Executive Summary

Thought Leadership Exchange for Financial Services

March 11, 2026

kyndryl

Overview

In this session, Kyndryl brought together senior technology leaders from major global financial institutions to discuss the sector's top operational and regulatory priorities. The conversations were focused on three areas: achieving DORA-aligned operational compliance, managing stringent data sovereignty requirements through private cloud architectures and enforcing robust governance across AI and third-party software ecosystems.

Host/SME

Stewart Hyman
Kyndryl, Chief Technology Officer for Strategic Markets

Key topics

Operational resilience and third-party risk management

- Financial institutions implement continuous governance structures and rigorous contract negotiations to maintain compliance with DORA regulations across vendor networks.

- Executives agreed that achieving DORA compliance requires a continuous governance model rather than a static endpoint. One participant noted that an organization can slip out of compliance overnight, requiring permanent operational frameworks. These frameworks must consistently monitor processes and manage technical debt to pass annual audits.

- Third-party and fourth-party risk is the dominant challenge. Across banks and providers, the hardest problems are contract remediation, SLA/KPI enforcement together with visibility into critical suppliers and their subcontractors, while regulators increasingly expect end-to-end accountability.

- Leaders emphasized the difficulty of enforcing resilience standards throughout their supply chains, particularly with smaller vendors. Participants shared that updating contracts to include strict service agreements remains a massive undertaking. This process requires dedicated internal teams to negotiate and monitor third-party relationships constantly.

- Participants identified managing their primary vendors' suppliers as a significant compliance hurdle. Companies acting as intermediaries must review every downstream subcontract to ensure regulatory adherence. As a result, financial institutions are implementing stricter criteria to limit the number of officially classified critical vendors.

- The group discussed the importance of using structured incident reporting and crisis management playbooks during cyberattacks. One executive shared that conducting simulated tabletop exercises greatly improved their team's readiness. This practice empowered them to communicate transparently with regulators during sensitive breaches.

- Executives debated the lack of a standardized industry taxonomy for defining critical business functions under new regulations. What one institution considers a critical step in the process may differ significantly from another's view. This misalignment creates challenges for regulators when assessing compliance, as institutions may be marked as compliant or noncompliant despite operating under different definitions and thresholds.

Choosing a partner already operating under regulatory scrutiny comparable to their own helps reduce compliance effort for financial institutions and increase confidence in the resilience of the services they rely on. As a designated Critical Third-Party Provider (CTPP), Kyndryl is directly overseen by the European Supervisory Authorities (ESAs) to ensure our robust risk management, governance and resilience practices meet their expectations.

Building digital trust for financial institutions

Learn more

Cloud sovereignty and infrastructure repatriation

- To mitigate geopolitical risks and ensure operational control, leaders are increasingly reshaping their cloud strategy through the lens of sovereignty.

- Participants framed sovereignty across data, operational, and technological dimensions, driving strategies such as encryption-before-cloud, vendor-agnostic architectures, private or sovereign cloud options and the selective repatriation of workloads from SaaS and public cloud to regain control.

- Participants categorized their sovereignty concerns into securing data privacy, maintaining operational control against external interference and avoiding technology provider lock-in. An infrastructure executive noted that global conflicts have made public data centers visible targets. This realization drives organizations to develop private cloud environments to conceal and protect sensitive operations.

- To avoid dependency on any single provider, executives shared strategies for building automated, vendor-agnostic infrastructure. One banking representative detailed how utilizing container technologies allows their organization to provision workloads across different environments.

- Financial regulators are increasingly scrutinizing how organizations back up their data using foreign technology platforms. A participant explained that local banking authorities required their institution to implement custom encryption checkpoints before sending backup data to the Azure platform. This architectural change ensures the hosting provider can never access the information.

- Leaders operating in politically sensitive regions stressed the necessity of localized hardware redundancy. One member explained that they distribute independent software and hardware instances across multiple safe locations. This strategy guarantees uninterrupted financial services during extreme scenarios involving total geopolitical isolation.

- Several organizations are actively reversing their initial transitions to public clouds due to highly restrictive service conditions. A technology leader shared that their institution is returning to on-premises solutions because public platforms force unwanted operational changes. This intentional shift reflects a broader industry desire to restore absolute operational control.

"As digital sovereignty becomes more prevalent, enterprises may increasingly be required to repatriate data to regionally based public clouds, data centers or servers."

- Kris Lovejoy, Global Head of Strategy at Kyndryl

In an uncertain world, enterprises are repatriating their data

Learn more

AI governance and software independence

- Driven by concerns about data leakage, several executives reported imposing strict constraints on the use of public artificial intelligence tools. Participants emphasized that the immediate risks to corporate data sovereignty outweigh the potential operational efficiency gains. Consequently, many financial institutions are formally pausing the widespread adoption of these external technologies.

- To safely harness emerging technologies, organizations are building proprietary, internal artificial intelligence engines. One leader shared that they systematically route all employee interactions through a highly designed to secure, custom-built portal. This enclosed infrastructure completely isolates institutional data from external systems and easily meets the strict tracking requirements set by regulators.

- Participants expressed growing unease with their deep operational reliance on comprehensive and ubiquitous software services. Organizations are intentionally initiating strategic projects to move away from these dominant providers. To regain strategic independence, institutions are developing core applications in-house or utilizing on-premises software alternatives.

The Kyndryl Agentic AI Framework is an approach that empowers organizations to be truly AI-native. It reimagines workflows, scales AI throughout operations and integrates agents into an upskilled workforce.

Learn more

kyndryl

The FSS Leadership Exchange is hosted by Kyndryl. To learn more or to become a member of this community, please connect with Stewart Hyman on LinkedIn or send an email at stewart.hyman@kyndryl.com.