enterprise CONNECT

# AI Governance: Putting the Horse in Front of the Cart

Key Takeaways

The **Enterprise Connect** conference session on AI Governance, led by Melissa Swartz and Brian Harrison, addressed the critical need for organizations to develop robust AI governance frameworks. As AI tools become more integrated into daily operations, organizations face unique challenges regarding security, compliance, data privacy, and ethical considerations. The discussion emphasized proactive governance, cross-functional collaboration, and continuous policy updates to mitigate AI-related risks.

## Key Takeaways:

1. The Need for AI Governance
2. Cross-Functional AI Goverance Framework
3. Data Protection and Privacy Considerations
4. AI Tool Authorization and Monitoring
5. Employee Education and Change Management
6. AI in Customer Service and Business Opeations

## Session Panelists:

**Melissa Swartz**
Independent Consultant, Global Tech

**Brian Harrison**
Chief Technology Officer, Broward College

## The Need for AI Governance

AI adoption is growing at an unprecedented rate across industries, often outpacing the development of proper oversight mechanisms. This rapid integration of AI technologies into various processes has created a complex landscape where traditional governance models struggle to keep up. Employees at all levels of organizations are increasingly turning to AI tools such as ChatGPT and other large language models for a wide range of tasks. While these tools offer significant productivity gains, they also raise serious concerns about the potential exposure of sensitive information and the ethical implications of AI-driven decision-making.

As organizations grapple with these new challenges, it's becoming increasingly clear that AI governance must be approached differently from traditional IT governance.

The unique characteristics of AI technologies demand a more nuanced, flexible, and proactive governance framework that can account for several critical factors:

- **Speed:** AI processes enterprise data in real-time, requiring immediate governance mechanisms.
- **Scale:** A single AI prompt can expose vast amounts of sensitive information.
- **Invisible Risks:** AI-powered applications integrate into standard tools, making data leaks harder to detect.
- **Integration Challenges:** AI is becoming a built-in feature of everyday business tools, complicating governance efforts.

## Cross-Functional AI Governance Framework

A robust AI governance model requires representation from multiple disciplines within an organization to effectively address the complex challenges posed by artificial intelligence adoption. As AI technologies become increasingly integrated into various business processes, it's crucial to establish a comprehensive framework that considers technical, ethical, legal, and operational aspects of AI implementation. The solution; creating an AI Governance Council as a central body to oversee and guide AI initiatives across the organization. This council would bring together diverse expertise and perspectives to ensure a holistic approach to AI governance. By incorporating key roles from different departments, the council can effectively balance innovation with risk management, compliance, and ethical considerations. The proposed **AI Governance Council** includes key roles such as:

- **Chief Information Officer (CIO):** Provides technical oversight.
- **Chief Information Security Officer (CISO):** Ensures security compliance.
- **Legal & Compliance Teams:** Address regulatory requirements.
- **Privacy Officers:** Safeguard personal and corporate data.
- **Business Unit Leaders:** Validate AI use cases.
- **Human Resources (HR):** Manage employment policies regarding AI usage.


**Building Your AI Governance Program**
The Three Pillar Approach

**This structure ensures AI governance is a shared responsibility, reducing risks and aligning AI initiatives with company policies.**

## Data Protection and Privacy Considerations

Data classification is a fundamental aspect of AI governance, serving as the cornerstone for protecting sensitive information and ensuring compliance with privacy regulations in the age of artificial intelligence. As organizations increasingly leverage AI technologies to process and analyze vast amounts of data, the need for a structured approach to data handling becomes paramount.

Implement a comprehensive **Data Classification Framework** designed to guide AI interactions with organizational data, addressing the complex interplay between data sensitivity and AI capabilities. This framework not only helps organizations safeguard their most critical information assets but also enables them to harness the power of AI responsibly and effectively. By categorizing data based on its sensitivity and potential impact, organizations can implement appropriate controls and protocols for AI systems, balancing innovation with risk management.

