Achieving operational resilience

Bank Governance Leadership Network

May 2019

Bank Governance Leadership Network

May 2019

BGLN

VIEWPOINTS

Achieving operational resilience

> *"The conversation has really changed in the past year. The board needs to truly understand critical business services both for the bank and the market."*
> — Participant

Customers' increasingly demanding preferences and the evolving competitive landscape are putting pressure on banks to be innovative and agile. Despite the capital and energy recently invested in technology, many major banks remain in the early stages of becoming truly digital organizations. To date, investment dollars have focused primarily on enhancing customer service and efficiency, but these improvements have often been layered over or supported by decades-old 'legacy' systems that often obstruct the banks' achieving the full potential of end-to-end digitalization.

Becoming a fully digital financial institution creates new challenges to operational resilience from the significance of relationships with third-party platform providers, the further digitization of financial services, and ongoing threats to cybersecurity. Information technology (IT) outages and system-migration failures have captured the attention of frustrated customers, the media, politicians, and regulators. As banks maintain and replace their systems architecture, it will be critically important to embed operational resilience into planning and implementation.

On February 27 (London) and March 7 (New York), 2019, BGLN participants met to discuss the ways incumbent banks are approaching operational resilience: How should management teams, boards and regulators think about a topic as broad as operational resilience? What role should impact tolerances play in the future? How should banks test for operational resilience?

This *ViewPoints* synthesizes the key themes which emerged from the discussions in each of these meetings, and from conversations with network participants beforehand and immediately afterwards. These meetings also included discussions on upgrading legacy banking platforms. Themes from those parts of the discussions are summarized in a separate *ViewPoints*.

Operational resilience is a rising priority

The initial decade following the crisis focused on financial resilience, notably on capital and liquidity. However, over the last year or so, the focus for many regulators has shifted to operational resilience. As then-chair of the Financial Stability Board and Governor of the Bank of England, Mark Carney, put it, "An anti-fragile system must be as robust to operational failures as to financial ones."[1]

"Operational hiccups that nobody would've noticed years ago now are immediately noticed and amplified."

– Regulator

Regulators globally are shifting their focus to ensuring banks can continuously deliver services to their customers and withstand disruptions. Though different regulatory regimes are establishing their own definitions and expectations around operational resilience and are taking different approaches to overseeing the underlying issues, this is clearly emerging as a priority. One regulator said, *"What people need from a financial system has changed over the years. Operational hiccups that nobody would've noticed years ago now are immediately noticed and amplified."*

The Office of the Comptroller of the Currency (OCC) included operational resiliency as one of their priority objectives for 2019 and specified an "emphasis on maintaining information technology systems and remediating identified concerns."[2] In the UK in July 2018, the Bank of England, the Prudential Regulation Authority, and the FCA published a joint discussion paper entitled *Building the UK Financial Sector's Operational Resilience*.[3] The paper highlighted governance as a critical dimension, concluding that "Firms' and [financial market infrastructures'] boards and senior management are crucial in setting the business and operational strategies and overseeing their execution in order to ensure operational resilience." In January 2019, FCA head, Andrew Bailey, went as far as to suggest that banks should themselves link executive bonuses to IT resilience, or else the measure might be forced upon them.[4]

It is not just regulators driving this focus on resiliency. One director said, *"Our own standard in protecting against reputation risk is higher than what regulators will ask of us."* Customers are demanding 24/7 access, and new innovative digital technologies require continual operations. New business models require even greater dependency on third parties. The changing customer preferences that drive banks to vigorous innovation, along with more connection and increasingly digitized processes, are also creating new risks. Together, these factors are driving the focus on resilience in banks. System upgrades, while they should contribute to greater resilience, could be a significant contributor to increased outages in the short term. One regulator

said poor change management was often to blame: *"A lot of this is the result of poor planning around internal processes that the bank has control over."*

Despite—and because of—their large investments in technological improvements, banks regularly find themselves in the headlines (and in front of regulators) for outages, breaches, and downtime. In February 2019, the FCA announced a year-on-year increase of over 500% in technology outages at UK financial firms during 2018, as firms reported 145 breaches throughout the year, compared with 25 in the previous year.[5] A report from the FCA in late 2018 cited the greater consumer reliance on payments systems (over cash transactions) as a potential contributor to the increase in technology outages, as 2018 was the first year in which the total number of debit transactions was greater than total cash transactions.[6]

Banks must approach operational resilience holistically

"People always talk about the problems with legacy … more often than not—it's the shiny new application that's causing the problems."

