

---

# AI Risk & Readiness in the Enterprise

---

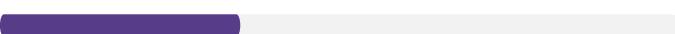
Risk Outpaces Governance  
AI is accelerating innovation across the enterprise—but risk is accelerating faster.

2025 REPORT

# AI Risk & Readiness in the Enterprise

This report, based on a survey of 233 security, compliance, and data leaders, uncovers a sobering reality: organizations are moving forward with AI adoption, yet leaving governance behind. From data leaks to regulatory blind spots to shadow AI running amok, the AI risk gap is widening. This report unpacks the findings question by question, weaving in enterprise takeaways, strategic guidance, and next steps to close the readiness gap.

## AI Risk is Outpacing Governance: Organizations Struggle to Keep Up

- ▶  **93.2%** of organizations lack full confidence in securing AI-driven data, leaving them exposed to security blind spots and compliance failures.
- ▶  **69.5%** of organizations cite AI-powered data leaks as their top security concern in 2025, yet **47.2%** have no AI-specific security controls in place.
- ▶  Over **80.2%** of organizations are unprepared for AI regulatory compliance, risking fines and reputational damage.
- ▶  **39.9%** admit they lack the tools to protect AI-accessible data, creating a dangerous gap between AI adoption and security controls.
- ▶  Only **6.4%** of organizations have an advanced AI security strategy, signaling widespread unpreparedness for AI-driven threats.

# AI Risk Awareness vs. Reality

Understanding AI risk is the foundation of AI governance. But without visibility into how models interact with sensitive data, enterprises are flying blind. Lack of oversight creates blind spots, compliance gaps, and potential exposure to unauthorized access, shadow AI behavior, or biased outcomes.

**Survey Question:** How well does your organization understand the risks associated with AI models and sensitive data exposure?

Response	
Early-stage risk assessment	<b>39.5%</b>
Aware but not actively managing it	<b>24.0%</b>
AI-specific security strategies in place	24.5%
Full visibility and control	6.4%
No visibility at all	<b>5.6%</b>

- ▶ **39.5% of organizations are in early-stage AI risk assessment, while 24% are aware but not actively managing it.**
- ▶ **5.6% of organizations have zero visibility into AI model risks, making them highly susceptible to AI-driven threats.**

## Key Insight:

**More than two-thirds of organizations admit they are early-stage or not actively managing AI risk—yet AI adoption is already in motion.**

**Takeaway:** AI transparency is critical for risk management. Enterprises must move beyond awareness to implementation—starting with visibility into how AI interacts with data. Organizations should implement AI risk monitoring solutions and data discovery tools that provide real-time visibility into AI interactions with sensitive data.

## Next Steps:

- Deploy AI risk discovery tools that identify model-data interaction
- Establish ownership for AI governance across security, privacy, and compliance
- Create an inventory of models, their data sources, and risk exposure

# AI-Powered Data Leaks & Shadow AI: The Top Threats of 2025

**Why It Matters:** As AI expands its footprint, so does its risk of exposing sensitive information. Shadow AI—unauthorized or unmonitored AI tools—further compounds that risk by operating outside of security visibility.

**Survey Question:** Which of the following AI risks is your organization most concerned about in 2025? (Select all that apply)

Risk Area	% of Orgs
AI-powered data leaks	69.5%
Unstructured data exposure	58.4%
Shadow AI / Dark AI	48.5%
Compliance with AI regulations	52.8%
Model access risk	40.3%

- ▶ **69.5% of organizations rank AI-powered data leaks as their biggest security concern.**
- ▶ **58.4% fear unstructured data exposure.**
- ▶ **48.5% worry about “Dark AI” or Shadow AI operating without oversight.**

## Key Insight:

**Data leaks remain the most feared threat—especially through AI’s interaction with unstructured data and the rise of unauthorized models. Organizations must act with urgency, implementing AI-specific data classification policies and access controls to prevent exposure and detect rogue model activity.**

**Takeaway:** Shadow AI isn’t a hypothetical—it’s already inside many environments. Lack of control over AI tools leads to uncontrolled risk.

## Next Steps:

- Enforce model registration and monitoring
- Use DSPM and classification to label AI-accessible data
- Flag unusual or rogue model behavior
- Take action to remediate risk: flag and tag data that’s safe for AI use; establish least privileged permissions for models accessing sensitive data; and minimize sensitive and regulated data to shadow AI exposure.

**BigID helps organizations uncover Shadow AI and monitor model-data interactions.**



# AI Security Controls: What's Missing

**Why It Matters:** Security must evolve to meet the complexity of AI. Traditional controls aren't built for AI pipelines, model endpoints, or training data governance. Without AI-aware tools, enterprises risk applying outdated solutions to a fast-moving problem.

