

# Staying Compliant with Private AI in Financial Services

Reaping AI-Fueled Innovation While Minimizing Security and Privacy Threats and Staying Compliant



Jerry Silva  
Program Vice President, IDC

## Financial Services Are the Biggest Investors in AI

Financial institutions globally are investing in technology and skill sets to implement AI, and generative AI as a subset of AI, to gain efficiencies, improve productivity, enhance customer and staff experiences, and innovate faster.

75%

of financial institutions are using AI technologies across the enterprise.

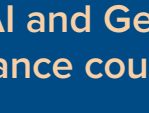
80%

of those report that they are currently using GenAI.<sup>1</sup>

IDC Financial Insights estimates that the **total investment in AI** by financial institutions topped **\$49 billion in 2024**

and is **growing** by over **30% annually**.<sup>2</sup>

The financial services industry (banking, insurance, and capital markets) **spends more on AI than any other industry worldwide**.



There is no doubt that financial institutions are expecting to get tremendous value from AI and GenAI, but concerns over security, data privacy, and compliance could limit the adoption of AI.

<sup>1</sup> Source: IDC's *Global AI (including GenAI) Buyer Sentiment, Adoption, and Business Value Survey*, October 2023

<sup>2</sup> Source: IDC's *Worldwide AI and Generative AI Spending Guide*, 2024

## Real Business Benefits of AI and GenAI

Nearly **90%** of financial institutions are able to **measure the business value of their data**, which is a key fundamental aspect of leveraging AI and GenAI.<sup>3</sup>

Approximately **37%** of institutions report that their GenAI-related launches met **60% or more of their business expectations and KPI metrics**. The same number reported that **their GenAI launches met 80% or more of their KPIs for success**.<sup>4</sup>

The top 5 business areas cited by institutions that are disrupting their competitive position or business model are:



<sup>3</sup> Source: IDC's *Future Enterprise Resiliency & Spending Survey Wave 7*, July 2024

<sup>4</sup> Source: IDC's *Future Enterprise Resiliency & Spending Survey Wave 4*, April 2024

## Security, Data Sensitivity, and Compliance Affecting AI Adoption

As a regulated industry, financial services are required to maintain trust with their customers and compliance with local regulations.

Security (56%)

Data sensitivity (51%)

were the leading factors that financial institutions worldwide cited in determining whether a workload or application would move to public cloud.<sup>5</sup>

Approximately **20%** of financial institutions are using IT governance (including cloud governance) to manage their AI risk, the number 1 capability at the institution being leveraged to govern AI.<sup>6</sup>

Existing regulations on the use of data are being augmented to further protect customers from bias in AI modeling.

(Existing regulations: the EU's General Data Protection Regulation [GDPR], the Financial Modernization Act of 1999, the Digital Operational Resilience Act [DORA] in the United States, and the Personal Data Protection Act [PDPA] in Singapore)

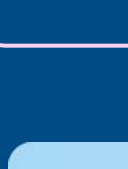
<sup>5</sup> Source: IDC's *Worldwide Industry CloudPath Survey*, April 2023

<sup>6</sup> Source: IDC's *Future Enterprise Resiliency & Spending Survey Wave 7*, July 2024

## How AI and Cloud Can Safeguard Institutions

Financial institutions are experiencing improvements in security and compliance from modern technologies.

As a result of creating enterprise AI policies and governance, financial services institutions are protecting against:



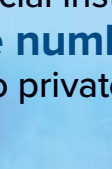
Security breaches



Regulatory risk



Exposing customer data



Damage to brand reputation



Liability concerns

According to financial institutions, **improved IT security was the number 1 realized benefit** from migrating applications to private and public cloud.<sup>7</sup>

34%

Moving to private cloud

28%

Moving to public cloud

Around **51%** of institutions are using, or plan to use, GenAI to **improve security** in the next 12 months.<sup>8</sup>

Approximately **46%** of institutions are using, or plan to use, GenAI to **improve fraud detection and mitigate risk** in the next 12 months.<sup>8</sup>

<sup>7</sup> Source: IDC's *WorldWide Industry CloudPath Survey*, April 2023

<sup>8</sup> Source: IDC's *Industry Tech Path Survey 2024*, August 2024

## Considering Private GenAI

The goal in financial services is to increase the pace of innovation while maintaining trust.

In order to reap the rewards of AI and GenAI in financial services, private AI has the potential to:



**Provide control over sensitive data.**

This means that **any data** subject to privacy regulations or that may be the cause of undue risk or threats from bad actors **remains under the control of the institution**, even in a distributed AI environment where other aspects are not local or on premises.



**Protect competitive differentiation.**

In an industry such as investment banking, **analytics are complex and are protected as intellectual property that provides competitive differentiation**. Under these circumstances, keeping data and models local and under the direct control of the institution is not a "nice to have" but rather is critical to the success and longevity of the institution.



**Achieve scalability and resilience**

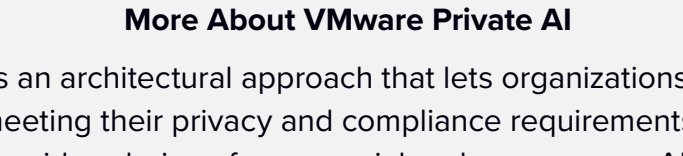
**Private AI provides scalable and resilient infrastructure** to meet the needs of financial services and insurance. Institutions must be able to seamlessly handle growing workloads and maintain uninterrupted services, even during periods of high demand.



**Enable collaboration with control.**

Although **private AI** can lock down access to sensitive data and models from outside the organization, it **allows for an environment of collaboration within the institution using model galleries**. Along with robust access control, these galleries help maintain a controlled, collaborative environment while giving each line of business flexibility to choose the AI models or services best for their needs.

## Message from the Sponsor



### More About VMware Private AI

VMware Private AI is an architectural approach that lets organizations unlock the business gains of AI while meeting their privacy and compliance requirements. It is a privacy-first approach to AI that provides choice of commercial and open source AI models and services.

[Click here to learn more](#)