

AI GOVERNANCE 360™

Govern AI responsibly. Enable innovation. Manage emerging technology risk.

EXECUTIVE SOLUTION OVERVIEW

AI Governance 360™ is a structured advisory solution for organizations adopting or scaling artificial intelligence. It establishes the governance, risk, security, privacy, accountability and oversight mechanisms needed to use AI responsibly while supporting business innovation.

AI	RISK	GOVERN	INNOVATE
Use-case visibility	Risk-based controls	Accountability	Business enablement

THE BUSINESS CHALLENGE

- Organizations are rapidly adopting generative AI, machine learning and AI-enabled software, often faster than their governance processes evolve.
- Without a defined governance model, organizations can face unmanaged AI risk across data protection, privacy, cybersecurity, intellectual property, model behavior, third-party providers, regulatory obligations and accountability.
- AI Governance 360™ provides an executive-to-operational framework for identifying AI use cases, assessing risk, establishing controls and embedding responsible oversight into the AI lifecycle.

WHAT AI GOVERNANCE 360™ DELIVERS

CAPABILITY	WHAT IT COVERS
AI Inventory & Use-Case Governance	Identify AI systems and use cases, ownership, business purpose and lifecycle status.
AI Risk Management	Classify and prioritize AI risks using a practical risk-based methodology.
AI Governance Framework	Define roles, responsibilities, decision rights, escalation and oversight.
AI Policies & Standards	Develop organization-specific AI policies, standards and operating procedures.
AI Security & Privacy	Integrate cybersecurity, privacy, data protection and secure-AI considerations.
Third-Party AI Risk	Assess vendors, models, platforms, data handling and contractual governance requirements.
Human Oversight	Define approval, human-in-the-loop, accountability and exception processes.
Monitoring & Assurance	Establish metrics, monitoring, evidence, review and continuous-improvement mechanisms.

AI GOVERNANCE 360™ — SERVICE PACKAGES

1. AI Governance QuickScan™	1-2 weeks
Rapid executive baseline for organizations that need to understand their current AI governance exposure.	KEY OUTPUTS • AI inventory discovery • Governance maturity review • Risk and gap scan • Executive readiness score • Priority recommendations • 90-day action plan
2. AI Governance Assessment™	3-5 weeks
Comprehensive assessment of AI governance, risk, security, privacy and operating practices.	KEY OUTPUTS • AI use-case inventory • Risk classification • Governance maturity assessment • Policy/control gap analysis • Third-party AI risk review • AI risk register • Prioritized roadmap
3. Responsible AI Framework™	6-12 weeks
Design and establish the governance foundation required for responsible enterprise AI.	KEY OUTPUTS • AI governance framework • AI policy suite • Risk classification model • Approval workflow • AI control framework • Roles and accountability • Monitoring framework • Governance roadmap
4. AI Governance Advisory™	Ongoing
Recurring advisory support for organizations that need continuing AI governance leadership.	KEY OUTPUTS • AI use-case reviews • AI risk assessments • Policy updates • Vendor reviews • Governance committee support • Executive briefings • Regulatory monitoring • AI incident advisory

AI GOVERNANCE LIFECYCLE

INVENTORY	CLASSIFY	ASSESS	GOVERN	CONTROL	MONITOR	IMPROVE
-----------	----------	--------	--------	---------	---------	---------

REFERENCE FRAMEWORK ALIGNMENT

CISOG can tailor AI Governance 360™ to the client's regulatory, industry and risk environment. Depending on scope, alignment may include the NIST AI Risk Management Framework (AI RMF), ISO/IEC 42001, ISO/IEC 27001, ISO/IEC 27701, NIST Cybersecurity Framework, privacy requirements and applicable industry or organizational policies.

KEY DELIVERABLES

- AI Governance Charter and Operating Model
- AI System / Use-Case Inventory
- AI Risk Classification & Assessment Methodology
- AI Risk Register
- AI Governance Policy and Standards
- AI Approval and Exception Management Process
- AI Security & Privacy Control Framework
- Third-Party AI Risk Assessment Model
- Human Oversight and Accountability Model
- AI Governance Metrics, KPIs and KRIs
- AI Governance Roadmap

WHO AI GOVERNANCE 360™ IS FOR

- CEOs & Boards: Need confidence that AI adoption is aligned with business strategy and risk appetite.
- CIOs / CTOs / CISOs: Need a practical governance model for AI-enabled technology and security risk.
- Chief AI / Data Leaders: Need repeatable controls for scaling AI use cases responsibly.
- Legal, Privacy & Compliance: Need traceability, accountability and evidence for AI-related obligations.
- Risk & Internal Audit: Need a defensible framework for identifying, assessing and monitoring AI risk.
- Business Units: Need a clear pathway to approve and deploy valuable AI use cases without creating unmanaged risk.

BUSINESS OUTCOMES

Visibility	Know what AI is being used, where and by whom.
Risk Reduction	Identify and prioritize AI-related risks before they become incidents.
Accountability	Establish clear ownership and decision rights.
Responsible Innovation	Enable business teams to adopt AI within defined guardrails.
Security & Privacy	Integrate AI governance with existing cybersecurity and data-protection practices.
Executive Confidence	Provide leadership with measurable governance and risk information.

OPTIONAL SPECIALIST MODULES

- AI Use-Case Risk Review™ — targeted assessment before deployment of a specific AI application.
- AI Vendor Risk Review™ — governance and risk review of third-party AI platforms and providers.
- AI Policy Accelerator™ — accelerated development of AI acceptable-use and governance policies.
- AI Board Briefing™ — executive briefing on AI opportunity, risk, governance and investment priorities.
- AI Governance Workshop™ — facilitated leadership workshop resulting in a practical AI governance action plan.

WHY CISOG

CISOG Technology Consults LLC combines cybersecurity, GRC, technology governance, digital transformation and AI governance perspectives. This integrated approach helps organizations avoid treating AI governance as an isolated compliance exercise and instead connect it to enterprise risk, security, technology strategy and business outcomes.

ENGAGEMENT MODEL

PHASE	ACTIVITY	PRIMARY OUTPUT
Discover	Stakeholder engagement and AI landscape discovery	AI landscape baseline
Assess	Maturity, risk, controls and gap assessment	AI governance assessment
Design	Framework, policies, controls and operating model	Responsible AI framework
Enable	Training, workflows and implementation support	Operational governance
Sustain	Monitoring, advisory and continuous improvement	Ongoing assurance

READY TO GOVERN AI WITH CONFIDENCE?

Schedule an AI Governance 360™ consultation with CISOG Technology
Consults LLC.

CISOG Technology Consults LLC | A Cisog Group company | Product: AI Governance 360™ | Datasheet