



Is your organization data-ready for AI? (and how to get there if you aren't)

There's data. Then there is *quality* data.

And when it comes to artificial intelligence (AI),
knowing the difference is a game-changer.

Presented by

AMERICAN BANKER.

Sponsored by



AI is at the top of almost every business leader's priority list: 86% of financial services IT and business executives say that AI is critically important to their business' success in the next two years.¹

86%

of financial services say that AI is critically important to their business' success

There are dozens upon dozens of use cases for AI, from real-time contract analysis to invoice processing to predicting delinquencies based on historical payment information to regulatory reporting. But even though AI is becoming a must-have for financial services institutions, the track record for AI success isn't great.

Gartner reports that 49% of organizations struggle to estimate and demonstrate the return on investment (ROI) of AI projects.²

AI challenges often boil down to issues surrounding data integrity. "When it comes to AI, the quality of the product you get is only as good as the data you feed into the models," explains Josh Langley, Iron Mountain's CIO.

Yet there's a disconnect: Even though data integrity is key to successful AI implementation, only 17% of business leaders consider a robust data strategy as the most effective way to ensure ROI on AI.³

Why this white paper is a must-read

AI ROI isn't guaranteed, but your upfront work will lay a foundation for success. This white paper explores how data quality impacts AI initiatives, the barriers to data integrity, how to overcome them, and best practices for addressing data readiness.

Perceived AI data readiness vs. reality

When asked, many organizations believe their data is AI-ready, but once you dig a bit deeper, you'll find areas of concern, with more than half of organizations saying they have AI implementation challenges that include data quality, data categorization, unstructured data, and data silos.⁴



When it comes to AI, the quality of the product you get is only as good as the data you feed into the models.

– Josh Langley, CIO, Iron Mountain

For example, although 88% of organizations say they have an information management strategy, 44% admit that their strategy lacks basic components such as data archiving and retention policies, lifecycle management solutions, and inadequate strategy leading to data quality issues.⁵

You are not ready for AI without getting a handle on data integrity. Data integrity refers to the accuracy, consistency, and reliability of data, including structured and unstructured data and data that exists in physical documents.

"AI insights are reliant upon data integrity," notes Langley.

¹ www2.deloitte.com/us/en/pages/consulting/articles/ai-in-banking.html

² www.gartner.com/en/newsroom/press-releases/2024-05-07-gartner-survey-finds-generative-ai-is-now-the-most-frequently-deployed-ai-solution-in-organizations

³ cdn.avepoint.com/pdfs/en/shifthappens/AI-IM-Whitepaper-v4.pdf

⁴ www.cio.com/article/3512743/get-your-data-ai-ready.html

⁵ cdn.avepoint.com/pdfs/en/shifthappens/AI-IM-Whitepaper-v4.pdf

Addressing the significant data challenges impacting AI success

Various factors impact data integrity, including unstructured data, dark data, and increasing data volumes.

Unstructured data accounts for at least half of all data—and probably more. Forrester found that an average of 31% of enterprise data is semi-structured, and 27% is unstructured.⁶ Unstructured data typically doesn't make it into AI models, meaning institutions base important decisions on less than half their data, creating business blind spots.

While financial institutions have progressed in managing unstructured data, they need to do more to extract, contextualize, and make it accessible. The effort is well worth it since institutions that invest in mining unstructured data are nearly three times more likely to experience double-digit revenue growth than those that don't make the investment.⁷

Dark data—data that is accessible but not knowable—is another challenge. It poses risks by adding to business blind spots but also opens financial institutions up to regulatory risks since unknown data may not be compliant.

Two-thirds (64%) of organizations manage at least 1PB of data, and 41% manage more than 500PB.⁸ Data volumes will continue to increase, so kicking the data integrity problem down the road only means that you'll have a more significant challenge when AI project failures force you to address data integrity issues.

5 signs your data is ready for AI

AI is exciting, and the use cases are compelling. However, a prudent approach is best for ROI. "Don't jump right to solutions," advises Swami Jayaraman, Senior Vice President and Chief Enterprise Architect at Iron Mountain. "Get a deeper understanding of data to enhance insight and develop strategic, targeted solutions for your business."

Following are five critical components of AI-ready data.

