Utilising Third-Party Technology Products & Services to Boost the Operational Resilience of Investment Banks

Despite experiencing unprecedented circumstances in 2020, financial institutions are required to remain compliant with regulatory mandates that were designed for quite different operational conditions. Since the onset of the COVID-19 pandemic, banks have worked to maintain business-as-usual for customers, while operating remotely for long periods, and teams tasked with ensuring banks' operational resilience are confronted with a range of unforeseen challenges. This article explores how financial technology vendors have responded.

The Rise of Managed Services

The patchwork of in-house and vendor-provided solutions that evolved in many banks since the inception of digitalisation led to complex cross-enterprise interdependencies that mean they are struggling to operate smoothly given the now mostly distributed workforce. Put bluntly, the rapidly implemented workarounds that were put in place to enable firms to ensure continuity of service at the onset of the pandemic are, in many cases, not fit for purpose in the long run.

As the world comes to terms with the fluidity of this new normal with dynamic government-issued demands on location of the workforce, banks see the appeal of cloud-based managed services and the flexibility that they provide makes this operating model attractive. Indeed, banks are looking to cloud and other technology solutions to help them meet the high-quality data and reporting standards required by regulators and to improve the performance of their businesses despite the fluid circumstances.

In parallel, UK regulators are focusing on ensuring that third-party vendor-managed services do not impact operational resilience. GreySpark expects to see regulators place more stringent requirements on banks to ensure that both they and their service providers are resilient to adverse conditions.[1]

Financial Technology Vendors to Assist

Much has already been written since March 2020 about the challenges that national and local lockdowns of varying severity levels are having on the financial sector, and the pain points are now well understood. In light of the operational changes financial services firms are facing, vendors are responding by bolstering their offerings to provide the additional support that banks need to address the current challenges. Most operational issues stem from the inability of bank staff to work in their usual environment, and this has led to five challenges for financial institutions:

- Reduced access for personnel to key on-premises enterprise systems;
- Restrictions on travel limit selling and launching of new services in other geographic regions;
- Limitations on the physical monitoring of personnel;
- Significantly less face-to-face intra-team collaboration; and
- Increased supplier risk in the uncertain macroeconomic environment.

Unsurprisingly, vendors are working hard to help banks address these challenges and ensure that they maximise customer retention in these turbulent times.

Reduced Access for Personnel to Key On-premises Enterprise Systems

Over the last couple of years, the digitalisation of trading workflows and processes has allowed banks to make leaps forward in terms of their overall performance by increasing operational efficiency and lowering costs. The efforts to digitalise trading across asset classes will pay further dividends, as banks the groundwork for the introduction of artificial intelligence (AI) to enhance performance and reduce human touchpoints further. Artificial Intelligence has been a hot topic in the financial services for several years without much actual deployment in live production environments. However, the industry has reached a tipping point where tangible solutions are now available to banks.

AI solutions can support the demands of e-trading markets by combining AI-enabled decision-making tools and dynamic markets access. Indeed, AI is expected to allow banks to automate up to one-third of their processes; replacing time-intensive manual processes with automated processes and notifications, removing delays and eliminating human error, as well as enabling early risk assessments and responses that reduce the number and cost of regulatory non-compliance incidents. In a nutshell, AI may reduce the dependency on human integration with many operational aspects of financial institutions, negating the risks associated with a dispersed workforce.

[1] FCA, 2020. *Outsourcing and Operational Resilience.* [online] FCA. Available at: <https://www.fca.org.uk/firms/outsourcing-and-operational-resilience>

Restrictions on Travel Limit Selling & Launching of New Services in Other Geographic Regions

Almost all banks have utilised the offerings of cloud service providers for assist with parts of their overall operation. The remaining reticence to move systems that are critical to the business off premises was suddenly overturned with the onset of the pandemic. With staff not able to physically travel and face-to-face interactions no longer being the norm, cloud platforms were able to provide tools that gave back to banks the ability to launch new products and sell into new markets regardless of the location of the prospective clients.

In particular, vendors with cloud-native solutions have had a head start in adapting to the change of circumstances, and those banks that utilise their products have benefited from it. Vendors with enterprise solutions and fledgling cloud versions are having to significantly invest in collaboration and workflow technology in order to remain competitive.

