Joshua Rosenberg: Operational risk management at the Federal Reserve Bank of New York

Remarks by Mr Joshua Rosenberg , Executive Vice President and Chief Risk Officer of the Federal Reserve Bank of New York, at the 18th Annual OpRisk North America 2016 conference, New York City, 15 March 2016.

* * *

Good morning. I would like to thank the organizers for inviting me to speak at this year's OpRisk North America conference. Today, I will share my perspectives on operational risk based on my experiences at the Federal Reserve Bank of New York including those in my current role as the Bank's Chief Risk Officer. Before I begin, I wanted to state that the views I will be expressing are mine and do not necessarily reflect those of the Federal Reserve Bank of New York or the Federal Reserve System.

As you know, operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems, or external events. The New York Fed faces operational risks because, like other public and private institutions, it relies on people, processes, and systems to execute its objectives, and, in the same way, the Bank is subject to external events that can impact the effectiveness of our people, processes, and systems.

To give you a better sense of the New York Fed as an operational entity, I wanted to touch briefly on the broad range of the Bank's operations. Most familiar are likely to be the Bank's execution of market operations to implement monetary policy directives of the Federal Open Market Committee and financial supervisory activities. As significant in the Bank's operational profile are the financial services that the Bank provides to the U.S. government, financial institutions and businesses, and to foreign central banks and international institutions. Notably, the Bank operates the Fedwire® electronic payments and securities transfer service, which is a critical part of the nation's payment system infrastructure. The Bank performs fiscal agency functions for the U.S. government including the auction of Treasury securities, and it provides correspondent banking and custody services to foreign central banks and international institutions.[1]

The Bank's risk framework

Operations imply operational risk, so how does the Bank approach operational risk management? Let me back up for a moment, since a useful starting point to answer this question is to begin by describing the Bank's overall approach to managing risk within the Bank's risk framework.

In particular, the risk framework is designed to enable the Bank to understand and communicate its risk profile to key stakeholders, assess how risks may change in response to planned activities or changes in the environment, take action to ensure risks remain at acceptable levels, recover quickly and effectively from risk events, and continuously improve the effectiveness and efficiency of the risk management.

As part of the risk framework, the Bank defines risk management roles and responsibilities using the three lines of defense model.[2] The three lines of defense model creates a set of layered defenses that align responsibility for risk taking with accountability for risk control and provide effective, independent risk oversight and escalation. In the three lines model, the assignment of risk management roles is clear and comprehensive in order to prevent gaps,

---

1 https://www.newyorkfed.org/aboutthefed/fedpoints.html.

2 IIA Position Paper: The Three Lines of Defense in Effective Risk Management and Control, January 2013.

ambiguities, or overlaps in responsibility. More specifically, the business areas are the first line of defense, independent risk management units are the second line of defense, and internal audit is the third line of defense.

In the Bank, the first line of defense is comprised of the business areas that execute and support the execution of the Bank's mission. These first line units are responsible for both the operational activities that result in risk as well as control of the resulting risks. The first line "owns" its risk in the sense that it is accountable for both positive and negative outcomes and is empowered to manage the distribution of outcomes.

At its core, the three lines model recognizes the strong incentives for effective risk management created by aligning accountability and responsibility. In other words, from the perspective of the first line, there is "skin in the game," and risk management is not viewed as someone else's problem. In addition, putting the first line in charge of risk management has efficiency and effectiveness benefits, since the first line can adapt risk solutions to its specific needs and nimbly respond when the risk environment changes.

The Bank's second line of defense – independent risk management areas including my Group, the Risk Group – provides independent assessment and oversight of the risks taken by the first line as well as frameworks that provide a common structure for risk management processes and practices. The second line also provides an integrated view of risk to senior stakeholders through consolidated analysis of the Bank's risks.

A second key insight of the three lines model is that a layered defense increases safety and reliability by providing an independent check that reduces the chance of error. The second line is the second layer, and provides a view of risk that is independent of the business area's assessment. What is the value-add from having this type of second opinion? To start, while the business has the deepest understanding of its environment, operations, and objectives, the second line offers a perspective based on expertise in risk identification, analysis, and mitigation that is informed by its institution-wide view of operations and risks. This allows the second line to provide unique insights by aggregating risks across business lines, identifying interactions across risk types, and spotting anomalies in risk exposures or risk practices that deserve additional attention. There also may be externalities to actions taken in one business line that have implications for the risk of the institution as a whole; it is the second line's responsibility to articulate that perspective to senior management.

The second line's responsibility for establishing a common framework for risk management creates benefits in terms of both efficiency and effectiveness. The second line is an institution's center of excellence in risk management and is in an ideal position to identify and promulgate best practices and standards. In terms of efficiency, the second line is well-positioned to collect and analyze risk information coming from all of the business lines, to provide common risk management tools, and to provide guidance to business areas to improve their risk management capabilities.

The Bank's third line of defense, Internal Audit, provides assurance to senior management and the Board of Directors that first and second line risk management and control activities are effective. Although I did not say it before, the second line is not fully independent of management. This is because second line risk management (in our case, the Risk Group) is involved in a broad range of management decisions related to the Bank's risk controls, and, in terms of reporting lines, I am part of the Bank's Management Committee and report to the Bank's president. Our Audit Group, however, provides a fully independent, final layer of defense. Internal Audit does not participate in management decisions, and our General Auditor reports to the Chair of the Audit and Risk Subcommittee of the Bank's Board of Directors.

