What banks need to know about the Fed's new Banking as a Service supervisory program

EY
Building a better working world

Federal Reserve Novel Activities Supervision Program: enhanced oversight of Banking as a Service relationships

The Federal Reserve (Fed) announced in a recent Supervisory and Regulation Letter (SR 23-7) a new supervision program targeting higher-risk, novel activities banks are undertaking. The Novel Activities Supervision Program aims to provide enhanced supervision of banks engaging in, among other activities, "complex, technology-driven partnerships with non-banks to provide banking services."[1] These partnerships allow FinTechs the ability to offer deposit and/or lending products to their customers using a bank's infrastructure and licensing, and banks to provide new and innovative products to a wider array of customers through the FinTech. These arrangements are often referred to as Banking as a Service (BaaS).

The Fed released its notice on the heels of interagency third-party risk management guidance released in June, which addressed risks related to bank-FinTech (or BaaS partner) relationships.[2] Notably, the Fed's letter makes no reference to a bank's asset size as a qualifier for this supervision program and demonstrates the Fed's understanding of BaaS partner business models. Due to transaction-based revenue opportunities (particularly for banks with less than $10 billion in assets), risk related to BaaS partner relationships typically outpaces balance sheet growth. Under this model, a bank can more accurately measure its risk profile by examining risks related to its specific products and the number of households it serves.

The program will augment the Fed's existing supervision and examination approach by providing additional expertise and supplementary examination procedures, rather than replacing current structures. Banks included in the program should expect to receive a written notice from the Fed.

The Fed's message is clear: Federal regulators view the delivery of financial services through BaaS partnerships as differentiated from traditional banking to the point of requiring a new playbook. In its announcement, the Fed indicated it would also be publishing new guidance targeted at banks engaging in this activity. Banks should take note. Recent examinations of BaaS providers have brought uncharacteristically large examination teams, likely being used as a training ground for the first appointees to the new program. If the Federal Reserve believes its own examiners do not possess the requisite skill sets to appropriately examine banks engaging in these relationships, requiring a dedicated team and supplementary examination approach, what does that say of its belief in the banks' own capabilities?

"The Fed's message is clear: Federal regulators view the delivery of financial services through BaaS partnerships as differentiated from traditional banking to the point of requiring a new playbook.

Risk in BaaS relationships

BaaS does not introduce new types of risk to a bank, other than product-related risk, to the extent these relationships introduce new offerings. It does, however, amplify the profile of traditional risks that any bank must manage, including those related to compliance, third-party, financial and reputation, among other risks.

The fundamental difference in a BaaS relationship is that customer engagement and service delivery, ordinarily undertaken by a bank's business line or "first line of defense," are now undertaken by separate entities that sit outside the federal regulatory perimeter. BaaS partners, by definition, tend to be technology focused, solving problems with efficiency and speed, and bringing new innovations to traditional financial products. Their focus is primarily on product development and customer experience, and they are not held to the same risk management standards as traditional banking systems. As such, BaaS partners do not generally prioritize risk management, and even when regulated in some capacity (such as state-licensed money transmitters), they do not ordinarily have compliance and risk management capabilities that would compare to a federally regulated bank. Banks placing reliance on their BaaS

