Deloitte.

Together makes progress

Operationalizing your bank

Cyber risk and resilience

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.

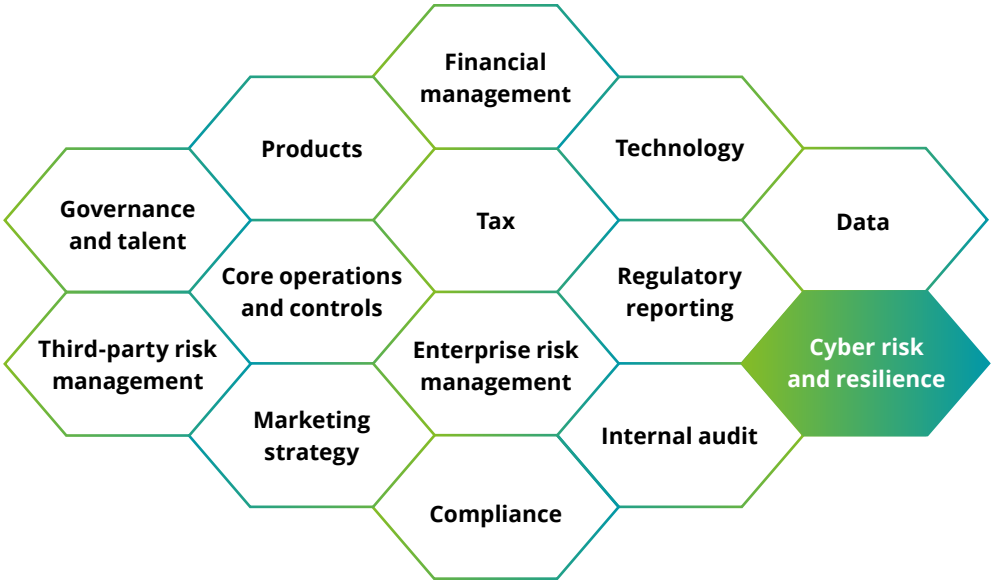
In this edition, we focus on cyber risk and operational resilience, both foundational capabilities that enable banks to protect critical operations, manage cyber threats, and sustain core business services through disruption. The cyber risk and operational resilience framework should establish the governance, controls, resilience strategies, incident response processes, technical solutions, and third-party oversight needed to support critical banking capabilities during severe disruption scenarios. The result should be a program that is proportionate to the bank's complexity and capable of supporting safe, sound, and resilient operations from Day 1 and as the institution grows.

Regulators expect new banks to demonstrate that critical cyber risk and operational resilience capabilities are in place and functioning before launch. This includes the ability to:

- respond to and recover from cyber incidents and disruptions
- identify and ensure critical business capabilities can continue to operate or be recovered within acceptable timeframes
- provide effective governance and board oversight of cyber risk and operational resilience

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 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 cyber risk and resilience

As a bank prepares to launch, it should establish cyber risk and operational resilience capabilities that demonstrate operational readiness and risk management sufficient to support safe, sound, and sustained bank operations. Regulators will evaluate cyber and operational resilience risk governance, including where the bank may sit within a larger enterprise or organization that may not need to adhere to the same regulatory obligations. Criteria that examiners will use to evaluate operational resilience and the control environment include management's ability to:

- identifying core business capabilities with underlying technical assets and data
- protecting critical infrastructure
- recovering from severe disruptions
- managing third-party and shared-service dependencies
- escalating, managing, and reporting incidents through clear decision-making channels

Where these capabilities fall within the remit of the parent or an affiliate entity, the bank can leverage these services in a way that is consistent with regulatory expectations for independence, safety, and soundness. But services that are provided by the parent or an affiliate entity will need to be documented through service-level agreements based upon arm's-length pricing and monitored by the bank (see our publication on third-party risk management for more information on affiliate transactions).

Core insights

1. **Resilience centers on critical banking services:** Operational resilience is measured by whether the bank's most important services can continue or recover promptly following a severe disruption. For a de novo bank, this includes maintaining a minimum viable operating capability during events such as a destructive cyberattack or the loss of a critical service provider. Regulatory attention extends to recovery strategies involving immutable backups, protected data vaults, isolated recovery environments, and regular testing. Applicable computer-incident notification requirements may also be triggered. Where a parent or its vendors provide essential services, those dependencies remain part of the bank's resilience profile.

2. **Incident response must work in practice:** An effective incident response program enables the bank to assess an event quickly, determine its potential impact, and coordinate a timely response. Regulators look beyond written plans for evidence that the process can operate under pressure. Key elements include clear decision thresholds, escalation paths, regulatory contact protocols, vendor notification channels, and internal and external communications procedures. The process also needs to support timely notification when an incident meets applicable reporting requirements. For a de novo bank, the ability to make and document these decisions is an important indicator of operational readiness.

