- Trusted Advisor to global organizations in AI governance, risk, and compliance.
- Currently building in the AI space over the past ~3 years.
- PECB Training Partner: www.auditpartners.com/training

AuditPartners



Why are we here today?

- AI adoption is accelerating → trust and compliance risks are rising.
- Governance ensures responsible, ethical, and effective AI use.
- “AI without governance is innovation without accountability.”

What Is AI Governance?

- Framework of policies, roles, and controls ensuring AI systems are ethical, transparent, accountable, and compliant.
- Principles: Fairness, Transparency, Accountability, Security & Privacy, Reliability





AI Governance Model



Why AI Governance Matters ?

AI Governance aligns risk management with trust, compliance, and business value.

Risks Without AI Governance

- **Control failures** → **Bias and discrimination** (e.g., hiring, credit approvals).
- **Regulatory exposure** – Fines under EU AI Act, GDPR, and FTC enforcement.
- **Reputation risk** – Negative audit findings can damage public trust.
- **Audit gaps** – Lack of documentation, traceability, and accountability.
  - Applies to a service organization trying to maintain customer trust.

Benefits of AI Governance

Building Trust and Value Through AI Governance

- **Enhanced trust and assurance** – Stakeholders see transparent, governed AI use.
- **Innovation with controls** – Safe adoption backed by governance testing.
- **Smoother compliance audits** – Alignment with ISO/IEC 42001, NIST RMF, EU AI Act, OECD.
- **Competitive edge** – Organizations with AI governance reduce audit findings and gain market trust.

Global Standards Are the Guardrails

Global AI standards provide a benchmark auditors can align policies and controls against.



Key Frameworks



EU AI Act – Risk-based law



ISO/IEC 42001 – First certifiable AI governance system



NIST AI RMF – U.S. focused, globally referenced



OECD AI Principles – International policy baseline

ISO/IEC 42001- AI Management System



ISO/IEC 42001 – AI Management System

- First international standard for AI governance (published 2023).
- Requires **documented policies** (intent) and **technical controls** (enforcement).
- Applies to **any organization developing, deploying, or using AI**.

NIST AI Risk Management Framework (AI RMF)



NIST AI Risk Management Framework (AI RMF)

- US-centric but widely adopted globally.
- Four core functions auditors can test: **Govern, Map, Measure, Manage**.
- Applies to **public and private organizations** seeking risk-based governance.

EU AI Act (2025 forward)



- Risk-based law across the European Union.
- “High-risk AI” (e.g., in HR, healthcare, finance, public sector) requires compliance evidence.
- Applies to any company placing AI systems in the EU market, regardless of HQ location.

Audits ≠ Governance/Security

Audit Takeaway:

- ISO & NIST = **Structured control frameworks** auditors can test.
- EU AI Act = **Hard law** with penalties → auditors must verify compliance.
- OECD & Singapore = **Principles and best practices** → Auditors can benchmark policies.



Why AI Governance Now?

- **Explosive Adoption** – 77% of companies are experimenting with or deploying AI (PwC, 2024).
- **Shadow AI Risks** – Employees already using unapproved AI tools (data leakage, IP risk).
- **Regulatory Momentum** – EU AI Act, NIST AI RMF, ISO/IEC 42001, and FTC actions set global expectations.
- **High-Profile Failures** – IBM Watson, Amazon hiring AI, UK grading fiasco show the cost of poor governance.
- **Trust as a Differentiator** – Clients, investors, and regulators prefer organizations with transparent AI practices.
- **Audit Demand** – Boards and regulators are asking auditors to validate AI use just as they did for cybersecurity and SOX.

Risk Scenarios Without Governance

Real-World Examples:

- **Healthcare:** IBM Watson Oncology misdiagnosis.
- **Recruitment:** Amazon AI tool discriminated against women.
- **Finance:** Mortgage lenders sued for biased AI loan approvals.

Case Study 1

Healthcare: IBM Watson Oncology

• **Background:** IBM Watson for Oncology was marketed as a breakthrough AI to support cancer diagnosis and treatment recommendations.

• **Issue:** The system produced **unsafe or incorrect treatment advice** in multiple instances, due to being trained largely on **synthetic cases created by a small group of doctors**, not real-world patient data.

• **Impact:** Hospitals that trialed Watson reported **inaccurate recommendations**, reputational risk for IBM, and loss of trust in AI in healthcare.