The proposed Data Classification Framework encompasses several tiers, each with specific guidelines for AI interaction:

1. **Public Data:** Safe for AI experimentation and public-facing use.
2. **Internal Data:** Requires vetted AI tools with proper security protocols.
3. **Sensitive Data:** Restricted AI usage with monitored access.
4. **Critical Data:** No AI exposure allowed due to high security risks.

### Challenges

- Employees unknowingly expose confidential data by using AI tools without proper safeguards.
- Organizations lack clear policies on AI tool selection and compliance.

### Recommendations

- Develop an internal AI App Store with pre-approved AI tools vetted for security, compliance, and integration capabilities.
- Implement Data Loss Prevention (DLP) systems to monitor and restrict AI interactions with sensitive data.
- Educate employees on responsible AI usage and classification guidelines.

## AI Tool Authorization and Monitoring

AI governance requires a comprehensive approach that combines robust technical controls with diligent human oversight to ensure compliance and mitigate risks associated with AI adoption. As organizations increasingly integrate AI tools into their operations, the need for a structured framework to evaluate, authorize, and monitor these tools becomes paramount.

The AI Tool Authorization Framework is a systematic approach designed to assess AI tools based on critical factors that impact security, transparency, and ethical considerations. This framework serves as a crucial component of a broader AI governance strategy, enabling organizations to make informed decisions about which AI tools to adopt and how to implement them responsibly. By establishing clear criteria for AI tool evaluation, companies can better manage the potential risks associated with AI usage while harnessing its transformative potential.

The **AI Tool Authorization Framework** evaluates AI tools based on several key factors:

- SOC 2 Compliance
- Audit Logging Capabilities
- Single Sign-On (SSO) Integration
- Transparency & Explainability
- Bias and Fairness Considerations

Monitoring AI usage across the organization is equally critical.

### Key recommendations include:

- Deploying **AI activity scanners** to detect unauthorized AI usage.
- Using **automated classification tools** to track AI-generated data.
- Establishing an **AI Incident Response Plan** to address policy violations swiftly.

## Employee Education and Change Management

Employee awareness is a major challenge in AI governance, emphasizing the critical role of workforce education in successfully implementing and maintaining effective AI policies. As artificial intelligence becomes increasingly integrated into various business processes, organizations face the complex task of ensuring that all employees, from entry-level staff to senior management, understand the implications, risks, and responsibilities associated with AI usage in the workplace. This awareness gap not only poses potential security and compliance risks but also hinders the full realization of AI's benefits across the organization.

### Employees must be educated on:

- **How to differentiate** between legitimate AI tools and misleading applications.
- The risks of **inputting proprietary or personal data** into AI models.
- The organization's AI governance policies and acceptable **use guidelines**.

### Proposed initiatives include:

- AI awareness workshops and interactive training programs.
- Mandatory compliance courses for employees handling sensitive data.
- AI governance updates communicated regularly through internal channels.