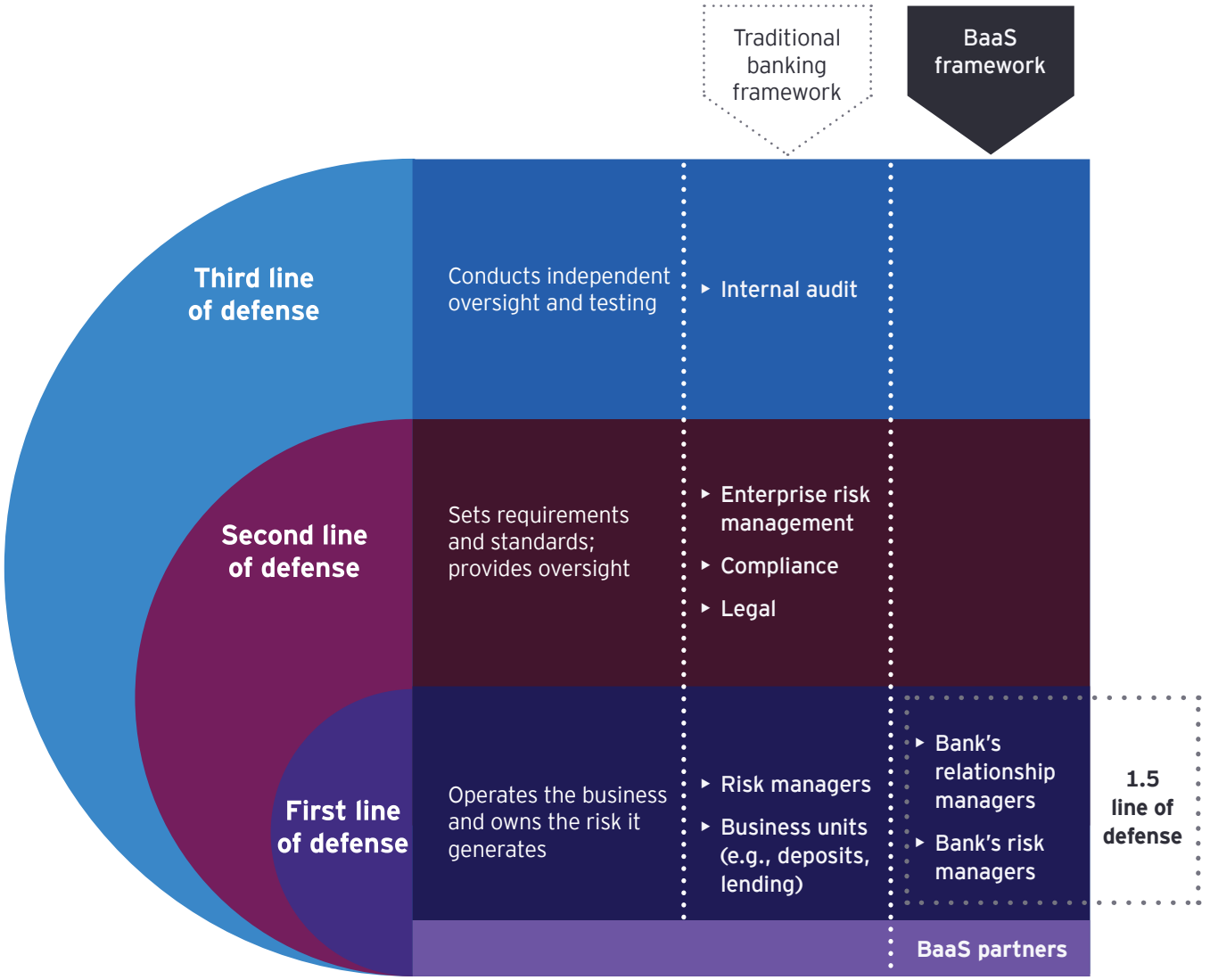

Figure 1

Risk in BaaS relationships (cont.)

partners, which sit outside of the federal regulatory perimeter, for core activities such as customer acquisition, distribution, and certain operational and compliance functions, is the principal risk that should be addressed.

A typical risk management framework includes defined roles and responsibilities across three lines of defense, as illustrated in Figure 1. Each line of defense plays a critical role in managing the institution's risk profile, beginning with the first line, which is typically the line of business that ultimately owns and is responsible for managing the risk generated through its business activity and implementing controls to mitigate those risks. The bank's second line of defense generally consists of compliance and risk management oversight functions and is responsible for assessing and monitoring risk, setting enterprise policies and standards for managing risk, and providing oversight of the business. The third line of defense, typically a bank's internal audit function, provides independent oversight of the first two lines of defense through testing to ensure the bank's controls are implemented and operating effectively.

The introduction of the BaaS relationship creates the need for an intermediary line of defense, which can be thought of as the "1.5 line of defense." This intermediary line encompasses the bank's risk and relationship managers, which should now participate in the maintenance of effective internal controls and execution of risk and control procedures, by providing direct oversight of the BaaS partner's activities.

In the delivery of their own products and services, banks typically have established compliance and risk management capabilities, enabling the bank to set standards and monitor their internal lines of business's adherence to requirements and risk guidelines, based on a board-approved risk appetite. This can become more challenging in the case of BaaS relationships, given the banks' often indirect and filtered relationship with the end customer of the BaaS partner.