• **Governance Gap:** No independent validation, limited auditability of training data, lack of documented bias/accuracy policies.

• **Audit Insight:** *Auditors would ask:* Where is the **evidence of model testing and validation**? Were clinical safety controls documented and enforced?

Case Study 2

Recruitment: Amazon AI Hiring Tool

• **Background:** Amazon developed an internal AI tool to screen job applications.

• **Issue:** The system **discriminated against women**, downgrading résumés that contained the word "women's" (e.g., "women's chess club captain").

• **Cause:** The AI was trained on 10 years of historical résumés — mostly from men, reflecting tech industry bias.

• **Impact:** Tool was scrapped in 2018, generating public criticism and reputational harm.

• **Governance Gap:** Lack of a **Bias & Fairness Policy**, no diversity controls in training data, no regular audits.

• **Audit Insight:** *Auditors would ask:* Did the organization conduct **bias testing**? Was there a documented policy requiring review of training data quality and representativeness?

⚙ Governance Pillars

- ✓ **Data Privacy and Protection** – GDPR, Clearview AI fined €20M.
- ✓ **Security and Resilience** – Adversarial AI examples in healthcare.
- ✓ **Bias and Fairness** – Hiring and lending lawsuits.
- ✓ **Transparency** – UK grading scandal created public outrage.
- ✓ **Accountability** – Regulators may hold boards personally liable.

Top 10 AI Governance Policies

Governance Policies (Intent / Paper)

1. AI Use Policy – Defines acceptable/unacceptable usage

2. Transparency and Disclosure Policy – Label AI-generated outputs

3. Bias and Fairness Policy – Mandate testing for discrimination

4. Data Privacy and Security Policy – Align with GDPR/HIPAA

5. Model Risk Management Policy – Lifecycle oversight

Technical Policies (Enforcement / Controls)

6. Third-Party and Vendor AI Policy – Enforce vendor due diligence

7. Incident Response & Escalation Policy – Log and escalate AI issues

8. Access and Usage Control Policy – Enforce RBAC, restrict high-risk AI tools

9. Employee Training and Awareness Policy – Mandatory training with attestations

10. Audit and Monitoring Policy – Continuous logging, DLP, automated monitoring

Operationalizing AI Governance

Where do we go from here….



Establish cross-functional governance committees

- Assess AI use cases and risks
- Establish charters



Embed AI risk into enterprise risk management

Map relevant standards



Implement AI policies across HR, IT, and Security, etc.



Lifecycle governance: design → deploy → monitor



Scale across enterprise

Challenges and Pitfalls



- Lack of executive buy-in



- Checkbox compliance



- Over-complication slows innovation

Protecting Against Deepfakes and Payment Fraud

Policies to consider….

- **Dual-factor authorization for high-risk AP payments.**
- **Biometric validation (voice or facial recognition) for executive approvals.**
- **Call-back verification for first-time vendor payments.**
- **Real case: 2019 European energy firm lost €200K in CEO voice deepfake scam.**

Preventing Data Leakage into AI Models

Policies to consider…

- **Use Intune + MDM to block copy/paste into ChatGPT or LLMs.**
- **Apply Conditional Access: restrict AI access to corporate-managed devices.**
- **Implement DLP to detect sensitive data before it leaves endpoints.**

⚙ Overlooked Organizational Controls

Policies to consider…

- **Third-party AI risk assessments:** Require vendors to disclose AI training data and controls.
- **Model access segmentation:** Enforce role-based access and limit data exposure.
- **Watermarking and logging:** Apply watermarks to AI outputs and centralize audit logs.

AI Policy/Controls

- **Clear AI use policies for employees (no client data uploads).**
- **Regular training on deepfake fraud and AI scam risks.**
- **Restrict AI bots in Slack/Teams unless formally sanctioned.**

? Q&A – Common Concerns

Where should we start? → Map current policies to AI risks.

Which framework first? → ISO/IEC 42001 globally, NIST in the U.S.

How do we balance compliance vs. innovation? → Address high-risk AI use cases with stronger controls, allow flexibility where risk is low.

Who should own AI governance?

- Cross-functional: IT/security, compliance, legal, and business units.
- Audit committees should oversee governance maturity just as they do with cyber risk.

Q&A Session



K.I.T – Keep in Touch





For any questions or comments you can contact us below:

- support@pecb.com