– Regulator

Discussions around resilience have tended to focus on cyber-security and outage prevention. Regulators and experts alike are now urging banks to think more comprehensively about resilience, a concept whose breadth can make it difficult for boards to develop effective oversight practices.[7] A participant said, *"Thinking about this end-to-end is crucial. It's about what you're doing before, during, and after. It used to be just about prevention, but operational resilience has moved beyond that."*

Participants highlighted additional elements of an effective focus on resilience:

- **Resilience must be baked into digital transformation efforts.** Resilience needs to be a factor in any major tech transformation efforts. Institutions must ensure that any new initiatives or partnerships have been appropriately vetted and assessed for risk and that controls are in place. One regulator said, *"People always talk about the problems with legacy; sometimes that makes me laugh because—more often than not—it's the shiny new application that's causing the problems."*
- **IT upgrades carry risk but are necessary for long-term resilience.** It may be tempting to be cautious, in an atmosphere where banks continue regularly to make the headlines for IT and cyber concerns, but this very approach could induce resilience issues. An executive said, *"I've seen when you're over-cautious about small outages, you create a reluctance for change that can cause massive outages down the line."* Another participant asserted, for example, that *"you can get five times resilience running on the public cloud. We've tested it."*

- **Response strategy is critical.** As banks have improved digital offerings and given clients the scope to interface with bank services in real time, the downtime and response mechanisms are under pressure. A director said, *"We are victims of our own success. We built a mobile banking system that people rely on and so they're doing exactly that: they're relying on it."* Not surprisingly, banks are seeking out ways to better manage through crises and recognizing that preparation is key.[8] Some of the preparation includes *"considering the manner in which our customers are dealt with during a disruption,"* said one director, including considering whether and how to waive fees or provide alternative access to services to mitigate customer harm.

  One regulator said, *"You need to plan with failure in mind. Cyber makes that obvious, but the mindset needs to be pushed into operational business as well."* Continuous interaction between banks and customers means that when something goes wrong, the public outcry is more immediate and demanding, pushing firms to respond to service-interruptions faster than ever before. Boards must have well-established response plans if critical services go down. An EY SMA suggested boards should be asking, *"What are your 10 most critical business processes today? And what's the strategy when they go down? Put the probabilities aside: when it happens, are you comfortable where you stand? Will you be a week later?"*

> *"What are your 10 most critical business processes today? And what's the strategy when they go down?"*
>
> – EY SMA

- **Timely board involvement is critical.** An EY SMA noted that boards should ensure they are informed early on when an incident occurs: *"In almost every investigation we've seen, communications have not worked properly, and the board was not informed in a timely manner."*
- **Recovery and ongoing learning drives improvements**. After disruptions occur, firms need robust recovery plans that bring systems and data back on line in a well-controlled, reconciled manner. Each disruption provides an opportunity to learn and improve. As one director put it, *"We have started a large effort to determine what went wrong, and what can be done to improve across the firm."*

Setting impact tolerance is essential

A director noted that it is critical to consider impact tolerance in the context of customer expectations: *"If your tolerance doesn't line up with customer expectations, you may have a problem. Defining the threshold is very hard. You can't just say, 'We are OK with 1% of our customers being impacted', because that's still millions of customers for a very large bank. Plus, timing is a*

> *"If you are requiring perfect service, you will never get it. So, what's the definition of tolerable harm?"*
>
> – Director

big factor. Even if there's just one second of downtime, if it's the wrong one second it can be critical."

The joint discussion paper from UK regulators states that "Setting impact tolerances which quantify the amount of disruption that could be tolerated in the event of an incident may be an efficient way for boards and senior management to set their own standards for operational resilience, prioritize and take investment decisions. An example would be a maximum acceptable outage time for a business service."[9] Though it may be difficult to define for very large institutions, setting impact tolerances may help boards and management to consider what is needed to get comfort regarding the bank's operational resilience. A regulator said, *"The board role pre-disaster is becoming more important. In the past, you were focusing on the board role in response. Firms haven't always thought about recovery-time projections. Many firms don't even have an estimate! You should ask your management about this. The role of the board is to be informed on what management has done in this area."*

Some participants suggested that there may be benefits to banks and regulators working together to try to reset public expectations for banking systems. A director said, *"If you are requiring perfect service, you will never get it. So, what's the definition of tolerable harm?"*

A challenging aspect of the impact tolerance concept—and operational resilience, more broadly—is the need to consider the business service from end-to-end. Historically, firms focused on resilience of key assets or specific functions or activities. Now, regulators want firms to identify the most critical business services that they deliver to their customers and to the market, and map the entire process from customer, across the organization, to any third parties that support that process. *"Today, resilience plans have to include everything that supports delivery,"* said one regulator.

