SPOTLIGHT

Sponsored by: Splunk

While new technologies such as generative AI are promising to transform the institution's capabilities, this technology will not survive, much less thrive, if the proper controls aren't in place to ensure continued compliance and security

Business Benefits for Banks Investing in Resiliency

June 2024

Written by: Jerry Silva, Program Vice President, IDC Financial Insights

Introduction

Financial services is a heavily regulated industry, and this can make it difficult to move as quickly as financial institutions would like. They must address the constantly increasing customer demands, battle competitive pressures (especially from less-regulated players such as some fintechs), and keep costs down, all while maintaining regulatory compliance, operational resilience, and security. Responding to market and customer demands while maintaining digital trust is a key factor in an institution's brand, reputation, and success in the market.

The regulatory environment shows no signs of slowing down as global regulatory bodies address resiliency and security in the financial services industry. Regulatory bodies focusing on these factors and some recently implemented requirements include but are not limited to:

- Digital Operational Resilience Act (DORA) (European Union)
- The Prudential Regulation Authority (PRA), Financial Conduct Authority (FCA), and Bank of England (United Kingdom)
- The Australian Prudential Regulation Authority (APRA)
- The Monetary Authority of Singapore (MAS)
- The SEC Cybersecurity Rule of July 2023 (United States)
- The Office of the Superintendent of Financial Institutions (OSFI) (Canada)

AT A GLANCE

KEY STAT

Security, risk, and compliance are the capabilities most immune to budget cuts at financial institutions worldwide. However, with the increased focus on technologies such as AI, 74% of those organizations cite security concerns as their largest challenge to data operations.

KEY TAKEAWAY

Security, risk, and compliance are the most fundamental capabilities for financial services institutions. But technology imperatives — such as digital infrastructure expansion, generative AI (GenAI), and the struggle to find IT talent — are putting pressure on the institution's ability to maintain resilience, security, risk, and compliance.

In fact, security, risk, and compliance were cited by 28% of banks as the most immune area to budget cuts by banks worldwide, which was the top response (source: IDC's *Future Enterprise Resiliency and Spending Survey, Wave 2,* February 2024; n = 68 banks). So how can banks balance the market's needs with compliance to increasingly tighter regulatory scrutiny? While some believe that regulations may distract from the bank's ability to invest in innovation, IDC believes that investments in both operational resiliency and cyber-resiliency will have real business value and augment the institution's brand and customer experience excellence.

Trends

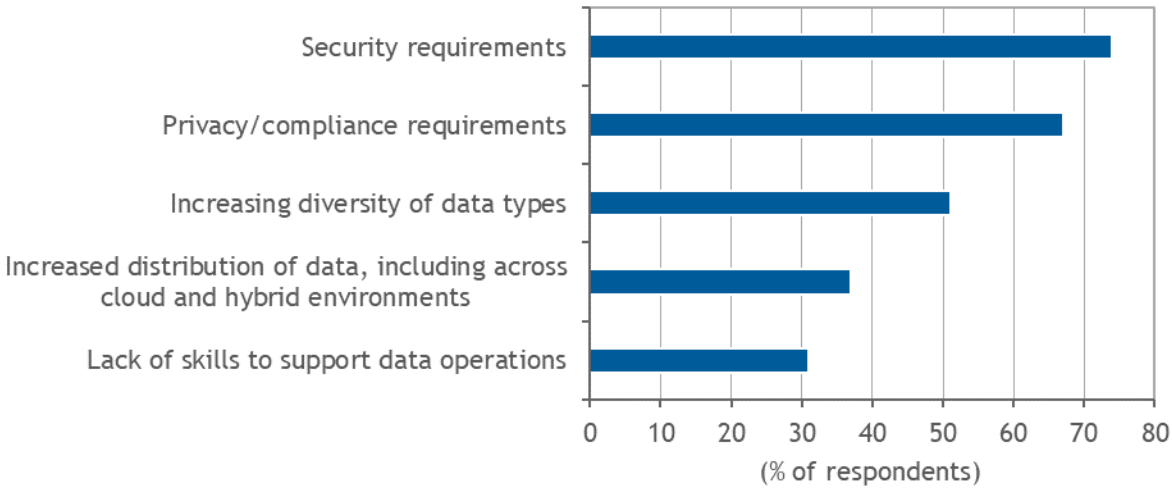
The complexities of modern architectures inherently increase risks by adding more points of vulnerability in the environment, changing the development and support organizations at the institution, and potentially increasing the number of vendors and tools brought in with every new component. This makes it increasingly difficult to address resilience and security. In detail:

