kyndryl

Data custodianship

Unlocking value through effective data governance

Table of contents

Introduction

Powerful AI systems can now surface hidden patterns from mountains of information, turning tiny, overlooked data points into game-changing insights. But those insights are only as reliable as the data beneath them. And with the rise of agentic AI, the stakes climb higher: autonomous agents may act on incomplete, inaccurate, or misclassified data. That makes protecting data integrity not just important — but also urgent.

Leaders across industries need confidence their data is secure and trustworthy. Breaches, regulatory lapses, and business disruptions can erode trust, disrupt operations, and prove costly.

As data volumes soar, so too does the complexity of protection. Leaders must safeguard ever-growing troves of information, comply with new regulations, and prepare for emerging threats — from advanced cyberattacks to quantum computing's challenge to today's encryption.

Risks now extend across entire digital supply chains, where weak links can expose the whole enterprise. Resilience demands tracing data end-to-end to close those gaps.

And this work is important — now more than ever. Understanding where data is located, how it's classified, who has access to it, and what it's used for is essential if data is to remain an asset rather than a liability. Unlocking the full value of this data, however, is a complex undertaking that requires a robust and unified data strategy.

Data governance — the act of creating rules and standards that control how data is collected, stored, used and disposed of — requires the involvement of multiple enterprise functions. To be effective, leaders must extend the responsibility for managing the quality, security and availability of an organization's data across the entire company. Today, everyone is a data custodian.

71%

of business leaders who don't feel their AI implementation is ready to manage future risks.

Source: Ai Readiness Report, 2025

A critical priority

Data governance has become a critical matter for every stakeholder involved in business success — customers, boards, employees, and partners.

Robust governance presents new opportunities to accelerate digital transformation, improve decision-making, and more nimbly adapt to global regulations and standards while conducting business across borders. With good governance practices, businesses also stand to increase their readiness to benefit from AI implementation — a critical need at a time when leaders are looking to see more positive returns on their AI investments.

42%

of business leaders who report seeing a positive return on their AI investment.

Source: Kyndryl Readiness Report, 2025

Emerging challenges in data governance

01. Expanding data risk

Managing risk is critical to safeguarding data and meeting regulations. With cyber disruptions now a matter of when, not if, businesses need proactive protection backed by strong governance. Breaches, losses, and compliance failures can bring steep fines, operational breakdowns, and eroded trust.

The threat is escalating. Over half of large organizations reported a disruptive cyberattack in the past year, according to Kyndryl's Cyber Gauge 2024 report, and 61% of those hit suffered four or more incidents. AI-driven attacks are compounding the risk, as hackers use autonomous systems to strike faster and with greater sophistication.

Internal governance alone is no longer enough. Third parties now account for a growing share of breaches and ransomware attacks, since vendor and partner technologies form a highly interconnected digital supply chain. Each weak link creates entry points for cascading damage, including cyberattacks and poisoned AI models. Evaluating partner data governance and cybersecurity is now as critical as securing your own.

Looking ahead, as bad actors seek to exploit AI to launch increasingly sophisticated attacks, AI-powered tools may also hold the key to solving challenges related to third-party risk. For example, businesses can implement AI-based continuous monitoring platforms that integrate multiple data sources to assess third-party risk in real time.

02. Tracing data's complex flow

Just as geographical maps provide direction, businesses need data mapping capabilities to determine the risk involved in future engagements with suppliers or navigate a system disruption. Further, enterprises need a clear picture of how and where data flows to not only strengthen data governance and enable compliance reporting, but to preemptively identify vulnerabilities and make improvements throughout their data estates.

But as the volume of data increases and originates from disparate sources, tracing its labyrinthine path poses a growing challenge.

This is doubly true when gathering information about data shared and stored throughout supply chains. Because of how enterprise technology is layered — with different structures and formats of data embedded throughout the tech stack in platforms, applications, and third-party tools — data mapping can be a strenuous, time-consuming, and complicated endeavor. When every chain of suppliers' systems connects to additional offshoots of more vendors and suppliers, the resulting webs can be nearly impossible to fully trace and investigate.