Third-party relationships are increasingly important

Banks are increasingly reliant on third-party technology providers, and some are considering going further in partnering with third parties to develop new platforms. Oversight of third-party risks has therefore become more critical for banks than ever before. A regulator said, *"The governance and maturity conversation we're having is incredibly important here. The blurred lines of responsibility with third-party providers are getting a lot of attention, and that will continue."* One executive noted that the risk is also expanding beyond third parties to include *"fourth parties, who we find out our third-party*

providers might be heavily reliant upon, but about whom we may know very little."

"Most resiliency issues we're seeing lately are from vendors."

– EY SMA

Participants discussed a few key aspects of third-party relationships:

- **Due diligence.** An EY SMA asked, *"Have you really tested your vendors? Most resiliency issues we're seeing lately are from vendors."* Several participants shared concerns regarding appropriate due diligence with third-party technology providers. A director said, *"If you ask the right questions and it still doesn't go right, what happens if the data is abused on that system? We can all ask the logical questions and maybe even get the right answers, but when it goes wrong and there is regulatory and political pressure to do something, that will be the real test."* Banks are identifying opportunities to improve information sharing and collaboration on third party risk management, including via industry-funded utilities.
- **Fintech partnerships.** Though several participants asserted the usefulness of partnering with fintechs in various areas, others advocated caution. One executive said, *"I think they are generally good at fraud detection but terrible at cybersecurity. They are usually not great at protecting the data that's been entrusted to them … As a general rule, there is a lot of risk associated with partnering with them."*
- **Cloud concerns.** A regulator said, *"Security of the cloud is their role; security in the cloud is yours (as the bank). Figuring out the bits of responsibility and service is important, and each provider offers different aspects of that. It is worth asking those questions: you want management to be very clear what they are responsible for and what the provider is responsible for."* One director noted that, although cloud providers are a relatively new entity in the financial services industry, they are not all that different from other third-party providers: *"I think you approach the question the same as you would for any other vendor. Remove the word 'cloud', and it's an IT vendor. You should apply the same rules you would otherwise."*

Data security is paramount

The daunting prospect of migrating vast amounts of bank data is a key execution risk in moving to new systems. The end goal is improved operations and resilience, but the transition can lead to systems failures or a loss of service or data. A participant said, *"Most of the challenges of migration are in the business domain and about defining how things will be migrated. When you think about migrating the design of your product, how many variants of the*

product you might migrate over … do you move them all over and what do you do with what you leave behind?" The participant added, *"It's a challenge, but there are a number of successful system conversions that have been done, so it's not impossible to do it."* Several participants noted that migrating data incrementally is a good approach, with one director saying, *"It's easier to migrate—within a bank—one system at a time, one platform at a time, one book at a time. But even that is challenging."* Participants broadly agreed that migration risk is a real threat and will continue to receive frequent attention in the boardroom.

"Data corruption is the nightmare scenario we should all be thinking about."

– Director

Participants also highlighted an area that goes beyond migration concerns: the integrity of bank data itself. As operational resilience continues to rise up the list of priorities for bank governance, several participants shared concerns specifically around ensuring and protecting data integrity. One director said, *"Data corruption is the nightmare scenario we should all be thinking about. If a data set at a very large bank is compromised, that could actually spell the end of a country's financial system."* Another director agreed, adding, *"It's miles above any other concern we have at the moment. It's an unconscionable situation to find yourself in as a bank."* Some participants noted that their firms have been conducting scenario-planning exercises in this area.

Testing and reviewing resiliency practices will increase

Banks undertake a broad set of table-top simulations across the year, ranging from cyber, to liquidity, to operational situations. However, some regulators say the testing currently being conducted in banks, even the largest firms, is insufficient. A regulator stated, *"The post-crisis view is not if something happens, but it has happened, so what do you do?"*

Supervisory expectations are becoming more demanding. A regulator said they will be conducting reviews of operational risk to include reviewing the resiliency of critical functions and what testing is being conducted. A participant suggested banks will be expected to demonstrate:

- What testing is being conducted?
- What is being tested and how frequently?
- How comprehensive is the testing?
- What has the testing revealed?
- What plans are in place to respond to issues identified?