Limitations on the Physical Monitoring of Personnel

Pre-pandemic, the monitoring of staff in banks, focused on two areas: online activity and physical activity. Limitations were placed on behaviours – a well-known example being that staff were not allowed to bring mobile phones onto the trading floor, but there are many others. Since remote working has meant that physical monitoring is not possible at all, the need to achieve more accurate detection of malfeasance online is critical.

Technology to detect insider trading, collusion and other non-compliant behaviour in real-time would enhance the accuracy of online monitoring, and vendors are working to help banks more successfully weed out false positives from their alert lists. Machine learning is being used to rank every communication by risk based on how a team has coded prior alerts, and natural language processing is increasingly being used to identify language that suggests inappropriate behaviour by front-office staff. A number of vendors have adopted this approach and are also building new features and functionalities for their clients, and these can include the use of bots and automation to improve everyday workflows for compliance staff.

> **“Artificial Intelligence has been a hot topic in the financial services for several years without much actual deployment in live production environments.”**

Significantly Less Face-to-face Intra-team Collaboration

Prior to the pandemic, teams sat together in offices to facilitate collaboration and knowledge sharing. With the financial services industry operating remotely, communications vendors witnessed a boom in the use of collaboration tools such as Microsoft Teams, Slack and Zoom. Banks can provide a more collaborative environment using such tools for everyone from operational staff to traders.

Since the beginning of the outbreak, use of Zoom surged by 50%.[2] Many teams opted for free-use packages to enable them to collaborate with team colleagues, but this made it almost impossible for firms to meet their monitoring requirements. Even for those who have fully-integrated collaboration tools, the vast number of employees using them outside of a controlled office environment has made it substantially harder to meet compliance requirements.

[2] CNBC, 2020. *Zoom shares pop after users grow from 200 million to 300 million in a matter of days.* [online] CNBC. Available at: <https://www.cnbc.com/2020/04/23/zoom-shares-pop-after-users-grow-from-to-300-million.html>

To help create a secure and compliant communication channel, a number of vendors are upgrading their own communication mechanism to combine conventional chat, voice and video conferencing onto one platform in an effort to replace traditional communications (Outlook, Skype, Bloomberg Chat). An encrypted chat-based collaboration tool would allow users can send messages, share files, automate trade flows and meet in real-time, and securely archive, retrieve and control interaction records for compliance purposes.

Collaboration tools are not just important for internal teams; this recent change in business workflows has seen increased focus on automation and electronic communication to external clients too, and solutions such as Symphony are creating financial services communities have stepped further into the spotlight in recent months, not only for communication and messaging, but also for the support of full end-to-end workflows and services.

Increased Supplier Risk

The COVID-19 pandemic has exposed the fragility of supply chain ecosystems. Failings in due diligence, whether at supplier onboarding stage or with ongoing third-party risk monitoring, have become increasingly apparent. A recent survey showed that, in financial services sector, 40% of third-party relationships have not been subjected to due diligence checks.[3] Banks and other financial services firms are highly reliant upon third-party suppliers, and the need to closely monitor and manage risks linked to the suppliers' financial health in order to identify hidden dangers is becoming more apparent in 2020. Indeed, supplier, distributor and partner management has never been greater than it is today.

Vendor risk management systems with features and tools that can manage vendor risk, ensure compliance and improve the effectiveness of a bank's third-party risk management programme, not just at onboarding but also across the entire vendor lifecycle, are being enhanced by product management teams in fintech firms. Enhancements include in-built automated alerts to notify banks when vendor risk goes beyond acceptable thresholds, so that they can proactively take appropriate and timely measures to address it.

Firms to Consider Technology Solutions for the Future

The current crisis has renewed the focus by financial services firms on the maintenance of their own operational resilience, and vendors with solutions that can assist them are reinvigorated. Both product and sales teams have no better market to generate interest in their wares. Financial services firms must ensure they can maintain business-as-usual while staff operate remotely, and this means shoring up their platforms, tools and infrastructure. If the case was not made in previous years, today it is clear to many that AI and cloud technology lay the foundations for strong operational and business resilience and enable financial institutions to achieve more with less.

[3] Refinitiv, 2020. *The Real Risks: Hidden Threats Within Third-Party Relationships.* [online] Refinitiv. Available at: <https://www.refinitiv.com/content/dam/marketing/en_us/documents/reports/hidden-threats-within-third-party-relationships-2020.pdf?utm_source=Solutions&utm_medium=Blog&utm_campaign=270181_RefinitivPerspectiveBAU2020&elqCampaignID=11586>