Scalable mapping tools that integrate on-prem, cloud, and hybrid data give businesses a clear view of data flows and a single source of truth. Emerging trends—like metadata-driven mapping, real-time updates, and AI-powered automation—are turning mapping into a catalyst for data-driven transformation. That matters: half of business leaders cite limited access to relevant data as their top risk-management challenge.

03. Data flows, interrupted

Keeping up with a rapidly evolving regulatory landscape is a constant effort, as new legal and technological developments and geo-political risks shape the global movement of data.

Since its enactment in 2018, the EU General Data Protection Regulation (GDPR) has played an important role in transforming and harmonizing the global regulatory landscape, helping to secure international data flows and protect data subject rights. The principles of GDPR are being broadened by regulations like the Digital Operational Resilience Act (DORA). Focused on the banking and financial services sector, DORA encompasses non-personal information and operational resilience, further raising the importance of business-wide data custodianship. Companies that provide IT services to EU financial entities will be expected to adhere to contractual arrangements designed to meet DORA's requirements.

In opposition to this global convergence, however, we are now seeing increasing legislative divergence caused by data localization and regionally-specific privacy and access rules. As the era of effortless data movement fades, data sovereignty concerns are reshaping how organizations store, govern, and share information. Nations are tightening control over where data can reside and who can access it, turning data governance into a strategic imperative rather than a compliance function.

In this new environment, intentional architectures — rooted in strong governance, observability, and policy enforcement — are essential to maintaining trust, preserving interoperability and enabling AI innovation across borders. Data sovereignty is no longer a constraint to navigate, but a design principle that determines who can operate, compete, and innovate in a fragmented digital landscape.

This shift toward tighter control is already reshaping regulatory frameworks around the world. As of early 2023, there were already over 100 restrictive data localization laws in place across 40 countries, while the laws of certain countries permit government access to data without due process. Complying with these varying and sometimes conflicting regulations creates significant challenges for multinationals, turning the digital supply chain into a geopolitical lever, as evidenced by fluid conversations around international trade and digital services taxes.

At a strategic level, keeping pace with changing regulations requires agility. By setting high standards for governance, adopting a flexible data architecture and infusing data custodianship across their business, organizations can tailor their data practices to comply with any mandate without sacrificing innovation.

04. Responsibly integrating AI

Artificial intelligence is being rapidly deployed across enterprise IT environments around the world and businesses want to benefit from more efficient AI-powered services. However, business leaders report data privacy and security as the top barrier to AI adoption, according to the Kyndryl Readiness Report.

AI systems require not only more data, but more types of structured and unstructured data that may be used in new and novel ways. Businesses must therefore carefully evaluate the kinds of AI systems they procure or build, the data used to train these systems, and the data these tools and systems can access.

The increasing use of AI systems — and particularly agentic AI — also highlights the importance of data quality. No matter how advanced an AI model is, poor input will result in poor, even detrimental, output. As AI agents gain access to vast data sources in order to work together to solve multi-step problems, data quality assurance and curation become significantly more important; successful and responsible AI implementation hinges on data integrity.

As they invest in AI, companies must balance concerns around privacy, confidentiality, and ethics with their push for AI-driven innovation. Do they want their data to be used to train foundational AI models, for instance? And do they want control over how their data is used by vendors to train systems used by other businesses?

Determining how to proceed is easier said than done when the data risks connected to each individual AI use case may be different — and when nations are pursuing different regulatory approaches that will impact AI governance. While some nations such as the U.S. take a decentralized approach, others in the EU are working toward risk-based and unified standards. As part of the EU AI Act, for example, businesses are required to classify and prioritize high-risk cases — such as those that involve the collection of biometrics — as well as identify prohibited cases. To do that, organizations need the ability to evaluate tools for data misuse, accuracy, and hallucinations, among other issues.

31%

of business leaders who report data privacy and security as a top barrier to AI adoption.

Source: Ai Readiness Report, 2025

Advancing data custodianship

As they navigate these critical data challenges, enterprises have a significant opportunity to take a more modern, proactive approach to governing data throughout its full lifecycle — and encourage the same from their supply chain partners. Data custodianship can be a powerful driver of strong data governance, trusted data stewardship, and more valuable data insights.