- The expanding digital infrastructure (i.e., on premises, cloud, third-party partners, networks, and edge) creates an increasingly challenging environment that can be difficult to manage centrally. In IDC's April 2023 *Worldwide Industry CloudPath Survey* (which surveyed 70 banks worldwide), IT governance, security, difficulty with centrally managing IT systems, lack of IT skills, and integrating cloud services were listed as the top 5 concerns that banks had in adopting the cloud.
- Solving for siloed data stores and the need to expand the data infrastructure can challenge a bank's progress toward digital business. Banks have historically had data sources uniquely tied to their specific systems based on diverse lines of business. Modern data strategies need to overcome this challenge as well as create an open environment that can bring in external alternative data to drive better decision making. IDC calls this "enterprise intelligence," a strategy and an architecture that acknowledge a "data everywhere" environment and whose goal is to improve decision velocity, accuracy, and fairness at the institution.
- The move to AI, machine learning (ML), and GenAI makes the data challenge even more acute. Whether ensuring that models are explainable and avoid bias or creating and/or using large language models on which to base GenAI models, banks are challenged to ensure that data platforms maintain compliance and security.
- Industry ecosystems, which include open and embedded finance while expanding the ease of financial services delivered to customers, self-evidently create uncertainty in compliance and security among all participants in any individual ecosystem.
- Finally, as a bank continues to operate while it transforms into a digital business, the need for skilled workers in new areas and to support legacy operations becomes more complex, potentially leading to multiple operational processes, tools, and performance metrics. Staffing was the top risk factor identified by financial institutions in a recent IDC survey (source: IDC's *Future Enterprise Resiliency and Spending Survey, Wave 2,* February 2024; n = 68 financial institutions). This disparity between support and development staff at the institution can expose weaknesses and compliance challenges in creating a resilient organization.

IDC believes that solving the data challenges is fundamental not only to the institution's operational resilience and cyber-resilience, but to its business success as well. But financial organizations are still challenged in transforming their data operations (see Figure 1).

FIGURE 1: ***Data Operation Challenges***

Q ***Which of the following have been the biggest challenges in the implementation of data operations solutions at your organization?***



n = 100 financial institutions in North America

Source: IDC's North America Banking Technology Survey, November 2023

Business Benefits

By creating value from existing and alternative data and leveraging the power of cloud, while addressing both operational resilience and cyber-resilience, banks can improve every aspect of their business, including the following:

- Customer experience benefits can from improved availability and responsiveness across every channel through which the customer interacts with the institution. This is especially true for larger, mission-critical relationships that the institution has with their business customers.
- Improved access and speed to available data will improve the institution's ability to detect and prevent financial crime before it has a detrimental effect. This ability improves the detection of not only transactional fraud such as payments but also fraud from non-real-time processes such as lending, KYC, and AML.
- Continuous business innovation can only happen if the data architecture is agile enough to allow for the development of new products and services while automatically addressing the fundamental concerns of security, resilience, and compliance. This capability opens the door to faster time to market and efficiency for new offerings.
- Regulatory compliance, particularly in operational resilience and cyber-resilience, can become second nature through automation. Executing a resilience strategy that adapts to market changes and the bank's own strategies frees the bank to focus on the business of financial services.

In addition to the business benefits previously mentioned, creating such an enterprisewide, scalable, and secure technology environment through operational resilience and cyber-resilience should be the goal of the financial institution. This is especially true as the institution moves to deployment models such as the cloud, improved data architectures, and advanced AI platforms to increase the institution's business agility in a fast-moving market. To do this, a focus on observability and response to operational disruptions, using automation to minimize the human impact on the organization, is critical to digital transformation. The bank's digital infrastructure should approach intelligent and autonomous operations, based on the individual characteristics and risk profile of the specific institution. In most cases, this requires close partnerships with services, infrastructure, and software providers that can, under the bank's governance, simplify the operational resilience and cyber-resilience stance of the institution while allowing the bank to focus on solving the business and financial needs of its customers.

Technology or Vendor Profile

San Francisco–based Splunk was founded in 2003 to support financial institutions' goals to become more digitally resilient as new technologies challenge their ability to maintain security, compliance, and risk. The company focuses on the financial services industry with a suite of security, observability, and data management solutions meant to address the unique challenges that financial institutions face, including:

- Financial crime and fraud
- Compliance
- Customer experience

Splunk uses advanced analytics and ML capabilities that can enable real-time detection and prevention of fraudulent activities and financial crimes. The platform enables financial services organizations to streamline compliance processes, meet stringent regulatory requirements, and minimize the risk of penalties. In addition, Splunk's solutions aim to help financial institutions gain insights into customer behavior, enabling them to deliver personalized experiences and drive loyalty. The company has over 1,100 patents and is driven by a culture of innovation. The company's mission is to build a safer and more resilient digital world by helping security, IT, and engineering teams in financial services keep their organizations secure and reliable.