Most BaaS providers, whether new, emerging or established, are generally classified as community or smaller regional banks and are accustomed to a level of supervision commensurate with their size and scale, traditionally based on the size of their balance sheet. The Fed's announcement, however, serves as a pointed signal that regulators are beginning to view size, scale and associated risk in terms that are not directly correlated to the balance sheet. Size and scale in the future will also be measured based on number of households or accounts, transaction volume, or other metrics that indicate the breadth of a bank's exposure to the US financial system. In turn, BaaS providers that are accustomed to a level of supervision and risk management expectations for a sub-$10 billion community bank may suddenly find themselves held to a level of compliance and risk management rigor typically reserved for larger regional banks, or greater. Under the Novel Activities Supervision Program, they will be measured against a new maturity scale and may find themselves unprepared to address the risks they have assumed.

"Most BaaS providers, whether new, emerging or established, are generally classified as community or smaller regional banks and are accustomed to a level of supervision commensurate with their size and scale, traditionally based on the size of their balance sheet.

Establishing risk management and governance

Fortunately, these risks can be effectively managed. Successful BaaS providers have adopted novel risk management approaches that are uniquely applied to their BaaS line of business. The BaaS risk profile necessitates dedicated line of business risk management and governance, wherein accountability for managing the bank's BaaS-driven risks is engrained in first-line relationship managers who are closest to the BaaS partner's day-to-day operations. Specific, BaaS-oriented considerations, such as those shown in Figure 2, should be accounted for at each stage in the risk management lifecycle.

In a mature environment, the framework of a BaaS partner relationship is set before the BaaS partner even enters the bank's purview. Within its governance and oversight framework, the bank should already have planned and decisioned internal risk standards and policies, which will inform the requirements of the BaaS partner relationship, per the bank's enterprise risk management framework. It is incumbent on the bank's board of directors to set the bank's risk appetite for the BaaS business, and on the bank's three lines of defense to institute the appropriate governance infrastructure; set the bank's

