Deloitte.

Together makes progress

Operationalizing your bank

Third-party risk management

July 2026

Center *for*
Regulatory Strategy
US

About the series

This perspective is part of Deloitte's 13-part *Operationalizing your bank* series, designed for applicants that have received conditional approval, are progressing toward final approval, or are focused on preparing for bank launch.

In this edition, we cover key considerations for establishing a credible, bank-ready third-party risk management (TPRM) framework to manage the risks associated with services delivered by third parties and affiliates, which often provide services central to bank operations. The TPRM framework and supporting policies, processes, and governance should address both relationship types and define how oversight and accountability are organized across the three lines. The result should be a program that is proportionate to the bank's complexity and capable of supporting resilient operations as the institution grows.

For purposes of this piece, a third party is an external vendor or service provider with no ownership relationship to the bank. An affiliate is an entity related to the bank through common ownership or control, such as a parent or sister entity.

Future editions of this series will focus on the remaining foundational areas listed in Figure 1.

Figure 1: Series topics

The term "bank" is used broadly throughout this series to cover considerations across common bank charter structures, including national banks, state member/nonmember banks, national trust banks, and industrial loan companies (ILCs). Foreign banking organizations, US branches, and bank holding companies would have a number of other nuanced and unique considerations. While this series aims to address broadly applicable operationalization considerations, organizations should evaluate this guidance within the context of their business strategy, targeted charter type and general circumstances, as institution-specific requirements may warrant additional considerations beyond what is outlined in this series.

Operationalizing third-party risk management

As the bank prepares to launch, it will be responsible for managing a complex mix of third-party and affiliate relationships. These relationships may either be inherited from the parent entity or newly procured to support critical bank operations. The bank should therefore establish, before launch, the governance, contract management, monitoring, and escalation capabilities needed to oversee these relationships and manage their associated risks. These arrangements are likely to receive early supervisory attention, particularly with respect to the bank's critical processes and services, service dependencies, operating model, and accountability structure. Regulators will want to understand who performs each activity, how performance and risks are monitored, how issues are escalated, and how the bank would maintain operations if a provider or affiliate experienced a disruption. Weaknesses in these areas could affect the bank's safety, soundness, resilience, and ability to operate effectively from Day 1.

Core insights

1. **The bank is accountable for third-party and affiliate oversight:** Prior to launch, a de novo bank needs to have a comprehensive view of third-party and affiliate service providers and understand the way in which each will support bank operations. Third-party and affiliate relationships should be inventoried, risk-tiered or classified, and mapped to the bank processes, services, or systems they support, along with the accountable business owner for each relationship. While new banks are permitted to leverage parent, affiliate, or third-party processes, this does not replace bank-level accountability and governance. Regulators will expect the bank to demonstrate that it understands the full scope of its relationships and is able to demonstrate how performance will be monitored and deficiencies addressed prior to launch.

2. **TPRM governance is key to meeting Day 1 readiness expectations:** Regulators expect a de novo bank to open with a fully functional TPRM governance structure. Board and management oversight of material third-party and affiliate risk must be aligned to the bank's overall strategic objectives and risk appetite, with a designated senior executive carrying primary accountability for the TPRM framework and its integration into the bank's broader risk management environment. Meaningful governance is demonstrated through board reporting routines, committee activity, and key risk indicator (KRI) frameworks that give senior management and the board real visibility into third-party risk exposures. Examiners will look beyond the existence of a TPRM framework to assess whether governance is functioning in practice, making the quality and consistency of pre-launch committee activity, approvals, and reporting a critical indicator of program maturity.

3. **TPRM manages third-party and affiliate risk across the full relationship lifecycle:** Third-party and affiliate relationships are often central to a new bank's ability to deliver its Day 1 products and services, making a structured, risk-based TPRM lifecycle one of the most important capabilities to get right before launch. The 2023 Interagency Guidance on Third-Party Relationships establishes clear expectations for banks to consider when building a TPRM program and lifecycle covering planning, due diligence and selection, onboarding, ongoing monitoring and termination. A mature lifecycle is distinguished by:

    - A top-down view of the full lifecycle that maps every activity needed to effectively oversee third parties and affiliates, in alignment with the TPRM program framework, and shows how those activities interrelate to support the TPRM program objectives
    - Clear sequencing of the activities, with assigned ownership, that enables seamless hand-off from one stage to the next and provides ongoing transparency into the status of each third party and affiliate within the program lifecycle
    - A level of risk oversight applied to each third party or affiliate that is right-sized to the level of risk it presents
    - The degree to which the lifecycle promotes coordination, collaboration and information sharing across the bank's teams responsible for identifying, monitoring and managing risks

4 **TPRM includes intercompany relationships:** De novo banks must ensure that service arrangements with affiliates (referred to as intercompany transactions) comply with Regulation W under 12 CFR Part 223. This includes establishing arm's-length terms, market-rate pricing, covered transaction limits, and board or committee approval for covered transactions. Intercompany agreements should be in place to define the scope of services, performance standards, escalation procedures, and termination rights. Transfer-pricing and fee structures should also be documented, with the chief financial officer's office typically retaining accountability for intercompany settlement.

5 **TPRM should address concentration risk and operational resilience:** De novo banks are often heavily dependent on a small number of affiliate or third-party providers for critical functions such as core banking technology, loan origination, deposit operations, and cybersecurity. These dependencies can create operational and regulatory risk if the bank cannot demonstrate viable contingency plans or exit strategies. The TPRM program should therefore document concentration exposure and identify single points of failure across critical providers. It should also maintain tested business continuity plans that provide fallback options for critical providers.

