SPEECH

Things That Have Never Happened Before Happen All the Time

October 27, 2022

Joshua Rosenberg, Executive Vice President and Chief Risk Officer

Remarks at the Central Bank of Nigeria's Second National Risk Management Conference (delivered via videoconference)
As prepared for delivery

Good morning, good afternoon, or good evening depending on whether you are at the event in person or logging in remotely from another part of the world. I am very grateful to Dr. Blaise Ijebor for inviting me to present today at the Central Bank of Nigeria's Second National Risk Management Conference.[1]

Let me start by saying that the views I will express are my own and do not necessarily reflect those of the Federal Reserve Bank of New York or the Federal Reserve System.

Today, I'd like to share my perspectives, experiences, and learnings to reflect on how we can use risk management to enable us to achieve our goals even in the face of surprises and challenges. The main point I want to make is that, by integrating risk management into plans, decisions, and actions, we can succeed over a wider range of possible futures, not just the future we expect (or hope for).

I'll initially highlight a few potential misunderstandings that might prevent us from getting the most out of risk management.

The first is that risk management is mainly a way to stop bad things from happening. Of course, risk management should help us reduce the frequency and size of negative events and then recover more quickly and effectively when negative events occur.

But, risk management, in my view, should also help the right things happen by giving us tools to work more effectively.[2] Innovation is an essential tool to manage risks, because not changing can be riskier than changing. For example, an incredibly powerful risk management activity is to transform a slow, manual process that often fails into a fast, efficient, automated process that can self-correct when there is a problem. Clearly, it is just as important to understand the risk of not doing something as it is to understand the risk of doing something. And, when we understand our risk appetite and our risks, we can comfortably conduct controlled experiments, learn faster, and innovate. We're no longer driving in the dark; we're getting where we want to go with headlights on, and we can stay inside the guardrails and not skid off the road.

Second, risk management could be misunderstood as primarily the responsibility of risk management specialists. Actually, effective risk management is a way for everyone in an organization to help things go right. From the economic analysts to the cash processing operators to the software engineers, we can make better plans, decisions, and actions when we are prepared for change and have the capacity to adapt to surprises. So, most of the risk management that occurs in an organization will be done by people who don't have the word "risk" in their job title.

And third, risk management could be misinterpreted as an attempt to create a contingency plan for every possible thing that could go wrong. It is important to prepare by scanning the horizon, exploring the range of possible futures, and understanding how those futures could help or impair desired outcomes. We do want to invest in effective responses to key scenarios.

However, no organization has the resources to prepare for all possibilities. And, no matter how creative we are, we still can't imagine every one of them anyway. As it is said, "Things that have never happened before happen all the time."[3] So, effective risk management is more than planning. It is creating the capacity to adapt to and recover from unexpected shocks, which is what we often mean when we talk about resilience.[4]

To me, successful risk management is as much about culture as it is about structure. My version of the saying "culture eats strategy for breakfast" is: "culture eats structure for breakfast."[5] Practically speaking, we have policies, procedures, and rules to help us make decisions. But, much of the time, decisions aren't clear, and it is organizational culture that shapes the tradeoffs that we make and the actions we take. We want to define and chart a course toward our desired culture, so that individual decisions reflect the interests of the organization and the intent of the rules.[6]

To me, there are four central aspects of culture that support effective risk management: learning, listening, helping, and speaking up.[7] In a learning culture, we think about and plan for what might happen. And, we learn from experience, what went well and what didn't, so we can improve for next time. In a listening culture, we seek advice, appreciate a fresh perspective, and are open to

other's strengths, and helping when we have an opportunity. And, in a speaking up culture, we let our colleagues know when we see a problem or after something goes wrong so that we can get started fixing it.

Risk management is a creative, social process. It is a way of thinking, doing, and interacting. To bring it to life, we need to work together across the organization, staying continuously curious about the changing risk landscape and possible futures.

Risk Management During the Pandemic Crisis

Now, I'd like to share how our risk management practices and culture have helped us manage challenges throughout the pandemic crisis at the Federal Reserve Bank of New York.

In mid-March of 2020, the health crisis was especially severe in the New York City area, where our main office is located and where most of our employees live. To protect the health and safety of all employees and to continue our critical activities, we had to adapt to a situation none of us had ever seen before.

That started with changing how we worked. To reduce the health risks to our employees, we only allowed staff who had to be onsite to remain in the office, while everyone else worked remotely. For example, some open market operations, cash services, and technology support activities could only be conducted on location. To protect onsite staff, we implemented a range of protective measures including masking, social distancing, quarantine requirements, and staggered work schedules.

Another priority was helping employees cope with added responsibilities like lack of childcare and elder care, so we provided as much flexibility as possible to staff to manage their time.