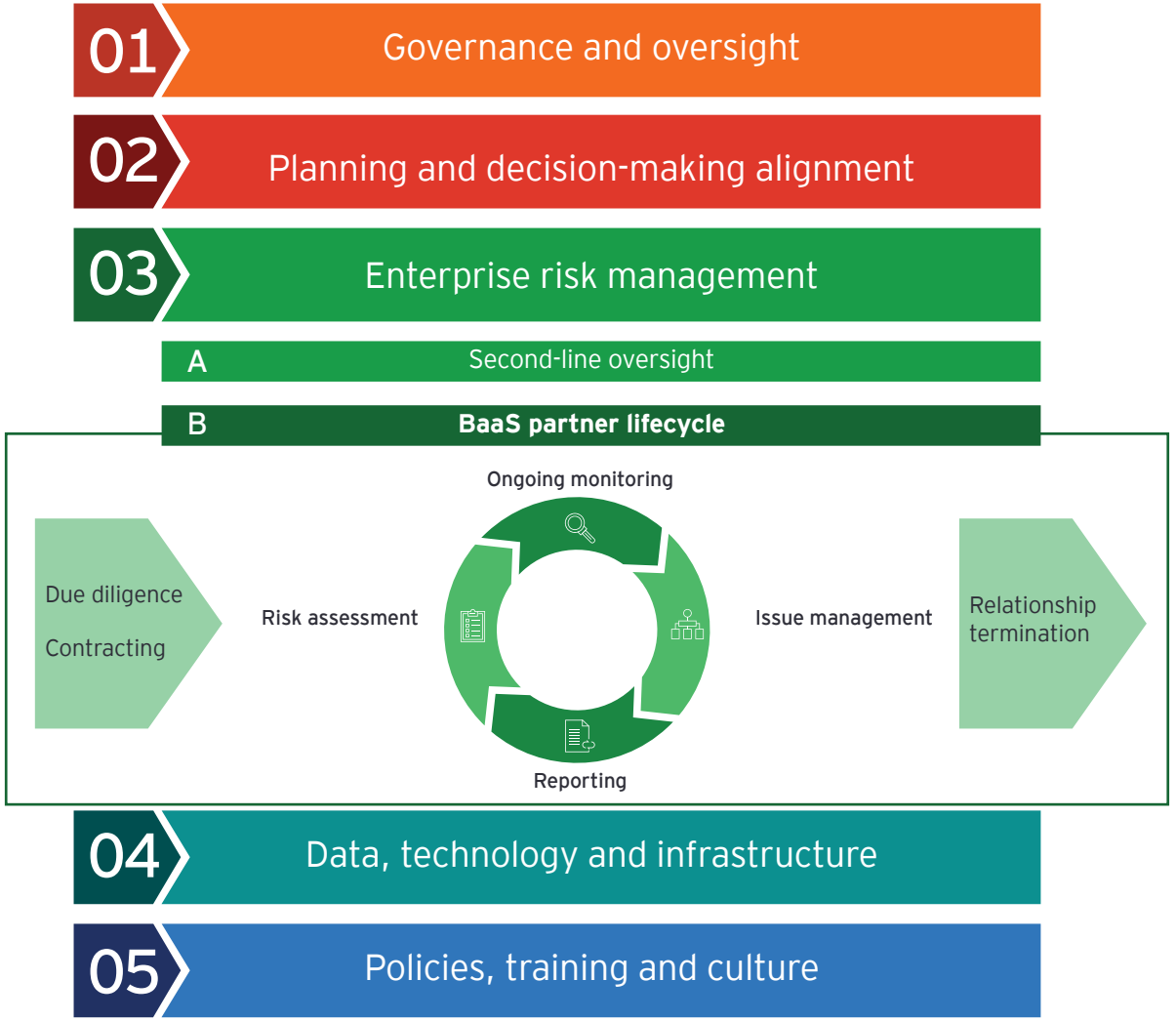

Figure 2

Establishing risk management and governance (cont.)

policies, procedures and standards; perform risk-based monitoring, testing and audit activities; and report key risk trends and metrics through appropriate levels of management and the board.

Prior to entering a BaaS partnership, the bank should conduct due diligence to determine whether the BaaS partner aligns with the bank's internal standards and policies. Assuming no red flags are raised during due diligence, the bank should then create a contract that defines the flow of data and information between the entities; the bank's right to audit the BaaS partner; and the bank and the BaaS partner's risk management and operational roles and responsibilities, service-level agreements (SLAs), timelines, and consequences should the BaaS partner fail to deliver or meet the bank's own regulatory obligations created by the products offered through the BaaS partner. A strong contracting phase is the first risk mitigant a bank can employ and will typically continue paying off throughout the partner lifecycle.

Initial and periodic risk assessments can identify any gaps between the bank's and BaaS partner's frameworks and verify the BaaS program is fully integrated into its risk management program. Risk assessment should inform the bank's ongoing monitoring activities. As issues are identified, either by the bank or its BaaS partner, they should be addressed in accordance with established policy and reported to relevant stakeholders. Even the terms of relationship termination should be planned well in advance to mitigate risk associated with unwinding a complex and interwoven partnership and minimize consumer impact.

BaaS relationships can impact all of a bank's risk domains, both financial and nonfinancial. Banks should continue to address their identified operational, financial, compliance and other applicable risks, while identifying the incremental effort and activities necessary to address the amplified risks their BaaS partners present.

Ultimately, a bank's risk management approach should be tailored to the particular risks associated with a BaaS relationship. For example, certain relationships may carry elevated consumer protection risks based on the products and/or services and target market (e.g., a FinTech specializing in low-income lending products), whereas others may not invoke consumer protection requirements but may pose elevated money-laundering risks (e.g., a B2B cross-border payments platform).

Figure 3

Compliance risk considerations

To illustrate the risk management framework for compliance risk, banks should consider the following:

- **Due diligence.** Assess the BaaS partner's policies, procedures, and operational and technical capabilities to facilitate compliance with consumer protection laws and regulations.
- **Contracting.** Clearly document compliance-related roles and responsibilities assigned to the BaaS partner in the contract. Contracts should also consider SLAs, reporting requirements, escalation and consequence measures for noncompliance, the flow of information and data between entities, and the bank's right to audit.
- **Risk assessment.** At onboarding, and periodically thereafter, evaluate the inherent compliance risk of a BaaS relationship, and the BaaS partner's and the bank's controls to mitigate that risk, and adjust ongoing monitoring and controls to address any changes in the risk profile.
- **Monitoring.** Banks should monitor key risk and performance indicators on a regular basis to identify potential emerging compliance issues and should monitor consumer complaints received by the BaaS partner and the bank to identify possible issues. Banks should conduct periodic testing of BaaS partners' operations and review advertisements to confirm adherence to compliance requirements. Banks should also design processes to ensure regulatory and product or service changes are adequately assessed and implemented between the bank and BaaS partners. For example, banks should monitor for changes to a BaaS partner's user agreements, and product terms and conditions, and should implement a compliance review process to assess the impact of any changes the BaaS partner proposes. Banks should monitor for regulatory changes and timely disseminate new or modified requirements to their BaaS partners to ensure appropriate changes are adopted.
- **Issue management.** Banks should develop an issue management framework to define the roles and responsibilities for identifying, escalating, assigning, tracking and remediating compliance-related issues between their frontline risk managers and relationship managers (defined as the 1.5 line in Figure 1, above) and its BaaS partners. This framework should also include the types and severity of issues and how each should be remediated and closed. This program should serve as the first filter of information in the risk-based monitoring and testing function, to channel the most important information up the reporting chain. The bank's issue management framework should also hold the BaaS partner accountable for remediation of issues and help drive effective risk mitigation for the bank and its BaaS partners holistically.

Compliance risk considerations (cont.)

- **Reporting.** The flow of information up and down the reporting chain is vital to ensure effective communication between the bank and the BaaS partner and to direct the flow of resources to the areas of the program with the most need. As previously mentioned, the bank's board and senior management are responsible for setting and communicating standards and policies down the reporting chain, and the business is responsible for escalating key performance and risk indicators and detailed information up the chain. Not only should a bank define the metrics it deems important and communicate those guidelines to the BaaS partner, but the reporting framework should include what type of information is required for executive decision-making and the appropriate level of detail for reporting packages at each level.
- **Offboarding.** Banks should maintain plans to transition BaaS partners off the platform with minimal consumer impact, in the event of a partner's noncompliance with requirements and in accordance with contractual escalation and consequence clauses.

Each pillar of a firm's risk management framework does not function in isolation — they work in conjunction with each other, building, informing and maturing at every step. Successful BaaS providers have developed frameworks to holistically assess, monitor and report risk related to individual BaaS partners (and across their BaaS line of business) in a scorecard-like fashion, enabling the business, compliance function and board to readily identify BaaS partners posing the highest risk, detect upcoming risk appetite breaches, and adjust the bank's risk management program to the highest-risk BaaS partners and high-risk areas.

Across all elements of the risk management lifecycle and risk areas, banks should consider the following as they assess their capabilities across people, processes and technology:

- **People.** Banks should allow for adequate staffing to manage day-to-day operations, compliance and risk management activities associated with their BaaS relationships. BaaS partners often experience customer and transaction volume growth orders of magnitude faster than the traditional banking sector, which presents a critical challenge to a smaller community bank supporting these relationships. Banks should consider the use of third parties to address rapid needs for scale while managing cost. For banks that are able to hire personnel at sufficient rates to match business growth, maintaining operational and risk management excellence through high growth periods and with new personnel is a challenge, as is attracting sufficient levels of talent with the required skill sets and experience.
- **Technology.** Banks should identify key data points required to effectively assess and monitor risks related to their BaaS relationships on an ongoing basis and should allow that they have appropriate mechanisms to capture, store and manipulate data for risk measurement and reporting, including data provided by their BaaS partners. This is in addition to setting minimum data standards for the bank to fulfill minimum regulatory obligations, such as executing transaction monitoring or responding to customer disputes.
- **Process.** Banks should understand the operational burden associated with their BaaS relationships and should factor these direct and indirect costs into their agreements with BaaS partners to allow sustainable business growth. Prudent risk management does not need to come at the expense of profitability to the bank. For example, leading institutions have undertaken an analysis to identify operational units of work (e.g., compliance testing, transaction monitoring investigations) and quantify the cost of those units, with the aim of passing those risk management costs through to their BaaS partners. In addition, banks should embrace process innovation and look for ways to gain efficiency without sacrificing quality. Processes that may be suitable for a community bank's core banking activity may not be suitable for servicing a BaaS relationship, through which the bank serves hundreds of thousands of consumers.