**Survey Question:** What AI controls does your organization currently have in place?

Control Type	% Adoption
None (still evaluating)	<b>47.2%</b>
AI risk monitoring & response	35.2%
Access control for AI models	30.0%
AI-specific classification	<b>21.0%</b>

- ▶ **47.2% of organizations have no AI security controls in place.**
- ▶ **21% have AI-specific data classification and protection strategies.**

## Key Insight:

**Nearly half of organizations lack any formal AI controls—despite rising fears around data exposure and model misuse. Secure AI usage begins with governance. Build visibility across all model endpoints, enforce access rules, and monitor pipelines for shadow AI behavior.**

**Enterprise Takeaway:** You can't secure what you don't control. Model-level access and pipeline visibility must become first-class citizens in security programs.

## Next Steps:

- Build pipelines with classification and remediation hooks
- Enable access control and audit logs
- Prioritize policy enforcement tailored to AI-specific risks

**BigID provides native remediation and classification embedded into AI workflows, automating policy enforcement at scale.**

# Compliance & Regulation: The Lagging Priority

**Why It Matters:** AI regulation is no longer speculative—it's happening. The EU AI Act, US Executive Orders, and industry-specific policies are emerging fast. Enterprises caught unprepared face fines, disruption, and reputational harm.

**Survey Question:** How prepared is your organization to comply with emerging AI data regulations?

Response	
In progress, but unclear	<b>54.9%</b>
Not prepared at all	<b>25.3%</b>
Ready with governance frameworks	15.9%

- ▶ **54.9% are in progress preparing for AI regulations but lack clarity.**
- ▶ **25.3% are not prepared at all.**

## Key Insight:

**80% of organizations admit they are not ready or unclear on how to comply with emerging regulations. Organizations must prioritize AI compliance with structured, forward-looking frameworks that align to evolving global standards like the EU AI Act.**

**Takeaway:** AI compliance readiness isn't about checking boxes—it's about proving AI systems are transparent, ethical, and accountable.

## Next Steps:

- Align AI governance with frameworks like the EU AI Act and NIST AI RMF
- Define data usage, retention, and purpose limitations for AI
- Enable auditability and documentation at every model decision point

**BigID supports compliance by automating assessments, reporting, and enforcing AI-specific data policies aligned to evolving regulations.**

# AI TRiSM: Trust, Risk, and Security Management

**Why It Matters:** Trust is the cornerstone of enterprise AI adoption. If employees, customers, or regulators can't trust your AI, its value collapses. AI TRiSM requires understanding what your models are doing, what data they access, and whether they comply with internal and external rules.

**Survey Question:** How prepared is your organization to comply with emerging AI data regulations?

Response	
Somewhat confident	64.4%
Not confident at all	28.8%
Very confident	6.9%

64.4% of respondents are only somewhat confident in securing AI-driven data.

31.8% lack confidence entirely.

**Survey Question:** How confident are you that your AI models aren't using unauthorized or sensitive data?

Response	
Somewhat confident – gaps exist	55.8%
Not confident – no oversight	31.8%
Very confident – strict controls	12.4%

55.8% admit their models may be using unauthorized or sensitive data.

## Key Insight:

**Trust is low. More than half of respondents suspect their models may be mishandling sensitive or unauthorized data. AI TRiSM isn't optional—it's foundational. Establish model governance, map dependencies, enforce guardrails, and build auditability across every stage of the AI lifecycle.**

**Takeaway:** You can't build trust on top of uncertainty. AI TRiSM must be baked into every layer—from training to deployment.

## Next Steps:

- Map model dependencies to training data and data sources
- Monitor and document model outputs and risks
- Integrate privacy and risk assessments into AI DevOps pipelines

**BigID enables AI TRiSM with policy automation, audit trails, and full AI data lineage visibility across the AI lifecycle.**

# Industry Spotlights: Unique Risks by Vertical

**Why It Matters:** AI doesn't operate in a vacuum. Each industry faces unique risks and regulations. Security and governance must adapt to sector-specific data flows, compliance demands, and AI innovation maturity.

## Key Observations:

Industry	Notable Risk/Gap	% Affected
Financial Services	Lack of AI-specific data protections	62%
Healthcare	Struggling with compliance and oversight	52%
Retail & Consumer Goods	No visibility into AI model interactions with PII	48%
Technology & SaaS	No formal AI risk strategy despite rapid adoption	42%

**Enterprise Takeaway:** A one-size-fits-all approach won't cut it. AI governance must reflect your data types, threat landscape, and compliance pressure. Verticalized AI challenges require verticalized solutions. Each sector must align their risk, compliance, and AI deployment to their regulatory realities.