1. You've built a strong data foundation

Organizations with a strong data strategy are 1.5 times as likely to get advantages from AI as those that don't have a strong strategy in place.⁹

By 2028, organizations that implement comprehensive AI governance platforms will experience 40% fewer AI-related ethical incidents compared to those without such systems, Gartner predicts.¹⁰

However, only 28% of organizations have established AI governance and risk management best practices.¹¹ Four in ten (44%) do not have data archiving and retention policies.¹²

Organizations with a strong data strategy are

1.5x

as likely to get advantages from AI as those that don't have a strong strategy in place.

⁶ reprints2.forrester.com/#/assets/2/1881/RES180405/report

⁷ reprints2.forrester.com/#/assets/2/1881/RES180405/report

⁸ thecloudcommunity.net/business-performance/ai-and-copilot/ai-and-information-management-report-2024/

⁹ cdn.avepoint.com/pdfs/en/shifhappens/AI-IM-Whitepaper-v4.pdf

¹⁰ networkworld.com/article/3574556/gartner-top-10-strategic-technology-trends-for-2025.html

¹¹ prnewswire.com/news-releases/the-ai-maturity-gap-leaders-overestimate-ai-readiness-and-workers-lack-training-302258842.html

¹² cdn.avepoint.com/pdfs/en/shifhappens/AI-IM-Whitepaper-v4.pdf

“The success of AI is a foundation deeply rooted in security and compliance. Data sovereignty and data residency are paramount to success,” notes Jayaraman.

Your data strategy should thoroughly cover how data is stored, accessed, and managed across the institution to ensure that:

- Data formats are consistent
- Data governance is in place to monitor data practices and ensure compliance
- Data blind spots are addressed so you are fully aware of all your data, regardless of location or format
- Data owners possess and are responsible for information
- Established guardrails are in place to ensure compliance with security requirements
- The data framework considers access control and data encryption at rest and in transit

Although critically important, building a solid foundation isn't the most exciting project, and you may face pressure to start delivering AI use cases quickly. Set expectations upfront with your board and senior management and educate them on the value of uncovering and surfacing as much data as possible before jumping into AI.

2. You've invested in your enterprise platform layer, and your systems are connected

Any AI transformation must incorporate data across the entire financial institution. We don't know what we don't know, so take the time to understand your legacy system environment before modernizing and opening your technology stack. Evaluate platform performance and scalability for data volumes and transactions to future-proof your technology foundation and avoid costly upgrades.

Conduct a technical inventory that includes everything from core applications and databases to custom-built applications to rogue Excel spreadsheets. Understand how both internal and external systems interact. Is data sharing automated, or are there manual workarounds?

Connect enterprise platforms to ensure critical data is available as soon as possible for operational efficiency and fact-based decision-making.

One tactic to discover data integration bottlenecks is to look at each process through a customer journey lens. Identify pain points first and then look for ways to leverage automation to provide better customer experiences and streamline workflows.

Modernizing your technology platform and connecting systems will require new technologies like AI and blockchain. While these technologies enable superior customer experiences and robust risk management, integrating them into your platform requires meticulous planning and implementation.

3. You have a unified strategy for managing both digital and physical assets

Just because data is digital doesn't mean it's accessible. Almost half (46%) of data is stored in physical documents, 87% is stored in the cloud, and 51% is stored in self-hosted storage.¹³

¹³ thecloudcommunity.net/business-performance/ai-and-copilot/ai-and-information-management-report-2024/

Some data is hiding in plain sight; other data is locked away in boxes in someone’s office. And organizations know it: 96% say that a unified asset strategy for managing digital and physical assets is crucial to the success of gen AI initiatives.¹⁴

Since you need all these data assets to get the most out of your AI initiatives, you need technology such as AI, machine learning (ML), and natural language processing (NLP) to efficiently transform physical and digital data into structured formats.

“AI is a powerful portal between digital and paper documents,” says Jayaraman.

Intelligent Data Processing (IDP) uses AI and ML to automate the processing of unstructured data contained in documents by extracting, classifying, enriching, structuring, and searching documents for relevant information.



