

Shadow AI Risk Checklist

How IT Leaders Regain Control Without Slowing Innovation

The Observation: The Hidden Crisis of Ungoverned AI

IT leaders are facing intense pressure to accelerate AI adoption, but employees are already bypassing governance to get ahead. The rise of shadow generative AI means sensitive company data may be exposed to public AI tools or processed outside of secure, cost-controlled environments.

Shadow AI goes beyond rogue employees using ChatGPT. Everyday tools like M365 Copilot, Gong, and DemandBase now feature embedded AI. Without proper governance and access controls, this quiet proliferation exposes sensitive data and escalates your risk.

The Impact: The Hidden Costs of Inaction

Ungoverned AI creates severe business risks, including compliance exposure and a staggering \$670,000 added to average breach costs. Beyond security, unchecked AI models fed by stale data produce flawed insights that drive poor executive decisions. Furthermore, this unstructured usage creates unplanned spending through hidden API calls, redundant licenses, and unchecked cloud consumption.

"Shadow AI isn't just rogue public tool usage; it's the ungoverned AI capabilities embedded in the platforms you already use."

The Shift: A New Paradigm of Responsible Modernization

The goal is governed enablement, not reactive blocking. Attempting to lock down all AI usage will only drive it further underground and stall innovation

By establishing a strong foundation of governance, data readiness, and a hybrid architecture, organizations can scale AI safely without sacrificing control. Responsible governance accelerates the path from stalled pilots to production, reducing risk and driving faster board-level decision-making.



Regain Control of Your AI Environment

Use this action plan to identify exposure points and establish a foundation for secure innovation.

Inventory Usage and Access

Identify which AI tools teams are actively using, who is using them, and what data streams are involved. Crucially, validate how AI embedded in existing tools (like M365, CRM, and marketing platforms) accesses, processes, and surfaces your data.

Classify Data Exposure and Quality

Determine if users are feeding sensitive customer, financial, or proprietary information into public models. Simultaneously, audit your data to identify stale, outdated, or ungoverned information from causing flawed AI outputs.

Set Governance Guardrails

Define clearly approved tools, access rules, data handling policies, and escalation paths for exceptions.

Monitor and Control Data Access

Continuously validate that AI tools only access the data they strictly need. Enforce proper controls and least-privilege access across all systems.

Assess Cost Visibility

Pinpoint where unstructured AI usage is creating unplanned spend. Look for hidden AI feature licensing (like Copilot-style add-ons), unchecked public cloud consumption, and redundant tool licenses.

Validate Infrastructure Fit

Determine which AI workloads belong in the public cloud, private environments, or a hybrid model based on your specific security, latency, and cost containment needs.

Close the Operational Gap

Assign cross-functional ownership across security, infrastructure, and line-of-business teams so AI usage evolves from a shadow practice into a managed, strategic program.

The Payoff: Strategic Advantage Through Governance

Acting now provides your organization with fewer blind spots, better policy enforcement, and stronger cost predictability. Responsible governance is not just a defensive measure; it is the catalyst for safe, scalable modernization. Use this Shadow AI Risk Checklist to identify your biggest exposure points before expanding AI investments. **Let's connect to identify your next step in your journey to scalable, high-value AI.**

About TierPoint

TierPoint (tierpoint.com) is a leading provider of secure, connected IT platform solutions that power the digital transformation of thousands of clients, from the public to private sectors, from small businesses to Fortune 500 enterprises. Taking an agnostic approach to helping clients achieve their most pressing business objectives, TierPoint is a champion for untangling the complexity of hybrid, multi-platform approaches to IT infrastructure, drawing on a comprehensive portfolio of services, from public to multitenant and private cloud, from colocation to disaster recovery, security, and more. TierPoint also has one of the largest and most geographically diversified U.S. footprints, with dozens of world-class, cloud-ready data centers in 20 markets, connected by a coast-to-coast network.