3. **Day 1 requires layered, testable defenses:** Cyber resilience depends on a defense-in-depth architecture aligned with the external threat environment and the bank's likely attack paths. A Day 1-ready control environment combines preventive and detective measures across identity, access, endpoints, networks, data, applications, and transaction activity. These controls are expected to address risks such as credential compromise, ransomware, privileged-access misuse, data loss, synthetic identity fraud, and social engineering. Regulatory review focuses not only on control design but also on whether controls are integrated, operating as intended, and supported by testing that demonstrates protection of core banking services.

4. **Third-party resilience remains the bank's responsibility:** Many de novo banks depend heavily on cloud providers, processors, utilities, affiliates, and other outsourced services to support core operations. Those arrangements do not transfer accountability for cyber risk or operational resilience. Regulators therefore assess how third-party risks are reflected in due diligence, contracts, ongoing monitoring, issue escalation, concentration analysis, subcontractor visibility, and contingency or exit planning. The same expectations apply when a parent or affiliate provides shared services or manages vendors on the bank's behalf. Because a new bank may have limited operating history and concentrated dependencies, its third-party resilience framework may receive heightened supervisory attention.

5. **Governance must provide clear visibility and accountability:** Cyber risk and operational resilience require active oversight from the bank's board and senior management. Regulators expect periodic, substantive reporting on the bank's risk posture, material gaps, incidents, testing results, and remediation progress. Clear management ownership and effective independent challenge from risk, compliance, and internal audit help demonstrate that the framework is operating as intended. A parent or affiliate may contribute technology, expertise, or shared services, but bank-level accountability and decision-making remain essential. Governance arrangements therefore need clear connections between the bank and its parent, including defined escalation channels and authority for decisions affecting the bank.

Actions for launch readiness

1. **Define critical services, disruption tolerances, and dependencies:** A clear view of the bank's minimum viable operating capability should anchor resilience planning. For each critical service, the bank should define how much disruption it can absorb before customers or the institution experiences serious harm. End-to-end mapping should capture the supporting people, processes, technology, data, facilities, third parties, and parent or affiliate services. This information can then be used to test severe but plausible scenarios, identify single points of failure, prioritize remediation, and determine the investment needed to meet resilience expectations.
2. **Establish and evidence a Day 1 cyber control baseline:** The bank's opening-day environment should include layered preventive, detective, and response controls across its own operations and any supporting parent, affiliate, or critical third party. Preventive safeguards may address identity and privileged access, secure configurations, network segmentation, endpoint protection, and encryption. Centralized logging, security monitoring, vulnerability and patch management, alert triage, and incident playbooks provide the corresponding detection and response capabilities. Evidence should show that these controls are properly configured, operating as intended, and tested against threats to critical banking services.
3. **Formalize third-party oversight and incident escalation:** Clear accountability should extend across critical vendors, affiliates, shared services, and relevant subcontractors. Contracts and service agreements should address performance expectations, cyber protections, notification requirements, escalation procedures, and contingency planning. The incident process should also establish when an event may require regulatory notification, who makes that determination, how regulators are contacted, and how third and fourth parties join the response. Where a parent or affiliate provides services, a designated bank executive should remain accountable for oversight, issue escalation, and timely remediation.
4. **Prepare for heightened pre-opening scrutiny:** The pre-opening exam will test whether the capabilities described in the bank's application are operating in practice. Core configuration validation, vulnerability and penetration testing, fraud-control testing, and continuity and recovery exercises should therefore be completed before the review. Examiners are expected to focus on how third-party and affiliate dependencies have been identified and incorporated into recovery planning. Test results, identified gaps, accountable owners, and remediation timelines should be readily available to demonstrate that the bank's cyber and resilience plans are documented and executable. To the extent that a de novo institution is seeking a Federal Reserve master account, these capabilities are likely to be scrutinized by the Federal Reserve as well.
5. **Build an examination-ready evidence package:** An organized body of evidence can help management demonstrate how the cyber and resilience program aligns with applicable guidance and agency examination procedures. The package should connect regulatory expectations to policies, architecture, risk assessments, control inventories, testing results, incident procedures, third-party oversight, and recovery capabilities. Management should be ready to respond to regulators' information requests and be able to explain clearly how controls operate.

Where to go from here

Effective cyber risk management, resilience, and operational continuity practices are core regulatory expectations. Ahead of launch, banks should assess their current-state capabilities against the insights and actions outlined, prioritizing critical operations mapping, Day 1 control readiness, third-party oversight, and incident response preparedness. A resilience program should be built and organized to provide confidence that what matters most will run when it matters most. This will be critical for satisfying regulators' examination criteria and supporting sustained safe-and-sound operations.

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

Cyber Risk and Resilience

Meghana Kanitkar
Managing Director
Deloitte & Touche LLP
mkanitkar@deloitte.com

Paul Meynen
Principal
Deloitte & Touche LLP
pmeynen@deloitte.com

Daniel Soo
Principal
Deloitte & Touche LLP
dsoo@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 go to Deloitte independent senior advisor **Martin Henning** and Deloitte team members **Olivia Romeo** and **Ariel Marie Stevens** for their contributions and insights.

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.