Deloitte.

Together makes progress

Operationalizing your bank

Technology

August 2026

Center *for*
Regulatory Strategy
US

About the series

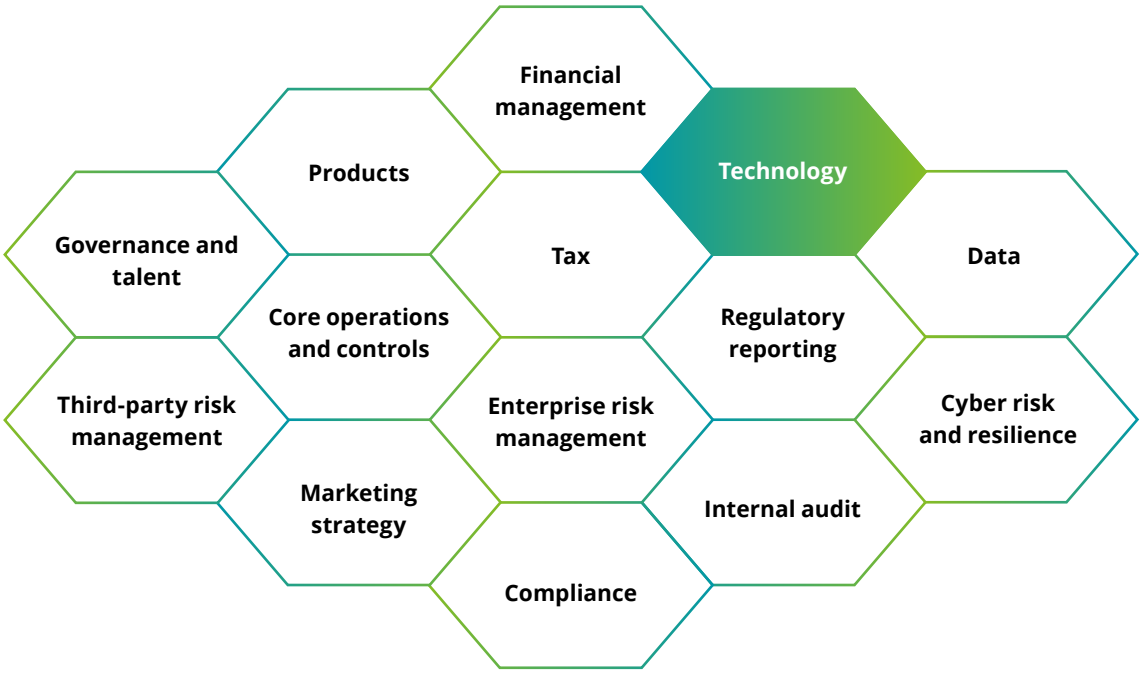
This perspective is part of Deloitte's *Operationalizing your bank* series, designed for applicants that have received conditional approval, are progressing toward final approval, or are focused on preparing for bank launch.

In this edition, we focus on technology and the realities of standing up a bank-grade environment where core platforms, customer-facing interfaces, compliance capabilities, and third-party dependencies must come together on a fixed regulatory timeline.

Regulators expect new banks to demonstrate that their technology environment can support safe and sound operations, regulatory compliance, operational resilience, and accurate reporting from the day the bank opens its doors.

Other editions of this series 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 technology

For organizations progressing through the bank chartering process, one of the most significant challenges is assembling a bank-grade technology environment ready on Day 1. The pre-launch window is short, and technology dependencies are sequential: the core banking platform must be selected before integrations can be built, integrations should be built before data flows can be tested, certifications operate on counterparty-controlled timelines, and the resulting environment needs to be sufficiently implemented before opening. Bank executives who treat technology operationalization as a systems integration and certification program with a fixed regulatory deadline are typically better positioned to achieve launch readiness on schedule.

Core insights

1. **Technology exposes whether the operating model is achievable:** Many organizations view technology architecture as an implementation exercise that follows operating model decisions. In practice, technology often determines the operating model itself. Decisions regarding platforms, integrations, and data ownership establish which activities can be performed by the bank, leveraged from affiliates, or outsourced to third parties. As a result, technology architecture becomes one of the primary mechanisms through which the target operating model is realized.

2. **Ownership and dependency gaps come into focus through architecture:** Organizations often begin technology planning by cataloging systems, integrations, and platforms. Through architecture design, management gains visibility into where regulatory gaps exist, where third-party dependencies create risk, and where new capabilities should be established. This upfront planning often reveals that the primary challenge is not deciding what technology to deploy, but determining how the bank will actually operate across systems, affiliates, and third parties. For example, customer-facing interfaces including mobile app, web experience, and onboarding and servicing flows should connect to the core banking platform and operate according to the bank's controls.

3. **The core banking platform is a binding constraint, and it is rarely the platform you already run:** A non-bank ledger built for wallets, balances, or payment flows is not a system of record for a chartered bank. New banks typically adopt a modern core banking platform or build on a ledger-as-a-service layer. Selection, configuration, the chart of accounts, and data migration drive the critical path. A common failure is underestimating core banking platform implementation time and discovering late that the platform cannot support the bank's products and reporting requirements.