Conclusion

As financial institutions continue to weather economic uncertainty, increasing regulatory expectations and shifting consumer expectations, banks have increasingly adopted the BaaS model to increase exposure to wider demographics, offer a broader array of products, and capture new revenue and profit growth opportunities. With innovation and the opportunity for greater reward comes a higher level of regulatory scrutiny. Positioning the institution to sustain this growth responsibly requires a shift in focus to maintain effective oversight of new partners, a dedication to scaling risk management activities and programs to match the accelerated business growth, and a thoughtful connection with regulators to demonstrate that these activities can be undertaken in a way that does not jeopardize the safety and soundness of the institution.

Regulatory expectations are evolving, and near-term examinations could be expected to hone in on novel risks highlighted in the Fed's supervisory letter as authorities continue to sharpen their focus on the incremental risks posed by BaaS partnerships. We expect other federal banking regulators to adopt a similar approach to the Fed, to address what is likely perceived as unmitigated risk. BaaS providers that have undergone a recent regulatory examination have likely begun to receive pointed feedback regarding their risk management and compliance programs, and those that have not come under pressure likely have yet to be examined. BaaS providers of all sizes should undertake an end-to-end evaluation of their risk management and compliance frameworks to identify potential weaknesses and be prepared to demonstrate to their regulators a practical plan to uplift their programs to scale with their level of risk.

BaaS partners themselves should also take note and expect to come under additional scrutiny from their bank partners. While federal examiners may not have authority to directly impose requirements on BaaS partners, they do have the ability to require banks to take actions that, in all likelihood, will include pass-through requirements to BaaS partners.

Conclusion (cont.)

Despite the additional burden that naturally accompanies enhanced supervision, the Fed's creation of this new program is an encouraging signal of its commitment to responsible financial innovation. In time, the industry will benefit from the Fed and other federal banking regulators publishing clear guidance articulating their expectations for BaaS providers' risk management programs, enabling banks to grow responsibly and serve consumers in innovative and more efficient ways.

EY teams have served both FinTechs and BaaS banks across the maturity spectrum on topics, including regulatory remediation, redesign of risk and compliance program frameworks, development of specific compliance program elements to oversee BaaS partner compliance, cost-effective and scalable operations, and designing strategies for addressing incremental risks associated with onboarding new partners. Our deep connection to both segments of the industry has strengthened our understanding of the business challenges and needs of the FinTech community as it searches for bank partners as well as the components of effective risk management programs. We bring this industry perspective, along with our interpretation of new regulatory developments, to help clients implement practical, risk-based solutions that are tailored to the specific risks applicable to their business models and bring clarity to an evolving regulatory environment.

Deep experience operating across the regulatory spectrum, dedicated financial services professionals, a regulatory network designed to engage with state and federal regulators, and a connection to both BaaS banks and the FinTechs with which they wish to partner positions EY professionals to support banks already engaged in BaaS activities and those that wish to enter the space. Contact us to learn more about how we can support your BaaS journey.

> "Our deep connection to both segments of the industry has strengthened our understanding of the business challenges and needs of the FinTech community as it searches for bank partners as well as the components of effective risk management programs.

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

What makes EY distinctive in financial services

Over 84,000 EY professionals are dedicated to financial services, serving the banking and capital markets, insurance, and wealth and asset management sectors. We share a single focus — to build a better financial services industry, one that is stronger, fairer and more sustainable.

SCORE no. 21289-231US
2308-4318338 BDFSO
ED None

ey.com

Key Ernst & Young LLP contacts

Michael Winter
Principal
Ernst & Young LLP
michael.winter@ey.com
+1 415 894 4244

Andrew Abdalla
Manager
Ernst & Young LLP
andrew.abdalla@ey.com
+1 415 486 3608

Sam Holt
Manager
Ernst & Young LLP
sam.holt@ey.com
+1 206 654 7613

[1]"SR 23-7: Creation of Novel Activities Supervision Program," Board of Governors of the Federal Reserve System, 8 August 2023, https://www.federalreserve.gov/supervisionreg/srletters/SR2307.htm.

[2]"Notices," Federal Register, Vol. 88, No. 111, 9 June 2023, https://www.govinfo.gov/content/pkg/FR-2023-06-09/pdf/2023-12340.pdf.