- **Financial Services:** Despite heavy regulation, only 38% of firms have implemented AI-specific data protections.
- **Healthcare:** 52% cite AI regulation compliance as a significant hurdle.
- **Retail:** 48% lack visibility into customer data usage within AI.
- **Technology & SaaS:** 42% report no formal AI risk strategy, despite leading innovation.

## Next Steps:

- Build vertical-specific AI governance playbooks
- Integrate data discovery with regulatory risk scoring (e.g., HIPAA, GLBA, PCI-DSS)
- Monitor AI models for purpose drift and compliance violations

**BigID's verticalized governance templates help financial, healthcare, and tech organizations meet regulatory requirements while operationalizing AI trust.**



# Who Owns AI Risk? The Governance Gap

**Survey Question:** Who in your organization is responsible for AI security, compliance, and governance?

Owner	
IT Security / CISO	<b>54.1%</b>
Data Governance Team	<b>29.2%</b>
Risk & Compliance Team	29.2%
Data Privacy Team	25.8%
No clear ownership	21.9%

**What It Means:** Responsibility is fragmented—and in 1 in 5 orgs, undefined. Without a clear owner, AI governance programs will stall or fail.

## Next Steps:

- Assign dedicated AI governance leaders or committees
- Connect governance with DevOps, DataOps, and SecurityOps
- Use a unified platform to give every stakeholder shared visibility

**BigID bridges teams with shared policy controls and centralized AI, privacy, security, and governance dashboards.**

# Strategic Priorities: What's Top of Mind in 2025?

---

**Survey Question:** What's your biggest AI-related priority in 2025?

Priority	
Compliance & governance	<b>36.1%</b>
Visibility into AI risk	<b>30.0%</b>
Preventing AI-driven data leaks	<b>15.0%</b>
Implementing security controls	<b>14.2%</b>

- ▶ **36.1% prioritize compliance & governance**
- ▶ **30% focus on risk visibility**
- ▶ **15% on preventing AI-driven data leaks**
- ▶ **14.2% on implementing security controls**

**What It Means:** The focus is still on visibility and governance—but operational controls are lagging. Too few organizations are focused on prevention and enforcement. Security priorities aren't matching security exposures. AI risk strategy must move from awareness to enforcement—with tooling, telemetry, and trust frameworks.

## Next Steps:

- Shift strategy from governance-on-paper to governance-in-practice
- Integrate real-time monitoring and automatic remediation
- Align tooling with stated priorities to close execution gaps

# Final Recommendations: Building AI Security That Scales

---

To close the readiness gap and reduce AI exposure:

- Deploy AI risk monitoring and shadow AI detection
- Build secure pipelines from training data to model output
- Implement AI-aware classification, remediation, and policy enforcement
- Embed AI TRiSM throughout development and deployment
- Align governance with global regulations and internal accountability

## ACTION TODAY PREVENTS EXPOSURE TOMORROW.

With BigID, enterprises can govern AI with precision—building trust, reducing risk, and preparing for what's next.

### Survey Demographics: Who Was Surveyed?

This report is based on responses from 233 security, compliance, and data professionals across multiple industries, geographies, and company sizes. The survey provides a comprehensive snapshot of how organizations are handling AI security risks and governance challenges.

#### Industries Represented:

**Technology & SaaS:** 34.3%

**Financial Services & Insurance:** 19.7%

**Government & Public Sector:** 8.6%

**Healthcare & Life Sciences:** 6.4%

**Retail & Consumer Goods:** 4.7%

**Manufacturing / Energy:** 4.3%

**Other Industries:** 21.9%

#### Geographical Distribution:

**North America:** 41.2%

**Europe:** 25.3%

**Asia-Pacific:** 18%

**Middle East & Africa:** 8.2%

**Latin America:** 7.3%

#### Company Size:

##### Small to Mid-Sized Enterprises

(**<1,000 employees:** 54.1%)

##### Mid-Market (**1,000-5,000**

**employees:** 24%)

##### Large Enterprises (**5,000+**

**employees:** 21.9%)

## About BigID

BigID helps organizations connect the dots across data & AI: for security, privacy, compliance, and AI data management. BigID enables customers to find, understand, manage, protect, and take action on high risk & high value data, wherever it lives.

Customers use BigID to reduce their AI & data risk, automate security and privacy controls, achieve compliance, and understand their data throughout their entire data landscape: from the cloud, on-prem, and everywhere in between.

## Connect the Dots Across Data & AI

**Security • Compliance • Privacy • AI Data Management**

Reduce risk, accelerate time to insight, and get data visibility and control across all your data - everywhere.



**Tools like BigID are the future.**

Organizations should be leveraging these tools to remove the manual processes from data discovery, provide better visibility, and help with prioritization of controls.



Ryan O'Leary

Future of Trust: Battling Data Discovery Confusion