Cisco acquired Splunk in 2024, strengthening its ability to help financial services organizations build resilience across their entire digital footprint. Splunk's client base includes many of the world's largest financial services organizations, supporting their need to keep their mission-critical systems secure and reliable.

Challenges

Many technology providers have sprung up to support the institution's drive toward better data management, resiliency, and security using different approaches. But IDC believes that these companies, including Splunk, potentially face a number of challenges specific to the financial services industry, including:

- Perhaps the largest challenge to solving the data modernization problem is the siloed nature of the institution's technology and organization. The business side of the organization is especially challenging — given that the institution's goal is to overcome technology silos — in that there often isn't consensus within the lines of business about the value of a data management solution and the value it can bring across the whole enterprise. It is

challenging to gather investments from the individual line-of-business leaders for an enterprisewide platform, making it difficult for any vendor to penetrate the whole organization, even that vendor that has the right technology to solve for data security and resilience.

- Changes in regulations, particularly in areas such as resilience and risk, are coming faster and faster. The financial institution isn't always able to keep up with and respond to new requirements, thus placing some of that responsibility on the solution provider and forcing that partner to take on at least some of the work in anticipating and responding to new regulations. Many technology providers have created subgroups within their own organizations to track regulations and provide advisory services and anticipate regulatory changes in their own road maps instead of waiting for the institution to ask for new functionality to comply to new regulations. This means investments in people and research that don't have a direct financial benefit to the vendor.
- Modernizing both data and data management is hard. As the size of the financial institution grows, the data environment becomes more and more complex, including not only the institution's own data but also all external data that the organization needs to maintain and grow its business. This requires the technology partner to maintain strong groups within its own organization that can support education, compliance, architecture, and service delivery, which, in turn, places pressure on the technology provider to focus as much energy on its internal capabilities as its customer.

IDC believes if Splunk can address the last two challenges, arguably the easiest of the three, it can respond effectively to the institution's need to continue its path to innovation without the threats of compromised security, risk, and compliance. However, the environment of siloed business at the institution means, at best, that the sales cycle at the institution will be long and will require patience and persistence to prove to the institution that the enterprise approach to Splunk's platforms are the path forward, and, at worst, that Splunk is unable to capture more than a single or few line-of-business solutions. This, in itself, would be a recommended path for Splunk as it deploys at any individual institution — proving the platform's worth in a single instance while maintaining its enterprise capabilities to fit into the institution's enterprise architecture and proving value across the organization.

Conclusion

There is so much technological change going on today that it is challenging the financial institution to focus on customer experience and product innovation. While new technologies such as GenAI are promising to transform the institution's capabilities across all lines of business, this technology will not survive, much less thrive, if the proper controls aren't in place to ensure continued compliance and security to minimize the risks of these platforms.

As with many new technologies and the challenges that financial institutions face with technology implementation within the realities of security, resiliency, and compliance, partnerships with domain expertise and solid platforms are critical in the continued success of the institution without threats to its risk.

Technology providers such as Splunk are positioned to support the financial organization in both focusing on solving the challenges of security, resilience, and compliance and allowing it to continue to focus on the business of financial services through continuous innovation, while maintaining digital trust and stewardship on behalf of all of its customers.

While new technologies such as GenAI are promising to transform the institution's capabilities, this technology will not survive, much less thrive, if the proper controls aren't in place to ensure continued compliance and security.

About the Analyst

Jerry Silva, *Program Vice President, IDC Financial Insights*

Jerry Silva is vice president for IDC Financial Insights, responsible for the global retail banking practice. Jerry's research focuses on technology trends and customer expectations and behaviors in retail banking worldwide. He draws on 40 years in the financial services industry to cover various topics, including digital infrastructures, cloud, AI/ML, workforce optimization, security and fraud, operations automation, enterprise mobility, and payments.

MESSAGE FROM THE SPONSOR

Building Digital Resilience in Financial Services

Financial service institutions are some of the most data-intensive and heavily regulated organizations and are subject to heavy fines for noncompliance. They are also the target of many of the most sophisticated cyberattacks, and much of the world economy depends on financial service institutions staying up and running despite escalating disruptions. The resilience of their digital systems is critical to building a safer and more resilient digital world.

Learn more about the top threats in financial services.

www.splunk.com/fsi

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com