## AI in Customer Service and Business Operations

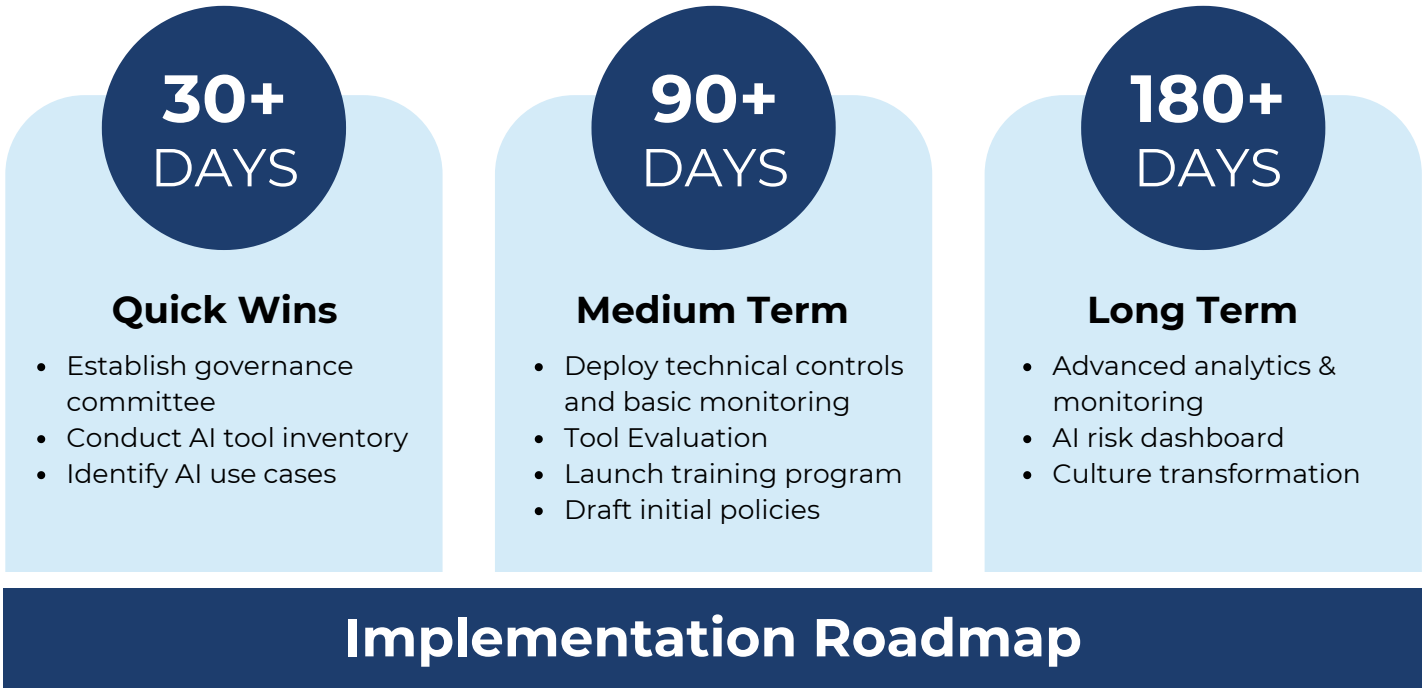
AI's growing role in customer service and enterprise applications emphasizes the need for organizations to adapt and evolve their strategies in response to the rapid advancement of artificial intelligence technologies. As AI continues to transform various aspects of business operations, companies must carefully consider the implications of its implementation, particularly in customer-facing roles and internal processes.

It is important to balancing the potential benefits of AI, such as improved efficiency and enhanced customer experiences, with the associated risks, including data security and privacy concerns. Organizations are now faced with the challenge of developing comprehensive strategies that leverage AI's capabilities while maintaining control over sensitive information and ensuring ethical use of the technology and emphasizing the need to:

- Adopt **internal AI models** instead of third-party generative AI for handling customer interactions.
- Use AI to **summarize meetings and process business intelligence**, ensuring efficiency without data exposure risks.
- Continuously refine AI policies as technology and business needs evolve.

## Actionable Next Steps for Organizations

- **Review & Update AI Policies:**
  Ensure current data protection policies explicitly address AI risks.
- **Establish an AI Governance Committee:**
  Form a cross-functional team to oversee AI implementation.
- **Implement a Secure AI Tool Framework:**
  Develop an internal AI App Store with authorized tools.
- **Launch AI Education & Training:**
  Train employees on AI ethics, security risks, and best practices.
- **Monitor AI Usage:**
  Deploy tools that track and analyze AI interactions within the organization.
- **Develop an AI Incident Response Plan:**
  Prepare for potential AI-related policy violations.




**Implementation Roadmap**

## Conclusion

AI governance is not an afterthought—it must be proactive, structured, and continuously evolving. Organizations must prioritize AI governance now to prevent security breaches, regulatory violations, and ethical dilemmas. By implementing cross-functional policies, data protection strategies, and ongoing monitoring, businesses can harness AI's power while maintaining control and compliance.

# Thank you for reading.

For more resources like this, visit our **Knowledge Hub.**

enterprise CONNECT