In addition to defining clear and comprehensive risk management roles and responsibilities using the three lines of defense model, the Bank's risk framework establishes governance, escalation, and reporting processes around risk exposures, risk decisions, and risk events. A

strong governance regime provides assurance to stakeholders (Management Committee, the President, and the Board) who delegate risk-taking authority to the business lines.

From first-line businesses and support functions, risk information flows to the second line, and then to the Risk Subcommittee of our Bank's Management Committee. The Risk Subcommittee discusses significant emerging and existing risks, provides perspectives on managing and mitigating risks, and supports Management Committee review and decision making. The Audit and Risk Subcommittee of the Bank's Board of Directors and the Board of Directors itself are at the top of the governance chain, although there are limitations on their roles with respect to supervisory and monetary policy issues.[3]

Operational risk management

The Bank's operational risk approach sits within, and is shaped by the Bank's overall risk framework. Roles and responsibilities as well as escalation and reporting follow the general structure I previously described. At this point, though, I can drill down into operational risk specifics.

In the first line of defense, operational risk management is conducted by staff in the front line units with support from first-line's centralized risk management resources (usually as part of a business' shared services function). The first line is responsible and accountable for the identification, analysis, management, and monitoring of the operational risks that arise as a result of its activities.

Second line operational risk management is led by the Central Operational Risk Function in the Risk Group. Central Operational Risk provides independent assessment and oversight of first-line operational risks and risk management practices and is responsible for maintaining and enhancing the Bank's operational risk framework.

Our third line, Internal Audit, assesses the design and implementation of the operational risk framework and provides feedback on risk issues as an observer on governance committees.

The foundations of the Bank's operational risk program are the risk event reporting process and the risk and control self-assessment process. These processes are central to risk identification, analysis, and response. The risk event reporting process involves real-time collection, classification, analysis, and escalation of operational risk events including establishment of root causes and determination of remediation plans. You are all likely familiar with reporting risk events that have impacted your institution and categorizing them as low, moderate or significant. We do this as well. In addition, we require reporting of near miss events, which is when a control failure has occurred but we've been fortunate that there was no impact to the Bank. These near miss events are a window into vulnerabilities that could cause an adverse impact in the future.

The risk and control self-assessment process establishes a methodology for business areas to periodically assess their operational risks and ensure that appropriate mitigation is in place for key business processes. Importantly, the Central Operational Risk area is responsible for synthesizing the outputs of these two processes, along with follow-up discussions with business areas, to identify significant Bank-wide residual operational risks.

We have found it useful to view operational risk through the lens of processes, risks, and controls. We have defined a comprehensive set of processes to characterize the Bank's primary services and transactions. Along with that, we have articulated a standardized set of risk drivers, risk events, risk event impacts, and, finally, controls that prevent, detect, or mitigate the consequences of a risk event. We are using this risk taxonomy on a forward-

[3] https://www.newyorkfed.org/aboutthefed/audit.html.

looking basis to assess the risks of Bank processes and as an analysis tool to investigate risk events after the fact.

Using standardized process, risk, and control types allows us to aggregate as well as slice and dice our risks around dimensions of interest. For example, we identify processes associated with the highest levels of residual risk and the largest number of risk events as areas for additional attention. It may be the case that additional mitigation is required or there are weaknesses in controls. We identify common control profiles for process types and assess their effectiveness based on risk ratings and past risk events. That informs the second line's recommendations to business areas on control protocols. We also use the common control profiles to assess where we are over-controlled and have the opportunity to shift resources to other priorities.

The risk information collected and the risk analysis performed by the second line is the basis for operational risk reporting in the Bank's risk profile report that is presented to the Risk Subcommittee, the Management Committee, and the Audit and Risk Subcommittee. The risk profile report shows the Bank's most significant risks (including operational risks) along with a risk rating and the status of mitigating actions and mitigation plans. In addition, the report highlights significant and notable risk events along with the event's impact, root causes, and remediation activities. We have found that the risk profile report provides the necessary flow of information to create meaningful committee dialogue around risk issues, feedback to business areas, coordination across Groups and lines of defense, and when necessary, additional escalation.

Past, present, and future

As the theory and practice of operational risk management and the complexity of our operations have evolved, so has our approach. In the mid-2000's, the Bank formalized its operational risk program. That included starting a Bank-wide Operational Risk Committee (a predecessor to the Risk Subcommittee) led by the First Vice President, establishing the risk event reporting and risk control self-assessment processes, and creating the Centralized Operational Risk Function (then located in the Bank's Corporate Group). Later developments included instituting new Bank-wide control policies reflecting a deeper understanding of sources of operational risk. For example, the Bank established policies to govern end-user developed automation tools and the management of contingent workers.

The past several years have been characterized by a focus on integration of the Bank's risk management program. As part of a review of the Bank's governance, the Risk Subcommittee of the Management Committee was established with a broad risk management mandate spanning financial, operational, and compliance risk. The Bank also enhanced the coordination of risk management, resource allocation, and strategic planning through linkages between the Risk Subcommittee and our planning and resources committee. Most indicative of this trend was the establishment in 2015 of the Risk Group's Enterprise Risk Management Function which is responsible for providing an integrated view across all of the Bank's risks.

In thinking about areas for future improvement, I ask myself: How can we accelerate organizational learning from our mistakes? Does our analysis of risks and risk events sufficiently reveal organizational and structural issues that contribute to the risk? How can I further create a positive risk culture that encourages reporting and escalating of risk issues? Are we finding the right balance in our controls between specificity of rules and the adaptability of principles?

These and other questions will continue to focus us on improving and enhancing our policies and practices with the goal of supporting the Bank's ability to manage risk within its risk tolerance.

Thank you.