An EY SMA suggested boards consider five questions regarding their oversight of operational and IT resiliency:

1. **Does the board know the firm's resilience strategy and how management is organized to manage resilience risk?** Has the board reviewed and discussed a resilience strategy that integrates operations, IT, and risk? Does the board know the roles of the COO/CAO, CTO, CISO, line-of-business leaders, and heads of resilience or business continuity? What is risk management's role? What is the role of internal audit?
2. **How should the board oversee resilience?** The risks related to resilience require full board attention, and specific aspects cut across risk, audit, and, where established, IT committees. Finetuning oversight will require agreed roles and responsibilities, distinguishing between resilience, cybersecurity, and privacy risks, and where these risks intersect.
3. **How can reporting to the board improve?** Is the board getting actionable, understandable information on significant initiatives and investments, major regulatory and supervisory matters, and emerging risks related to resilience?
4. **What is the role of the board in crisis?** increasingly, CEOs and their teams are participating in simulations to understand their roles and plans for managing through a crisis. Naturally, boards are starting to ask the same questions about their own role, how communication between management and the board will work in crisis, and when management will seek board input or approval.
5. **Does the board understand how resilience risk is going to be addressed as the firm transforms its business and operating models and technology?** Care is needed as firms transition away from core legacy technology platforms. Additionally, firms will increasingly depend on more and more third—and fourth and fifth parties—to operate. Some may enhance resilience, others may create new resilience risks. Some new technologies may bring their own resilience challenges: as firms depend more on automation, machine learning, and artificial intelligence, straight-through processing, and other emerging technology applications, ensuring resilience is built into those processes will be essential.

Addressing operational resilience challenges will take time. Adopting shared terminology, defining roles and responsibilities, and integrating issues that cross so many parts of the organization, will require a coherent strategy with board support and executive support.

About this document

About *ViewPoints*

ViewPoints reflects the network's use of a modified version of the Chatham House Rule whereby names of network participants and their corporate or institutional affiliations are a matter of public record, but comments are not attributed to individuals, corporations, or institutions. Network participants' comments appear in italics.

About the Bank Governance Leadership Network (BGLN)

The BGLN addresses key issues facing complex global banks. Its primary focus is the non-executive director, but it also engages members of senior management, regulators, and other key stakeholders committed to outstanding governance and supervision in support of building strong, enduring, and trustworthy banking institutions. The BGLN is organized and led by Tapestry Networks, with the support of EY. *ViewPoints* is produced by Tapestry Networks and aims to capture the essence of the BGLN discussion and associated research. Those who receive *ViewPoints* are encouraged to share it with others in their own networks. The more board members, senior management, advisers, and stakeholders who become engaged in this leading edge dialogue, the more value will be created for all.

About Tapestry Networks

Tapestry Networks is a privately held professional services firm. Its mission is to advance society's ability to govern and lead across the borders of sector, geography, and constituency. To do this, Tapestry forms multi-stakeholder collaborations that embrace the public and private sector, as well as civil society. The participants in these initiatives are leaders drawn from key stakeholder organizations who realize the status quo is neither desirable nor sustainable, and are seeking a goal that transcends their own interests and benefits everyone. Tapestry has used this approach to address critical and complex challenges in corporate governance, financial services, and healthcare.

About EY

EY is a global leader in assurance, tax, transaction, and advisory services to the banking industry. The insights and quality services it delivers help build trust and confidence in the capital markets and in economies the world over. EY develops outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, EY plays a critical role in building a better working world for its people, for its clients, and for its communities. EY supports the BGLN as part of its continuing commitment to board effectiveness and good governance in the financial services sector.

Appendix: discussion participants

In February and March of this year, Tapestry and EY hosted two BGLN meetings on upgrading core platforms and resilience. These meetings included more than 35 conversations with directors, executives, regulators, supervisors, and other thought leaders. Insights from these discussions informed this *ViewPoints*, and unattributed quotes from these discussions appear throughout.