Actions for launch readiness

1 **Set the TPRM program foundation:** New banks should establish a bank-specific TPRM policy aligned with the 2023 Interagency Guidance that defines the program's scope, risk-tiering criteria, due diligence standards, contracting requirements, and ongoing monitoring cadences. It's critical to build a third-party inventory that distinguishes bank-owned relationships from those inherited from or shared with the parent or affiliates and assigns a bank-designated business owner accountable for each relationship. The inventory should document the service description, risk tier, criticality to bank operations, and applicable oversight schedule.

2 **Codify service expectations with parent or affiliated entities:** Banks must establish formal agreements and corresponding service level agreements (SLAs) for each service that the bank receives from, or provides to, a parent or affiliated entity. These agreements should document the service scope, performance metrics, pricing methodology, escalation procedures, and termination rights. The SLAs should also address data security, regulatory change notifications, and the bank's right to audit the service provider. In addition, the bank should confirm that fee structures and transfer pricing comply with Regulation W's arm's-length requirements and have been approved by the appropriate committee or board. Legal counsel should review and approve all agreements before Day 1 operations.

3 **Complete pre-opening due diligence activities:** Critical and higher-risk third parties should be fully vetted before launch with documented due diligence, including reviews of relevant certifications and financial health assessments. Regulators will expect due diligence standards for affiliate-provided services to be equivalent to those applied to third parties. The bank should document the results of each assessment in the inventory, identify any gaps, and establish remediation timelines where deficiencies are found. This includes confirmation that ongoing monitoring schedules have been established and that responsible parties have been notified of their monitoring obligations before launch.

4 **Implement ongoing monitoring:** Monitoring routines for critical and high-risk providers demonstrate how oversight will extend beyond launch. This includes periodic evaluations of third-party and affiliate performance against the SLAs established in their contracts, as well as assessments of the effectiveness of controls within each provider's control environment. The bank should also establish processes to facilitate the ongoing management of identified issues and associated remediation plans.

5 **Test exit strategies for critical providers:** Demonstrating that the bank can maintain operations if a critical third-party or affiliate provider becomes unavailable is essential to operational resilience. For each third party or affiliate designated as critical to the bank's operations, the bank should document and test credible business continuity plans that address service-disruption scenarios and identify viable alternatives or fallback procedures. It should also confirm that the termination provisions in applicable agreements and associated SLAs are operationally realistic. Collectively, these measures enable the bank to demonstrate how it would transition away from a critical provider if necessary.

Where to go from here

Third-party and affiliate arrangements should be treated as both an operational dependency and a core risk management discipline for a new bank. At its core, an effective TPRM program is a decision-making tool: it enables management and the board to understand where risk is concentrated, whether key relationships are performing as expected, and whether the bank maintains sufficient control over the services on which it depends. As Day 1 approaches, the program should be operational and evidenced through a bank-specific governance model, a current relationship inventory, completed due diligence, executed agreements, established management and board reporting, and tested continuity and termination plans. Banks that can demonstrate these capabilities in practice, not merely in policy, are better positioned to support launch readiness, respond to disruption, and show regulators that third-party risk is being appropriately managed.

Regulatory insights to action

The Deloitte Center for Regulatory Strategy, US

DCRS helps financial services firms anticipate regulatory change and respond with confidence. We focus on four sectors: banking, capital markets, investment management, and insurance.

As global regulators adapt to shifting economic, geopolitical, and technological forces, they continue to reshape business models and operating frameworks. These shifts create both risks and opportunities for firms.

Our team combines private and public sector experience, supported by Deloitte's access to a global network and regional hubs in Asia Pacific and Europe, the Middle East, and Africa. With former regulators, industry specialists, and business advisers, we deliver practical insights to help organizations navigate complexity and stay ahead.

Additional insights can be found on our hub page here.

How can we help you?

Register for our monthly newsletter

Contacts

Licensing

Jennifer Burns
Managing Director
Deloitte & Touche LLP
jennburns@deloitte.com

Joshua Flyer
Senior Manager
Deloitte & Touche LLP
jflyer@deloitte.com

Jann Futterman
Senior Manager
Deloitte & Touche LLP
jfutterman@deloitte.com

Tara Wensel
Senior Manager
Deloitte & Touche LLP
tawensel@deloitte.com

Third-Party Risk Management

Suzanne Denton
Managing Director
Deloitte & Touche LLP
sudenton@deloitte.com

Brian Adams
Senior Manager
Deloitte & Touche LLP
briadams@deloitte.com

Deloitte Center for Regulatory Strategy, US

Irena Gecas-McCarthy
FSI Director, Deloitte Center for Regulatory Strategy, US
Principal
Deloitte & Touche LLP
igecasmccarthy@deloitte.com

Lananh Nguyen
R&I Director, Deloitte Center for Regulatory Strategy, US
Managing Director
Deloitte Services LP
lananhnguyen@deloitte.com

Aaron Salerno
Manager
Deloitte Services LP
asalerno@deloitte.com

Kyle Cooke
Manager
Deloitte Services LP
kycooke@deloitte.com

Special thanks and appreciation to Deloitte team member **Jake Willcox** for his contributions.

Center *for*
Regulatory Strategy US

About the Center
The Deloitte Center for Regulatory Strategy provides valuable insight to help organizations in the financial services industry keep abreast of emerging regulatory and compliance requirements, regulatory implementation leading practices, and other regulatory trends. Home to a team of experienced executives, former regulators, and Deloitte professionals with extensive experience solving complex regulatory issues, the Center exists to bring relevant information and specialized perspectives to our clients through a range of media, including thought leadership, research, forums, webcasts, and events.

Deloitte.