IDP has significant cost savings benefits. Forrester quantified the benefits of IDP on a composite organization in a three-year risk-adjusted, present-value financial analysis:¹⁵

- More than \$3.1 million saved due to 40% more efficient discovery of documents and information
- \$846,400 saved by improving cataloging and understanding of documents and information by 55%
- \$905,200 saved by reducing 26,000 hours of work through increased collaboration
- \$247,300 saved with better security and compliance processes that reduced auditing time by 25%
- \$211,400 saved in storage costs

4. You recognize that risk management is about people

Risk management isn’t just the responsibility of the chief risk officer. Risk awareness is everyone’s job. “Instill a culture of continuous learning and adaptation that is strongly underpinned by ethical and responsible data practices and security,” suggests Jayaraman.

Your employees are your front line and one of your best defenses against security incidents and data breaches. For example, 78% of cybersecurity incidents were due to errors and social engineering.¹⁶ Many of these were likely preventable with employee awareness training.

¹⁴ www.ironmountain.com/resources/whitepapers/c/capitalizing-on-generative-artificial-intelligence-the-role-of-a-chief-ai-officer

¹⁵ www.ironmountain.com/resources/whitepapers/i/iron-mountain-insight-improves-financial-services-organizations-information-management

¹⁶ www.verizon.com/business/en-gb/resources/reports/2024/dbir/2024-dbir-data-breach-investigations-report.pdf

Empower employees to identify and escalate security issues and openly communicate their concerns. Train employees on data privacy regulations and best practices. Regular audits can identify and mitigate potential vulnerabilities or breaches.

Another group that can jeopardize data security is customers. Educate customers about data security, usage, and collection, and communicate what your institution does to keep customers' data safe. Build trust by providing accessible privacy policies, consent management, and user-friendly tools so customers can manage their privacy settings.

5. You've invested in leading-edge cybersecurity technologies

Attackers develop new tactics daily, such as creating mutating polymorphic malware that leverages gen AI to evade detection from traditional security tools. Gartner predicts that 25% of enterprise breaches will be traced back to AI agent abuse by 2028.¹⁷

You'll need more than a perimeter defense system and firewalls to combat nefarious AI agents. Access control and encryption are table stakes.

Plan on continuously investing in cybersecurity technologies to align with a comprehensive cybersecurity strategy that includes people, processes, and technology. Upskill employees responsible for cybersecurity.

Jayaraman recommends that financial institutions leverage privacy-enhancing technologies to analyze data using sandboxing or a walled garden. Consider homomorphic encryption, which allows computation on encrypted data without comprising encryption.

AI models are data-hungry, requiring vast amounts of training data. To improve data security, use federated learning and train models using local data on edge devices instead of exchanging client data with servers, says Jayaraman. Train AI models on decentralized data sets without sharing individual data points.

The end goal

The use cases for AI in financial services are exciting—and the number of use cases is growing quickly. While AI provides actual cost savings and competitive advantages, achieving those benefits depends on the integrity of the data that fuels AI models.

Financial institutions are often confident that some of their data is accurate, complete, consistent, and reliable, but having access to only some quality data creates blind spots that can derail the most well-thought-out strategies. You need to include structured and unstructured data, both digital and in physical documents, from throughout your organization in your decision-making.

A strong data foundation that includes a connected enterprise ecosystem, a strategy for managing physical and digital assets, risk governance, and technology investments to protect your institution from cyberattacks plays a crucial yet sometimes overlooked role in AI success.

¹⁷ www.gartner.com/en/newsroom/press-releases/2024-10-22-gartner-unveils-top-predictions-for-it-organizations-and-users-in-2025-and-beyond

About Iron Mountain

Iron Mountain Incorporated (NYSE: IRM) is a global leader in information management services. Founded in 1951 and trusted by more than 240,000 customers worldwide, Iron Mountain serves to protect and elevate the power of our customers' work. Through a range of services including digital transformation, data centers, secure records storage, information management, asset lifecycle management, secure destruction, and art storage and logistics, Iron Mountain helps businesses bring light to their dark data, enabling customers to unlock value and intelligence from their stored digital and physical assets at speed and with security, while helping them meet their environmental goals.

To learn more about Iron Mountain, please visit: www.IronMountain.com and follow @IronMountain on [X](#) (formerly Twitter) and [LinkedIn](#).