The following individuals participated in BGLN discussions on upgrading core platforms and resilience:

BGLN Participants

- Homaira Akbari, Non-Executive Director, Santander
- Jeremy Anderson, Audit Committee Chair, UBS
- Mike Ashley, Audit Committee Chair, Barclays
- Aditya Bhasin, Chief Information Officer, Consumer Technology and Wealth Management, Bank of America
- Norman Blackwell, Chair of the Board, Nominations & Governance Committee Chair, Lloyds Banking Group
- Lee Bressler, Director, US Capital Markets Lead, Microsoft
- Amy Woods Brinkley, Non-Executive Director, TD Bank
- Pat Butler, Chair, Aldermore Group
- Juan Colombás, Chief Operating Officer, Lloyds Banking Group
- Jim Coyle, Non-Executive Director, HSBC UK Bank plc
- Andrew Dapre, EMEA Lead, Financial Services, Azure Engineering, Microsoft
- Michel Demaré, Vice Chair of the Board, UBS
- Beth Dugan, Deputy Comptroller, Operational Risk, Office of the Comptroller of the Currency
- Lynn Dugle, Technology & Operations Committee Chair, State Street
- Terri Duhon, Risk Committee Chair, Morgan Stanley International
- Betsy Duke, Chair of the Board, Wells Fargo
- Mary Francis, Reputation Committee Chair, Barclays
- Mark Gibbons, Chief Technology Officer, EMEA, BNY Mellon
- Nigel Hinshelwood, Non-Executive Director, Nordea; Senior Independent Director, Lloyds Bank plc and Bank of Scotland plc
- Antony Jenkins, Founder and Executive Chair, 10x Future Technologies
- Robin Jones, Head of Technology, Resilience & Cyber, UK Financial Conduct Authority

- Phil Kenworthy, Non-Executive Director, ClearBank
- Christine Larsen, Non-Executive Director, CIBC
- Callum McCarthy, Non-Executive Director, China Construction Bank
- Richard Meddings, Non-Executive Director, Deutsche Bank and Executive Chair, TSB
- Andy Ozment, Chief Information Security Officer, Goldman Sachs
- Mary Phibbs, Remuneration Committee Chair, Morgan Stanley International
- Nathalie Rachou, Risk Committee Chair, Société Générale
- Bruce Richards, Chair of the Board, Credit Suisse USA
- Patrick de Saint-Aignan, Risk Committee Chair, State Street
- Manolo Sanchez, Former Chair and CEO, BBVA Compass
- Alan Smith, Global Head, Risk Strategy, HSBC
- Danielle Vacarr, Vice President, Financial Institution Supervision Group and Governance & Controls National Co-Chair, Federal Reserve Bank of New York
- Suzanne Vautrinot, Corporate Responsibility Committee Chair, Wells Fargo
- Paul Williams, Senior Technical Advisor, Operational Risk & Resilience, Bank of England
- Tom Woods, Non-Executive Director, Bank of America

EY

- Omar Ali, Managing Partner, UK Financial Services
- Anthony Caterino, Vice Chair, Americas Regional Managing Partner, Financial Services Organization
- Olivier Colinet, Partner, Head of Cloud, Financial Services Advisory
- Dan Cooper, UK Banking & Capital Markets Leader
- John Doherty, Partner, Information Technology Advisory
- Steve Holt, Partner, EMEIA Financial Services Cybersecurity Leader
- Nik Lele, Principal, Financial Services Office
- Shankar Mukherjee, Partner, Financial Services Advisory UK
- Daniel Scrafford, Principal, Financial Services Risk Management Practice and Co-Lead, Global IBOR Transition Campaign
- Mark Watson, Deputy Leader, Center for Board Matters, Financial Services Office

Tapestry Networks

- Dennis Andrade, Partner
- Brennan Kerrigan, Associate
- Tucker Nielsen, Principal

Endnotes

[1] Mark Carney, "An Anti-Fragile System Needs Resilient Banks," *The Global Governance Project*.

[2] Office of the Comptroller of the Currency, *Fiscal Year 2019 Bank Supervision Operating Plan* (Washington DC: Office of the Comptroller of the Currency, 2018).

[3] Bank of England, Prudential Regulation Authority, and Financial Conduct Authority, *Building the UK Financial Sector's Operational Resilience* (London: Bank of England and Financial Conduct Authority, 2018).

[4] Karl Flinders, "UK Financial Services Regulator To Link Top Banker Bonuses to IT Performance," *ComputerWeekly.com* (blog), January 16, 2019.

[5] Madhumita Murgia, "Cyber Attacks on Financial Services Sector Rise Fivefold in 2018," *Financial Times*, February 25, 2019.

[6] Caroline Binham, "IT Failures at Financial Firms Have More than Doubled Says FCA," *Financial Times*, November 27, 2018.

[7] See EY, Getting serious about resilience: a multiyear journey ahead, December 2018.

[8] EY, Managing through crises: preparation is key, September 2018.

[9] Bank of England, Prudential Regulation Authority, and Financial Conduct Authority, *Building the UK Financial Sector's Operational Resilience* (London: Bank of England and Financial Conduct Authority, 2018), 7.