

Executive Summary

Leadership Exchange for Financial Services

June 17, 2025

kyndryl[®]



Overview

In this exchange, CIOs and CTOs from leading financial services organizations discussed critical challenges and perspectives on cloud sovereignty, strategic cloud adoption, and artificial intelligence (AI) implementation within the financial services sector. The conversation underscored the complex digital transformation landscape, emphasizing the need for robust controls, adaptable strategies, and informed decision-making amid evolving technological and geopolitical risks.

Host/SME

Andre Putter
Vice President,
Head of Solutioning, Kyndryl

Dipa Velagapudy
Vice President,
Cloud Practice Leader, Kyndryl

Key topics

PAGE

- 03 Cloud Sovereignty: A Multifaceted Imperative
- 04 Strategic Approaches to Cloud Adoption
- 05 Foundations and Challenges in AI Implementation

Cloud Sovereignty: A Multifaceted Imperative

- Dipa Velagapudy outlined a framework based on four core principles, emphasizing that true sovereignty requires addressing each area, not just isolated controls like common encryption. This framework includes data sovereignty (safe transfer, location, integrity, retention), technical sovereignty (encryption, micro-segmentation, air-gapped systems), operational sovereignty (skill management, third-party access, incident handling), and assurance sovereignty (zero trust, disaster recovery, auditability of workloads).
- Participants agreed that the priority of addressing challenges presented in the framework, particularly around data access, ownership, and control, was accurate and mirrored their own organization's painful experiences in ensuring third-party controls.
- Despite claims by some public cloud providers that encryption alone ensures sovereignty, participants stressed that network providers remain a risk. Building truly air-gapped systems is extremely difficult when connectivity to the cloud is required, posing a complex problem without an easy solution.
- Implementing all necessary controls for full cloud sovereignty is expensive. Organizations should therefore assess which workloads truly require 100% sovereignty versus those that can operate with fewer controls, balancing security with cost.

Cloud sovereignty is a concept with diverse interpretations, necessitating a comprehensive framework for effective implementation.

Perspectives on Sovereign Cloud

[Learn more](#)

Strategic Approaches to Cloud Adoption

- | | | |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none">- Cloud adoption is deemed inevitable, with participants urging organizations to stop resisting and instead focus on how they will embrace it in a way that aligns with business needs. This is particularly true as certain providers like Microsoft incentivize cloud use through licensing and product roadmaps that favor cloud versions of software products.- Following a penetration test, one organization discovered that its primary cloud platform posed the greatest security risk, leading to immediate mitigation efforts including micro-segmentation and encryption.- While executive committees acknowledge the importance of resilience and controls, securing funding for environmental strengthening remains a difficult internal discussion. Nevertheless, the Digital Operational Resilience Act (DORA) has helped allocate some budget for vulnerability assessments | <p>and third-party risk management, though it also uncovered additional needs.</p> <ul style="list-style-type: none">- A critical challenge is the slower pace of mindset change within technology teams compared to the rapid evolution of risks. Tabletop exercises and penetration tests are effective methods for early vulnerability identification and for educating personnel, helping to shift perspectives on security.- A significant challenge in cloud environments is managing the supply chain, a lesson reinforced by recent global events. Organizations must develop robust plans for managing suppliers, assessing risks, and devising clear exit strategies, even if complete portability is not feasible. | <ul style="list-style-type: none">- To mitigate vendor lock-in and foster competition among providers, many large organizations choose to implement a multi-cloud strategy, utilizing two or even three cloud providers. This approach, while requiring significant internal resources and diverse skill sets, can lead to more favorable pricing and greater control over service agreements.- To maintain control and ensure potential portability, it is crucial to avoid fully adopting a single cloud provider's native toolchain for critical functions such as security, configuration posture management, application monitoring, security event management, release pipelines, and especially key management. This strategic decision allows organizations to retain flexibility and mitigate vendor dependence. |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Embracing cloud technology is becoming unavoidable for many organizations, necessitating careful strategic planning and continuous adaptation.

Foundations and Challenges in AI Implementation

- AI sovereignty is a broad concept that extends beyond data, encompassing an organization's entire infrastructure, workforce, and the complete AI lifecycle, from model training to deployment and use. One member suggested that every country should consider establishing its own sovereign AI cloud, but the reality of immense investments in infrastructure and workforce development is a significant obstacle.
- AI is a significant driver for cloud adoption, as the necessary processing power and advanced solutions are often not feasible to implement on-premise. This pushes organizations, even hesitant ones, towards cloud environments.
- Organizations often face internal resistance, with some advocating for on-premise AI capabilities and others

prioritizing rapid cloud adoption for business value, acknowledging that many AI projects may not yield tangible results. To accelerate exploration, some organizations are enabling access to multiple AI platforms and models (e.g. Bedrock, Vertex, Copilot, Gemini) in the cloud to quickly test business cases.

- Effective data governance is foundational for successful AI implementation. AI models are only precise when fed well-structured and properly formatted data, which often requires significant effort to revisit and prepare existing content, especially unstructured data like manuals or FAQs.
- Early successes with internal AI applications, such as chatbots for call centers or OCR for invoices, have

created an appetite for adoption within organizations. However, they have also exposed the need to strengthen access controls and data architecture. This highlights that while business demand for AI is not yet overwhelming, it is expected to grow rapidly once the benefits become evident.

- A significant challenge is managing often “unjustified expectations” that AI can serve as a panacea for all problems. These expectations lead to inflated initial budgets and projects that fail to deliver expected outcomes. Organizations must, therefore, focus on validating use cases that demonstrate real value, whether through customer service improvements or cost savings, to ensure responsible and effective AI adoption. AI literacy training for users is also crucial to maximize the effectiveness of AI tools like Copilot.

Implementing AI solutions requires substantial foundational work, particularly concerning data governance and the management of organizational expectations.



The Leadership Exchange for Financial Services is hosted by Kyndryl. Please contact Andre Putter or Dipa Velagapudy with any questions about Kyndryl or this Exchange.

© Copyright Kyndryl, Inc. 2025

Kyndryl is a trademark or registered trademark of Kyndryl Inc. in the United States and/or other countries. Other product and service names may be trademarks of Kyndryl Inc. or other companies.

This document is current as of the initial date of publication and may be changed by Kyndryl at any time without notice. Not all offerings are available in every country in which Kyndryl operates. Kyndryl products and services are warranted according to the terms and conditions of the agreements under which they are provided.