Deloitte.

Together makes progress

Trusted & Secure AI (TSAI)

AI Program Risk Management

Accelerate and enhance AI deployments with effective governance and risk management

Deloitte's Trusted and Secure AI framework for Program Risk Management is designed to empower organizations to adopt and scale impactful AI programs. TSAI allows organizations to embrace AI with confidence, lending guidance, practical tools, and the knowledge needed to establish robust governance, manage risks, and meet evolving regulatory demands. By supporting secure and responsible use across an AI program, we help organizations unlock AI's promise while mitigating costly risks.

Process and standards
Collate the internal and external policies and guidelines, layer the dimensions of Deloitte's Trustworthy AI® framework, and package the processes and requirements for AI use by partner teams. Plan for ongoing refinement as regulations, technology, and organizational needs evolve.

Platform engineering
Configure and operationalize an AI governance platform, translating requirements into workflows, questionnaires, controls, dashboards, and integrations that support compliance at every life cycle stage. Continuously update performance, risk, and bias metrics to provide consistent reporting and clear guidance.

Solutions enablement
Develop an intake framework for discovery, evaluation, and approval of use cases, standardizing processes and evaluation criteria. Work with other governance ecosystem teams to support compliance and operationalize the intake framework in a tech-enabled solution.

Cybersecurity
Embed and continuously operate scalable, proactive protections, including zero trust access controls, monitoring/SIEM-driven response, code and data-flow risk reviews, role-based training, and AI-assisted red teaming for compliant, resilient, and reliable security as threats and AI use cases evolve.

Operations and monitoring
Collaborate with functional teams to embed AI governance practices into the organization's day-to-day operations, including through the establishment of phase gate checkpoints, development of KPIs and KRIs for executive review dashboards, and enablement of continuous monitoring with a tech-enabled solution.

Training
Design and deliver end-to-end, role-based training and change management, covering policies, processes, tools, workflows, and AI literacy. Reinforce learning and compliance with ongoing communication, and help organizations embody robust AI governance through daily habits, organizational norms, and operating rhythms.

With TSAI, promote innovation, drive accountability, and foster public trust for our clients.

Transparent AI governance. **Essential for safe and responsible innovation.**

AI Program Risk Management provides a structure within which AI may be developed, deployed, and managed responsibly and effectively. By tackling program risk management, organizations can accelerate implementation, drive strategic innovation, and reduce costs by executing effectively from the start.

Current-state assessment

Assess the AI and governance landscape

Aggregate a comprehensive understanding of the policies and regulations that shape the organization's approach to AI and evaluate the organization's existing approach, including the expertise, processes, and technologies currently deployed or planned. Identify gaps, bottlenecks, and opportunities for refinement, integration, and automation, which inform Deloitte's targeted Current-state assessment.

Value: Clear, actionable insights and identified opportunities, enabling your organization to confidently advance AI capabilities by understanding the current state, compliance requirements, and any limitations.

AI vision & strategy

Establish an AI vision & strategy

Leverage an AI Lab to define the organization's vision for AI use, anchoring the vision to the organization's stated mission. Consider the resources and activities needed to realize the stated AI vision, and develop a corresponding value framework that will be used to prioritize AI use cases.

Value: A well-defined and mission-aligned AI vision and value framework, developed through stakeholder consensus and an outcomes-based approach..

Construct a comprehensive roadmap

Using the gaps and opportunities revealed through the Current-state assessment and the AI Lab, organize a roadmap that charts the course from the current state to the desired future state for AI use across people, processes, and technology. Include plans for data classification, identification of appropriate hyperscaler platforms and needed technologies, necessary dashboards, reporting requirements, cybersecurity upgrades, training needs, and other elements to enable regulatory compliance.

Value: A grounded and organized set of steps to advance the organization's achievement of its AI vision and support compliance.

People and process enablement

Design and refine an intake framework

Using existing governance mechanisms and applicable regulations, construct an inventory and intake framework by which to evaluate, review, and monitor AI use cases. Refine the framework using stakeholder feedback and on-the-ground constraints and realities.

Value: An adaptable, stakeholder-informed intake framework that allows for risk management and regulatory compliance through the definition of processes, organizational risk tolerance, and by assigning roles and responsibilities.

Technology enablement

Operationalize AI governance

Evaluate potential AI governance technology platforms, considering organizational needs like scalable operations and monitoring, organizational priorities, constraints, and apparent trade-offs. Assess the configuration burden and available expertise.

Value: Selection of the most effective AI governance technology, optimizing resources and delivering a tailored fit for the organization's unique needs.

Tech-enabled AI governance

Implement an AI governance platform to automate, streamline, and enhance GRC processes, improving efficiency, increasing transparency, and enabling real-time monitoring and reporting. Reduce time and complication within the AI development lifecycle by codifying risks, controls, assessments, and existing processes for automation enablement.

Value: Accelerated AI adoption while promoting robust governance and empowering your organization with efficient, transparent, and continuously monitored AI operations.

Get in touch

Joe Conti
Trusted & Secure AI Leader
Deloitte & Touche LLP
joconti@deloitte.com

Anthony Fratta
Trusted & Secure AI Leader
Deloitte & Touche LLP
afratta@deloitte.com

Copyright © 2026 Deloitte Development LLC. All rights reserved.