4. **External counterparties and third-party dependencies often control the critical path:** Technology builds are frequently constrained by external counterparties rather than internal development timelines, and dependencies vary by the bank's products. For example, payment and card products typically require processors, card network certifications, payment rail integrations, or Federal Reserve account access. These dependencies are often sequential and operate on timelines outside the bank's control. A common failure is underestimating the time required to complete third-party onboarding and required certifications, resulting in late-stage delays to launch readiness.

5. **Compliance, controls, and resilience should be wired in and be production-grade at opening:** Bank Secrecy Act/anti-money laundering transaction monitoring, sanctions screening, and fraud detection require information flows from the core banking platform and customer-facing interfaces, along with an auditable alert-to-disposition trail. The bank should also reconcile a daily financial position between the core banking platform and general ledger, as well as generate detailed regulatory and management reports aligned with its products, services, and broader enterprise or parent structure. Underpinning all of it, cyber resilience, redundancy, and tested disaster recovery have to be in place at opening rather than iterated toward. Regulators evaluate whether these capabilities operate together as an effective control environment, and organizations should treat these capabilities as foundational before launch.

Actions for launch readiness

1. **Establish target-state architecture principles before selecting platforms:** Architecture principles should guide decisions across cloud strategy, integration patterns, resiliency requirements, data ownership, information security, and system boundaries among the bank, affiliates, and third parties. Alignment of the architecture principles with the bank's business plan, growth expectations, and regulatory requirements helps to make sure platform selections support bank objectives.
2. **Assess existing capabilities through a regulatory lens:** An assessment of applications, integrations, data stores, and supporting technology capabilities against banking regulatory expectations provides a baseline for identifying required enhancements. Rather than assuming a parent's capabilities can be reused without adjustment, organizations should identify where enhancements are required to address regulatory gaps, data retention requirements, resiliency expectations, control requirements, or independent bank oversight needs. The resulting assessment becomes the foundation for build, buy, and outsource decisions.
3. **Align technology components through a future-state architecture:** The future-state architecture serves as the blueprint for how customer-facing interfaces, applications, integrations, data, security, and infrastructure components operate together. The architecture should clearly identify which capabilities will be performed by the bank, leveraged from affiliates, provided by third parties, or built internally. Establishing this blueprint early helps avoid fragmented technology decisions and creates alignment across products, operations, risk, and compliance teams.
4. **Use structured vendor evaluations for critical platform decisions:** For core banking and other strategic platform selections, develop business, operational, regulatory, and technology requirements before engaging vendors. Solutions should be evaluated against a consistent assessment framework that considers functional fit, integration complexity, security, resiliency, scalability, regulatory requirements, implementation effort, and total cost of ownership. Vendor decisions made early in the build can have long-term implications for operational flexibility and regulatory readiness.
5. **Develop an implementation roadmap and cost model aligned to launch readiness:** A phased implementation roadmap translates the target-state architecture into defined workstreams, dependencies, milestones, technology builds, testing activities, and migration requirements. The roadmap should prioritize capabilities required for regulatory approval and Day 1 operations while establishing a clear view of both the cost to achieve and the cost to operate the future-state technology environment. This exercise helps management sequence investments, identify delivery risks, and demonstrate execution readiness to regulators.

Digital asset applicants

Applicants seeking a charter to custody digital assets or issue a payment stablecoin face distinct technology risks that are unlike those of traditional banks. For a custodian, the safeguarding of the private key is paramount. On-chain transactions are final and irrevocable, and the ability to move assets in and out of a wallet relies directly on access to the associated key. Therefore, key loss or compromise is the equivalent of asset loss and is generally unrecoverable. To mitigate this, dedicated hardware and software strategies exist to support custody architecture.

Because the GENIUS Act limits reserves to permitted assets, an issuer's technology must track and reconcile reserve composition against outstanding stablecoins in near real time, support required reporting, and process redemptions within mandated timeframes.

Technical readiness is integral to an issuer's ability to meet its new obligations, and priority should be given to designing, building, and testing the new applications and capabilities in order to satisfy regulatory requirements.

Where to go from here

Because technology often has one of the longest lead times, applicants that have not already begun designing their systems should mobilize quickly after receiving conditional approval. The architecture, platforms, integrations, and data environment selected today will influence how the bank operates, scales, and manages risk long after launch. Management should focus not only on what technology will be implemented, but also on whether the resulting technology environment supports the bank's operating model, control framework, regulatory commitments, and long-term growth plans.

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

Technology

Tim O'Connor
Principal
Deloitte Consulting LLP
tioconnor@deloitte.com

Hakam Haddadin
Specialist Leader
Deloitte Consulting LLP
hhaddadin@deloitte.com

Scott Lasher
Senior Manager
Deloitte Consulting LLP
slasher@deloitte.com

Ella Arazi
Senior Manager
Deloitte Consulting LLP
earazi@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 members **Ellen Boyer**, **Prathamesh Tawde**, and **Judy Wei** for their insights and 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.