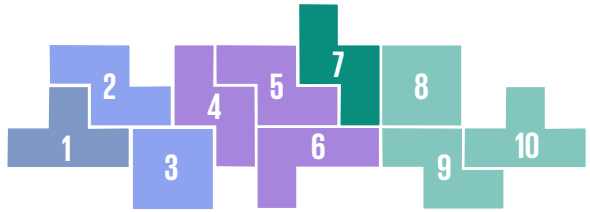
07 Ensuring Resiliency



Regulatory Signals

- **Business Continuity & Resiliency Planning**
- **Technology Interconnectedness**
- **Capital & Liquidity**

A growing focus on organizations' preparedness to withstand or recover from significant market stresses and disruptions that may impact non-financial operations (e.g., cybersecurity, technology) and financial risks (e.g., capital, liquidity).

"As banks advance their ambitions for expanded reach, management teams must operationalize strategic roadmaps that will enable them to thrive with a more competitive peer group."

KB Babar
Principal
Advisory

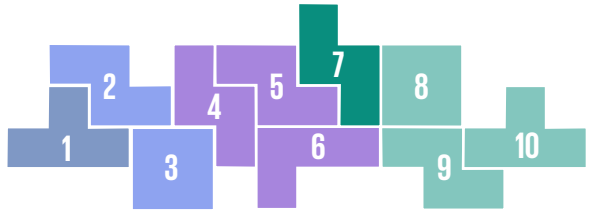
"Resilience is not achieved through isolated disciplines. Operational Resilience, Business and IT Continuity, and Incident and Crisis Management must converge into a single, integrated program—one that anticipates, absorbs, and adapts to disruption. Only through harmonized processes and unified oversight can organizations build the agility and strength required to thrive in an increasingly uncertain world."

Prince Harfouche
Principal
Advisory

"Tools such as AI and cloud services add complexities to an already complicated and interconnected environment. The speed with which these technologies are changing and the increasing reliance on them means organizations must continuously adapt their risk management, compliance, and operational strategies to keep pace with evolving threats and opportunities."

David Tarabocchia
Principal
Advisory

07 Ensuring Resiliency



Regulatory Signals

- **Business Continuity & Resiliency Planning**
- Technology Interconnectedness
- Capital & Liquidity

Signal

In response to increasing threats to information and technology security and complex interdependencies (e.g., supply chains, third-party service providers), regulators expect organizations to develop plans addressing critical functions, service-level agreements, and significant disruptions. Areas of focus include:

- Plan creditability (to maintain business continuity).
- Testing for critical operations and related third parties.

Consideration of easing expectations for some entities given certain overlapping requirements.

Examples

Actions from financial services regulators, including:

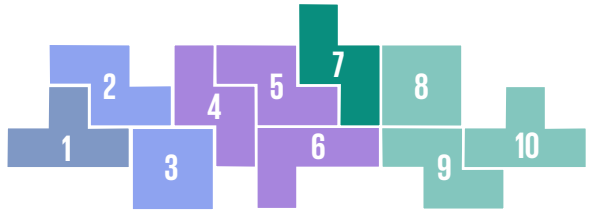
- Planning focused on “most relevant” information (e.g., FDIC FAQ)
- Potential easing of overlapping requirements (e.g., FDIC Statement (Hill) re: filers of FDIC IDI Rule and FDIC/FRB Title I plans; CFTC withdrawal of proposed operational resilience framework)
- Scrutiny of catastrophe resilience, pre-disaster planning, and cybersecurity (e.g., state laws related to P&C insurance)

Actions from other regulators including requirements for medical device supply chain disruption reporting (FDA) and data sharing on grid reliability (DOE).

