[Service Brief]

AI Governance & Controls Advisory

Bring Visibility, Accountability, and Defensibility to Enterprise AI Use

OVERVIEW

AI is moving faster than the governance around it. Most organizations can identify where AI is being used. However, few can say who owns it, what controls exist, or how they would defend its use under scrutiny. As AI adoption expands across business workflows, products, operations, and third-party platforms, organizations carry exposure they cannot fully see or account for. This raises the likelihood of security incidents, financial loss, intellectual property leaks, and regulatory scrutiny.

SDG's AI Governance & Controls Advisory gives organizations the visibility, structure, and controls framework required to scale AI safely and defensibly.

Why This Matters Now

The business mandate is to rapidly adopt AI, but regulatory requirements demand a controlled deployment.

In many organizations, leadership is no longer asking whether AI exists in the environment. The harder question is whether AI use is visible, governed, owned, and supportable when scrutiny arrives.

Many leadership teams are unable to clearly answer core questions, including:

- **Where is AI being used?**
- **Who owns AI decisions, risks, and outcomes?**
- **What controls, evidence, and documentation exist?**
- **Can we defend our AI use to audit, customers, regulators, or the board?**

CHALLENGES

The processes required to understand, govern, and oversee AI use are often fragmented, inconsistent, and still evolving.

In many organizations, AI is implemented faster than governance processes, control ownership, and oversight mechanisms can keep pace. This leaves leadership with limited visibility into current AI use, unclear accountability, and a growing burden to demonstrate that AI-related decisions are governed responsibly.

1. **Limited Visibility**

   AI spreads across workflows, products, and third-party platforms faster than the enterprise can track where it is in use and what it impacts.

2. **Fragmented Ownership**

   AI decisions, risks, and controls lack defined accountability and expectations across business, security, privacy, legal, data, and technology teams.

3. **Control Gaps**

   Security, privacy, documentation, and oversight controls are either undefined or not connected to the governance and technical mitigations required to manage AI risk.

4. **Defensibility Gaps**

   Scrutiny from audit, customers, regulators, legal, and the board increases faster than the documentation and evidence needed to support AI use.

5. **Third-Party AI Exposure**

   Third-party products silently embedding AI expand enterprise risk without effective oversight.

SOLUTION

SDG's AI Governance & Controls Advisory exposes AI's enterprise impact while adhering to AI governance frameworks and standards, such as NIST AI RMF, the EU AI Act, and ISO 42001.

AI Governance Advisory Process:

1. **AI Use Case Discovery & Stakeholder Alignment**

   Structured reviews identify current initiatives, stakeholders, third-party dependencies, and oversight expectations across the enterprise.

2. **Ownership & Accountability Mapping**

   Responsibility for decisions, risks, controls, documentation, and outcomes is mapped across business and support functions.

3. **Governance & Control Readiness Assessment**

   Current-state reviews evaluate governance, privacy, security, documentation, oversight, and evidence readiness across in-scope initiatives.

4. **Gap Identification & Exposure Analysis**

   Reviews highlight material weaknesses across policy alignment, control design, evidence, oversight, and third-party exposure.

5. **Risk-Based Prioritization**

   Findings are ranked based on business impact, governance risk, and likelihood of material exposure.

6. **Actionable Roadmap Development**

   Prioritized actions, sequencing, and ownership define the path to stronger governance, defensibility, and ongoing oversight.

KEY BENEFITS
What clients gain from the engagement

A clear picture of readiness and a defensible path forward.

1. **Greater Visibility & Control**

   Provides oversight of where AI is in use, who owns it, and where governance is weakest.

2. **Faster, Better Decisions**

   Enables quicker decisions on where AI can move forward and where added controls, remediation, or restriction are required.

3. **Stronger Defensibility**

   Strengthens evidence, documentation, and governance alignment needed to respond to scrutiny with confidence.

4. **Reduced Exposure**

   Identifies governance and control weaknesses before they lead to security incidents, financial loss, intellectual property leakage, or regulatory impact.

5. **Improved Coordination**

   Brings business and control stakeholders into better alignment around ownership, oversight, and decision-making.

6. **Clear Roadmap**

   Provides a prioritized path to secure current AI use cases, close material gaps, and reduce risk in future deployments.

DIFFERENTIATORS
What makes SDG's approach different

SDG connects AI controls to the exposure they are meant to address, the governance actions required to close gaps, and the technical mitigations that reduce real risk.

1. **Practitioner-Led Advisory**

   Led by experienced security, privacy, governance, and risk practitioners who understand how to identify exposure and define practical mitigations.

2. **Operating Model Focus**

   Evaluates how accountability, controls, oversight, and evidence hold up in practice — not just whether policies or frameworks exist.

3. **Risk-to-Mitigation Lens**

   Connects governance and control gaps to the exposures they create, and the actions needed to reduce them.

4. **Defensibility by Design**

   Focuses on the documentation, traceability, and evidence needed to support audit, legal, customer, regulatory, and board scrutiny.

5. **Enterprise-Wide View**

   Addresses internal and third-party AI risk through a single governance lens.

6. **Board Impact**

   Translates technical risk into business exposure, delivering executive-ready metrics that support prioritization and budget decisions.

WHAT SDG DELIVERS | AI VISIBILITY, GOVERNANCE, AND SECURITY

SDG helps clients see AI, govern AI, and secure AI — with identity at the core.

01 VISIBILITY

Know Every AI Agent and its Access

Inventory sanctioned and shadow AI across agents, copilots, models, identities, data, and connected systems.

Client Value: A prioritized baseline for ownership, risk reduction, and faster decisions.

02 GOVERNANCE

Assign Ownership and Enforce Control

Define policy, decision rights, lifecycle governance, and least-privilege access aligned to NIST AI RMF, EU AI Act, and ISO 42001.

Client Value: An audit-ready AI operating model leadership can scale with confidence.

03 SECURITY

Protect AI from Misuse and Attack

Assess, adversarial test, and continuously monitor AI across prompts, agents, models, tools, and human interaction points.

Client Value: Reduced exposure to prompt abuse, deepfakes, agent misuse, and control drift.

ABOUT US

With more than 30 years of experience partnering with global enterprises on complex business and IT initiatives, SDG is a trusted provider of advisory, transformation, and managed services. The firm empowers organizations to strengthen cyber resilience by integrating AI into identity, threat, and risk management solutions that protect digital assets and deliver measurable business value. Learn more at www.sdgc.com.

SDG

75 North Water Street
Norwalk, CT 06854
203.866.8886
sdgc.com

Contact Us: solutions@sdgc.com