On the technology side, we had an immediate need for teleconferencing bandwidth to support remote work. While not all technology worked perfectly right away, our technology providers quickly adjusted. With most staff working from home, a new risk we identified and addressed was the failure of home internet connectivity. Without going into detail, we've mitigated this risk, and successfully worked remotely through subsequent severe weather events.

Our business continuity planning and testing helped us navigate the early days of the pandemic, but this event was far more extreme than anything we had practiced, and we learned many lessons. I highly recommend a recent paper by the Consultative Group on Risk Management that brings together insights from central bank experiences managing business continuity risks during the pandemic.[8]

At the New York Fed, as we were changing where and how we worked, the pandemic's impacts spread to the economy and financial markets. From March to May 2020, gross domestic product in the United States fell by nearly one third (on an annualized basis) and employment dropped by 22 million. Equity markets sold off, and credit spreads surged to levels not seen since the 2008 Global Financial Crisis. Financial market functioning deteriorated with significant declines in liquidity; and, in the municipal bond market, underwriters cancelled new deals and municipal borrowing stopped.

In response to these conditions, the Federal Reserve System took action to support a strong economy and a stable financial system.[9] As part of this effort, pandemic crisis facilities were established to restore market functioning and support the flow of credit to households, businesses, and state and local governments.[10] The New York Fed was responsible for operating five of these facilities.[11]

Risk management was a cornerstone of that work, and we used our three-lines-of-defense risk model to build strong risk management into facility operations.[12] The first line of defense, the facilities teams, were responsible for understanding and managing their risks. The second line – my group (the Risk Group), the Compliance Function, and others – was responsible for independent assessment and oversight of those risks. And, the third line – our Internal Audit Group – was responsible for fully independent assurance.

Just to give a bit more detail about the second line of defense, we are responsible for designing and delivering a set of products, services, and relationships that lead to better plans, decisions, and actions that help the Bank thrive in any environment. We serve as trusted risk advisors, independent risk experts, and enterprise risk guardians.[13]

In our guardian role, we identify material risk issues and make sure that risks are understood, communicated, and addressed. We provide the stakeholders who are ultimately responsible for organizational success with a clear picture of the Bank's risk profile. In our expert role, we provide independent risk assessments, actionable risk insights, standards, and tools to help businesses manage risks. And, in our advisor role, we develop viable ideas and practical options to improve processes, controls, and business outcomes.

So, as the facilities were created, staff in my group joined the facilities teams to connect with the real-time information flow and decision making. That's because we knew that the traditional cadence of monthly meetings wouldn't work when decisions were being made by the hour or minute. And to be relevant, we had to accelerate to the pace of our advice to the speed of this

We also redesigned our risk management toolkit to see and address risks in real time. We started by working with the facilities teams to identify and triage the most significant risks. We partnered with experts across the Bank to cover the spectrum of financial and non-financial risks.

Once the facilities were operating, we created facility risk registers to further identify risks, prioritize responses, and track mitigation. We also looked for thematic risks across facilities that we could address in common ways. For several facilities, we more deeply analyzed end-to-end processes to further strengthen controls.

Because of our experiences during the Global Financial Crisis, we knew that facilities themselves and their risks had a lifecycle from design, to standup, to steady state operation, and finally to wind down and closure. So, this helped us better anticipate and manage the risks of the pandemic crisis facilities.

Vendor risk was a key area of focus for us, because vendors had critical roles in the operation of the crisis facilities including investment management and securities settlement. We had to create a fast and rigorous vendor onboarding and monitoring process, while at the same time recognizing new risks the vendors themselves faced across continuity, people, process, and technology. We made significant changes to our vendor management approach, many of which are serving us well today.

During the pandemic, we've adapted to a fast-changing, uncertain environment. We've seen how risk management has helped us respond effectively, used lessons learned to improve our approaches, and identified areas where we want to further develop our capabilities.

Building and Strengthening Organizational Resilience

Since then, we have continued to focus on how risk management can help us strengthen operational resilience, which "is the ability to deliver operations, including critical operations and core business lines, through a disruption from any hazard. It is the outcome of effective operational risk management combined with sufficient financial and operational resources to prepare, adapt, withstand, and recover from disruptions." [14]

A foundational component of resilience is that an organization can operate as a coordinated system in order to successfully adapt to changes in the environment. What does that take? Let's reframe the core components of operational risk – people, process, and technology – using a resilience lens.[15]

People are resilient when they are ready and able to adapt to change by adjusting priorities, replanning, and refocusing activities and resources. Resilient staff work with shared purpose across organizational siloes, operate effectively in environments of uncertainty and ambiguity, and are empowered to develop creative and innovative solutions.