What to Watch

- Possible FDIC proposal to, at a minimum, codify its 2025 FAQs into the agency’s IDI Rule and potentially also to streamline elements of the IDI Rule; concurrent consideration of streamlining requirements for entities filing pursuant to both the IDI Rule and the Title I Rule for BHCs
- Forthcoming compliance requirements with the OCC Recovery Planning Guidelines (staggered requirements beginning January 1, 2026) alongside a proposal to withdraw the Guidelines and related planning requirement
- Evolving/expanding regulatory expectations around operational resilience risk management practices (e.g., identifying critical operations and mapping interdependencies)
- Continued interagency collaboration on operational resilience

07 Ensuring Resiliency



Regulatory Signals

- Business Continuity & Resiliency Planning
- **Technology Interconnectedness**
- Capital & Liquidity

Signal

Elevated levels of operational risk reinforce the importance of operational and technology resilience, business continuity and incident response plans.

Risk attributed to cybersecurity and technology management largely due to third-party concentrations (e.g., cloud providers, FMUs, “off the shelf” software), increasingly sophisticated threat actors, and prolonged use of legacy systems.

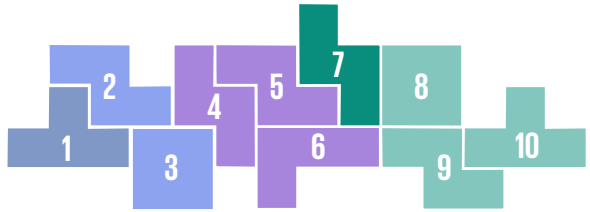
Examples

- OCC Semi-Annual Risk Perspective 2025
- OCC, FDIC 2025 Reports on Cybersecurity and Resilience
- Near-term risks in cyber resiliency and TPRM (e.g., FRB Statement (Barr))
- Top key risks including concentration risk, emerging technologies, and tech vulnerabilities (e.g., Treasury Financial Sector Risk Management Plan)

What to Watch

- Continued interagency coordination on operational resilience and cybersecurity supervision for large, complex, interconnected entities and significant third parties engaged in the delivery of critical services
- Continued interagency participation in FFIEC committees on cybersecurity, critical infrastructure and IT to share and align supervisory practices and efforts
- Potential reforms to IT examinations
- Heightened regulatory expectations for concentration risk assessments and contingency planning for critical service provider outages
- Potential for changing expectations related to cyber and ICT risk management, incident reporting, and third-party risk management along with resiliency planning, monitoring, and testing based on international requirements (e.g., DORA)

07 Ensuring Resiliency



Regulatory Signals

- Business Continuity & Resiliency Planning
- Technology Interconnectedness
- **Capital & Liquidity**

Signal

Actions to tailor regulatory requirements for elements of capital and liquidity based on institution size and risk, as well as providing for increased attention to transparency and accountability.

Examples

- Consideration of capital “modernizations” including stress testing, Basel III, community bank tailoring, indexing thresholds (e.g., Statements from FRB, FDIC, Treasury (Bowman, Hill, Bessent))
- Proposal to amend the ESLR (e.g., FRB, OCC, FDIC Interagency release)
- Proposals to reduce stress testing volatility and increase transparency (e.g., FRB, OCC, FDIC interagency release)
- Delay and reevaluation of liquidity risk management reporting (e.g., SEC Form N-PORT)

What to Watch

Continued focus on capital and liquidity “modernization” including:

- Final interagency rules on ESLR, transparency in stress test models and scenario development, and averaging of stress test results and related stress capital buffer
- Revision of the Basel III Endgame proposal
- Tailoring of community bank capital requirements, including the CBLR

Reassessment of the liquidity framework including:

- The role of the discount window and FHLBs
- Access to Federal Reserve “master accounts” as well as consideration of “skinny master accounts”
- Potential OCC codification of contingency funding plan expectations

07 Ensuring Resiliency

Regulatory Signals

- Business Continuity & Resiliency Planning
- Technology Interconnectedness
- Capital & Liquidity

Relevant Thought Leadership

Be organizationally and operationally resilient when—and where—it matters

Operational Resilience

Top Related Regulatory Challenges

01 Executing Mandates

03 Maintaining Cyber & Data Security

08 Driving Capital Formation & Growth

10 Enhancing Parties & Workforce