Develop a workforce of data custodians

Traditionally, data governance was considered the responsibility of a dedicated team, and company-wide education opportunities may have been limited to one annual training. In modern enterprises that depend on interconnected digital systems, and with AI's potential to turn enterprise data into a business catalyst, data custodianship has developed into a shared responsibility.

Everyone in an organization can play a role in organizing, standardizing and automating data practices to improve data quality, simplify risk management, and help their organizations better understand and protect their data assets. Organizations can empower their data custodians through strong governance and by embedding best practices for data hygiene across all business functions.

Broader technology modernization efforts can further support these efforts: one of the key benefits business leaders report as a result of updating their IT Infrastructure, systems and practices to meet the demands of the digital age is enhanced data security and regulatory compliance, according to the Kyndryl Readiness Report.

But turning data custodianship into a shared responsibility also requires cultural transformation. In the modern enterprise, employees are both the first line of defense — and the greatest source of risk. To that end, businesses must build a culture where safely and securely handling data is an everyday priority.

Holistic, engaging, and ongoing education is key to fueling this cultural shift. Beyond mandatory annual training in data privacy, cybersecurity and AI, enterprises can explore implementing interactive learning journeys using nudges, incentives and other techniques, while centralizing relevant policies and guidelines in an easily accessible portal. AI-powered adaptive programs that simulate real-world threats can also offer personalized experiences that automatically adjust difficulty level and provide real-time feedback.

Enterprises should invest in practical role-based programs, tailored to the data risks that are unique to each employee's daily work. Developers, for example, may be trained in secure coding practices, while training for marketing professionals may include proper use of generative AI when developing content. Such programs promote compliance with both internal governance and relevant laws — promoting AI literacy, for example, is a requirement of the EU AI Act.

But data custodianship is ultimately less about ticking compliance boxes and more about unlocking new value. By investing in continuous learning, promoting best practices, and creating a culture of data custodianship, enterprises can help their workforce understand what's at stake in a fast-evolving data landscape, manage emerging risks, and harness AI to seize new opportunities.

Recommended actions

Enterprises can take key steps to embed data custodianship across their operations:

01. Empower data custodians through strong governance

- **Know your data:** Map where it lives, how it's classified, who can access it, and how it's used.
- **Prioritize privacy from the start:** Businesses should incorporate privacy-by-design principles into their data governance to embed privacy considerations into system design from the start and throughout the full data lifecycle.
- **Simplify, standardize, and communicate governance** — Develop clear policies, provide centralized access to governance policies, and effectively communicate proper data practices through continuous training to all employees to help them understand the data landscape.
- **Turn data governance into a unified framework** — AI systems make data governance more complex, but a unified framework helps teams across the business to innovate while maintaining integrity and accountability.

02. Manage evolving data risks and regulations

- **Track regulations:** Stay current on data, security, and AI rules, and prepare reporting processes.
- **Strengthen defenses** — Apply zero trust, access controls, encryption, and continuous monitoring.
- **Modernize resiliency** — Use AI for anomaly detection, air-gapped backups, and tools for observability.
- **Secure the supply chain** — Demand transparency to at least the second tier and require governance standards from partners which include secure storage and transfers, and strict access controls.
- **Dispose wisely** — Keep only necessary data; secure and delete the rest.

03. Unlock data's value with AI

- **Prioritize privacy with AI innovation** — Balance AI implementation with data privacy, confidentiality, and ethics concerns to maintain transparency and control over how data is handled.
- **Govern AI collaboratively:** Engage cross-functional teams in vetting and oversight.
- **Build trust in AI implementation:** In addition to strong AI governance, businesses may consider adopting voluntary frameworks such as the National Institute of Standards and Technology (NIST) AI Risk Management Framework, or achieving ISO 42001, the first AI management system international standard.
- **Leverage AI for insight:** Use AI-driven platforms to monitor compliance, spot vulnerabilities, and generate business value.