Processes are resilient when they are robust to changing internal and external conditions, including issues with suppliers, inputs, processing, outputs, and customers. Resilient processes provide clear signals of their operating state, have the right level of automation, and continue to function under stress.

Technology systems are resilient when they are flexible, robust, and able to be recovered rapidly.

And then the overall organization is resilient when these three components – people, process, and technology – work together effectively. Resilient processes and technology should support the ability of the staff to successfully manage in normal times and during disruptions.

What are some concrete steps to strengthen resilience? In terms of processes, an important first step is to identify the processes that are critical to achieving organizational objectives. Gains are often found through simplification and automation of manual processes, especially when combined with performance metrics and risk metrics that provide real-time measures of process health.[16]

For technology, modernizing technology and software development processes can be a key area of focus. One goal is to create a fast, robust, and secure software development lifecycle that stays current by design (perhaps enabled through the agile development methodology and cloud platforms). And, approaches like red-teaming, threat hunting, and external benchmarking can provide insight into cyber resilience strengths and areas to improve.[17]

On the people side, does the current organizational culture help people successfully adapt to rapidly changing environment? Do staff have the skills that are needed to achieve organizational objectives today and in the future? These are important questions to explore and potential priority areas to address if there are mismatches.

Final Thoughts

I'd like to wrap up with a bit of realism followed by optimism. Here's the realism: while we might prefer never to be surprised, we will be. The optimism is: effective risk management can help us be less surprised and respond better when we are. And, a strong

[1] I would like to thank Greg Gaskel, John Reda, Dubra Shenker, David Stein, and other colleagues at the Federal Reserve Bank of New York for their feedback.

[2] See, for example, the concepts of Safety I and Safety II in Eric Hollnagel, Jorg Leonhard, Tony Licu, and Steven Shorrock, 2015, "From Safety I to Safety II: A Whitepaper," Eurocontrol.

[3] Scott D. Sagan, The Limits of Safety: Organizations, Accidents, and Nuclear Weapons, 1993, Princeton University Press.

[4] Basel Committee on Banking Supervision, "Principles for Operational Resilience," March 2021. Joshua Rosenberg, "Thrive in any Environment: Strengthening Resilience through Risk Management," November 2019.

[5] Quote Investigator, "Culture Eats Strategy for Breakfast," May 2017.

[6] Financial Stability Board, "Guidance on Supervisory Interaction with Financial Institutions on Risk Culture: A Framework for Assessing Risk Culture," 2014. The Institute of Risk Management, "Risk Culture Resources for Practitioners," 2012.

[7] These are adapted from safety culture concepts in, 1997, Ashgate Publishing. See also, GAIN Working Group E, "A Roadmap to a Just Culture: Enhancing the Safety Environment," September 2004.

[8] Risks highlighted include information and cyber security risks, physical and psychological health risks, technology risks and dependencies. See, Consultative Group on Risk Management, Bank for International Settlements Representative Office of the Americas, "Business Continuity Planning at Central Banks During and After the Pandemic," April 2022.

[9] Chair Jerome H. Powell, "Coronavirus and CARES Act," Federal Reserve Board of Governors, June 2020.

[10] Federal Reserve Bank of New York Economic Policy Review, Special Issue: Policy Actions in Response to the COVID-19 Pandemic, June 2022.

[11] Daleep Singh, "The Fed's Emergency Facilities: Usage, Impact, and Early Lessons," July 2020.

[12] Institute of Internal Auditors, "The IIA's Three Lines Model: An Update of the Three Lines of Defense," July 2020.

[13] For a "multiple roles" perspective of risk managers, see Matthew Hall, Anette Mikes, and Yuval Millo, "How Do Risk Managers Become Influential? A Field Study of Toolmaking and Expertise in Two Financial Institutions," April 2012. Also, see, Ben W. Heineman Jr., The Inside Counsel Revolution: Resolving the Partner-Guardian Tension, 2016, American Bar Association.

[14] Board of Governors of the Federal Reserve System, Division of Supervision and Regulation, "SR 20-24: Interagency Paper on Sound Practices to Strengthen Operational Resilience," November 2020. Also, see Striving for Operational Resilience: The Questions Boards and Senior Management Should Ask," Oliver Wyman, 2019.

[15] Basel Committee on Banking Supervision, "Revisions to the Principles for the Sound Management of Operational Risk," March 2021.

[16] Nathan Furr, Andrew Shipilov, Didier Rouillard, and Antoine Hemon-Laurens, "The 4 Pillars of Successful Digital Transformations," Harvard Business Review, January 2022.

[17] Bank for International Settlements, "Cyber-Resilience: Range of Practices," December 2018.