AVERTIUM

# AI Readiness Services

Organizations are anxious to leverage AI's ability to enable smarter decision-making, automate repetitive tasks, and enhance customer experiences to stay competitive without heavily burdening enterprise resources. But the possibility of inadvertently exposing their organization's sensitive data can be daunting to IT teams.

**Organizations looking to innovate must proceed with care to ensure responsible and secure adoption that meshes with company culture and business operations.**

Avertium understands the magnitude of this endeavor, and we're here to help. We make AI Readiness easier to incorporate into your normal operations and speed safe adoption **through three pillars:**

1. **AI governance**
2. **Technical enablement**
3. **Data centric controls**

## 1) AI Governance

AI's transformative potential is driving rapid innovation, with organizations eager to capitalize on emerging tools and technologies. As data volumes and the ability to mine them surge, the pace of implementation risks outstripping established best practices, making it essential to adopt effective strategies for responsible AI integration.

**86%** **of organizations are aware of AI regulations, but only 25% have a fully implemented AI governance program.** *Source*

To prepare for AI, organizations must lay the groundwork for a successful end state:

- Gain leadership buy-in to drive specific outcomes
- Define desired outcomes and develop associated use cases
- Understand current state and what achieving your desired outcomes requires
- Establish policies and procedures to define acceptable use of emerging technologies to enable organizational goals

### NIST AI RMF Assessment

The National Institute of Standards and Technology Artificial Intelligence Risk Management Framework (NIST AI RMF) provides a structured approach to managing AI pitfalls.

Avertium's NIST AI RMF Assessment service helps organizations to confidently align their unique needs with the framework's best practices. Whether developing AI in-house, using or integrating third-party models, or scaling AI across business units, **our expert-led assessment provides a clear path to responsible and secure AI adoption in the context of your business:**

- Enable secure innovation balanced with business productivity.
- Reduce risk exposure and identify shadow AI.
- Build stakeholder trust and integrate smoothly with business operations.
- Understand foundational requirements and needed remediation.
- Adhere to other frameworks (NIST CSF, HIPAA, HITRUST, PCI, etc.) and bundle services to streamline compliance efforts and reduce costs.
- **Deliverable:** Actionable report with detailed remediation recommendations

# 2) Technical Enablement

Effective AI tool configuration and deployment are essential for safeguarding security, maintaining compliance, ensuring accuracy, and building user trust – all while minimizing risks like data leaks, bias, and misuse. For organizations leveraging Microsoft, Copilot stands at the forefront of AI enablement - helping teams collaborate more efficiently and innovate across their Microsoft ecosystem. Responsibly and securely unlocking this technology's full potential requires strategic alignment, technical readiness and organizational preparedness.

**55%** **of enterprise IT security say they're not fully confident they have the necessary guardrails for deploying AI agents.** *Source*

## Microsoft 365 Copilot

Informed preparation is essential for Microsoft 365 Copilot to safeguard sensitive information, maintain compliance, and ensure accurate results in productivity tools such as Word, Excel, PowerPoint, Teams, and Outlook. Without readiness, Copilot could expose confidential data, increase security risks, or produce unreliable outcomes. Careful planning helps maximize productivity, align with company policies, and minimize operational and regulatory risks.

## Security Copilot

With Security Copilot's inclusion in Microsoft 365 E5 subscriptions, agents are built directly into the flow of work for Microsoft Defender, Microsoft Entra, Microsoft Intune, and Microsoft Purview. So, while it will be more manageable to use Security Copilot than ever before, E5 users must understand where their data security stands and how to improve.

## Copilot Readiness Assessment

Avertium's Microsoft Copilot Readiness Assessment evaluates the strength of your Microsoft 365 and Azure technical controls to determine current state, identify gaps and build a clear roadmap for successful Microsoft 365 Copilot and Security Copilot rollouts:

- Collect security control and maturity data from across your Microsoft Cloud platform.
- Compile findings and map them to multiple security frameworks to create a thorough gap analysis.
- Create recommendations and establish a roadmap for implementation.
- Optionally establish procurement schedules, timelines, and allocate resources to implement remediations.
- **Deliverable:** Actional report including executive summary and detailed remediation recommendations.

# 3) Data Centric Controls

The exponential growth of data volumes and generative AI applications is increasing risk, making robust data protection and governance essential. Organizations should implement data-centric controls - such as role-based access and least privilege - and prioritize identifying and classifying sensitive information to ensure secure, compliant AI adoption.

**31%** **of organizations are reported to have a clear, fully implemented data governance strategy.** *Source*

Microsoft Purview provides unified data governance, compliance, and risk management across your organization, creating a trusted framework that ensures responsible data handling & regulatory alignment.

## Purview Services

Avertium provides a multi-tiered service model that helps organizations to understand, adopt, and optimize Microsoft Purview's vast AI capabilities over a gradual process:

- **Data Security Envisioning Workshop:** Guidance on how Purview supports AI adoption through governance, retention policies, and communication compliance.
- **Purview Starter Kit:** Provides foundational support to ensure effective AI adoption preparation through data governance, retention policies, and communication compliance.
- **Purview Solution Deep Dives:**
  - **Information Protection -** Classify and safeguard sensitive data using AI-powered labeling and classification tools.
  - **Insider Risk Management -** Identify internal threats using behavioral analytics & AI-driven insights.
  - **Data Loss Prevention (DLP) -** Implement AI-enhanced policies to secure data across platforms and devices.
  - **Data Security Posture Management (DSPM) -** Activate, configure, and optimize features, ensuring safe AI adoption without compromising productivity or compliance.
- **Maturity and Optimization:** Build out a data governance program to maximize and advance E5 license holders' Purview platform implementation.

## 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.