Market imperative

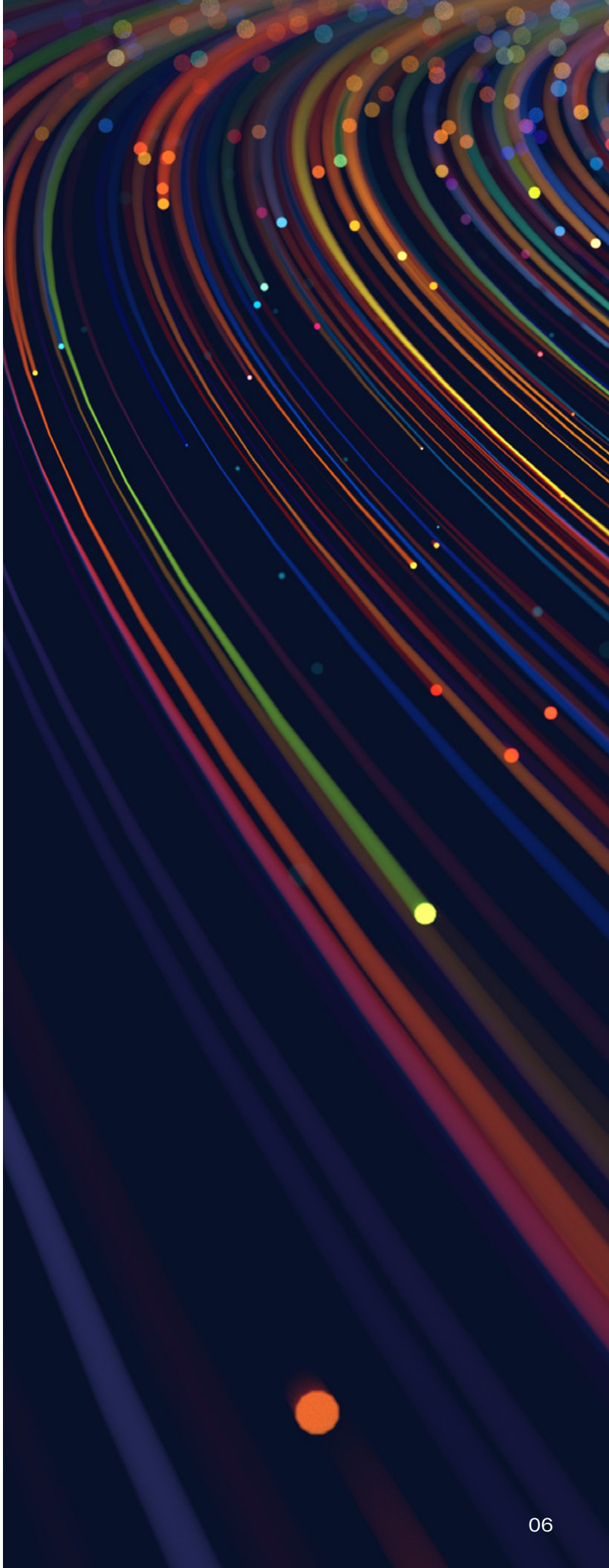
Data governance is an increasingly important undertaking, requiring extensive expertise in managing the risks that imperil sensitive data and the complex digital ecosystems through which it flows.

This is particularly true in hybrid IT environments, which include enterprise and third-party on-premise as well as private and public cloud environments with interconnected webs of hardware, software, and diverse data sources. Businesses that operate in these environments — particularly those in highly-regulated industries such as banking, healthcare, or energy — recognize that their ability to provide the services and products that fuel the global economy depends on how their data is sourced, maintained and secured.

The rapid proliferation of AI throughout enterprise IT environments is intensifying this focus on data assets and adding new layers of complexity as AI systems ingest increasing volumes of data and are tasked with optimizing and automating core enterprise processes.

By taking an integrated approach to data governance that aligns teams and strategies, enterprises can build a unified data governance framework and reduce complexity as they work together to protect, secure, and fully harness their data.

With strong support from senior leadership, the right technical skillsets and capabilities, investment in continuous education, and a dynamic culture that fosters a shared responsibility for safeguarding data, enterprises can adapt their current practices to better prepare their organization for emerging challenges and gain greater control over their data assets to accelerate business goals. In short, enterprises need a workforce of data custodians.



kyndryl