AI Governance Best Practices Checklist

First and Foremost...

- [ ] Secure executive buy-in to drive adoption and accountability from the outset to set your path for success

Organizational and Policy Foundations

- [ ] Define and document appropriate and inappropriate AI use in annual policies
- [ ] Assign clear accountability and ownership for AI decisions and outcomes
- [ ] Align governance with frameworks (NIST, AI RMF, ISO/IEC 42001, Microsoft Responsible AI, EU AI Act)
- [ ] Form a cross-functional committee (IT, security, compliance, legal, business leaders) that provides a representation from across your organization

Inventory and Monitoring

- [ ] Maintain a complete inventory of all AI tools, platforms, and agents, including “shadow AI” use
- [ ] Use tools (Microsoft Purview, Defender for Cloud Apps, endpoint monitoring) to detect and manage AI activity

Data Discovery, Classification, and Protection

- [ ] Discover where sensitive, regulated, or business-critical data resides (cloud, endpoints, legacy systems)
- [ ] Classify and label data (PII, PHI, IP, financial, HR, customer-sensitive, etc.) using automated tools
- [ ] Apply sensitivity labels, DLP, and encryption to control AI access and sharing

Exposure Based Controls

- [ ] Move beyond static, file-centric protections to exposure-based, context-aware policies
- [ ] Monitor both inputs (prompts) and outputs (responses) of AI systems for sensitive content
- [ ] Use DSPM for AI to map data flows, apply guardrails, and enforce real-time controls

www.avertium.com

AVERTIUM

marketing@avertium.com

Transparency, Explainability, and Auditability

- [ ] Maintain audit trails for all AI interactions (who, what, when, why) and restrict access to these audit trails
- [ ] Require AI models and agents to provide explanations for outputs in high-stakes scenarios
- [ ] Use Microsoft Purview and similar tools for audit and compliance reviews

Ethical, Fair, and Responsible AI

- [ ] Conduct regular ethical impact assessments and bias testing for AI model responsibilities
- [ ] Provide practical tools and training for development teams on responsible AI principles
- [ ] Integrate “ethical by design” practices into the AI lifecycle

Continuous Monitoring and Improvement

- [ ] Continuously monitor AI usage, data flows, and policy effectiveness
- [ ] Use risk scoring, anomaly detection, and real-time alerts to identify and respond to threats
- [ ] Iterate and improve governance controls as technology and business needs evolve

Technical Enablement

- [ ] Ensure secure configuration and deployment of AI tools (Copilot, Security Copilot, ChatGPT, etc.)
- [ ] Validate that only governed, classified data is accessible to AI agents
- [ ] Regulary assess technical readiness and remediate gaps before broad AI rollouts

Stakeholder Engagement

- [ ] Provide ongoing AI risk, governance, and responsible use training for all employees
- [ ] Encourage feedback and questions to refine governance practices

DOWNLOAD THE EBOOK FOR MORE PRACTICAL INSIGHTS

About Avertium

Avertium is an MXDR leader delivering comprehensive security and compliance services to mid-market and enterprise customers. Our unique “Assess, Design, Protect” approach addresses and improves security strategy, reduces attack surface risk, strengthens compliance, and provides continuous threat protection.

www.avertium.com

AVERTIUM

marketing@avertium.com