Remarks by

Deputy Comptroller for Operational Risk Carolyn DuChene

Before

OpRisk North America

March 27, 2014

Good morning. I hope you are enjoying the conference this week. The agenda contains an excellent array of topics for all practitioners in the area of operational risk. I hope, too, that you're networking with colleagues, making new connections, and sharing lessons learned. I'm a firm believer that while we can learn from our own mistakes, it's better if we can learn from those of someone else. Though, candidly, over the course of my 30-year career in bank regulation, I've had my fair share of learning experiences.

One of the strong features of the OpRisk North American conferences is the balance between operational risk quantification and risk management issues. That balance is important. The industry and regulators have been working diligently since 2007 to implement capital measurement approaches and wrestle with challenging technical issues linked to modeling operational risk exposures. That effort has paid off. Banks are making progress and quantification approaches are starting to mature. You do not have to look any farther for evidence of this than the recent announcement that eight U.S. firms are now permitted to use the advanced approaches to determine risk-based capital requirements. That is a significant step. However, banks and supervisors need to do more to ensure a balanced focus between capital measurement and risk management. Significant operational events remain all too common these days. As a result, operational risk is a board-level discussion topic across the financial services

industry. The toll these events take on banks is considerable, not only in terms of direct remediation costs but, equally, if not more importantly, the impact on banks' reputations and trust with their customers. Comptroller of the Currency Thomas Curry and the OCC have emphasized the importance of sound operational risk management, robust governance oversight, and a proactive risk culture. So, today, I'd like to highlight some of the risk drivers that pose distinct challenges and why the right responses, the right approaches to effective operational risk management and oversight, are so important.

While my remarks focus on large and midsize banks, there may be lessons that community banks can take away to help them meet the operational challenges that they face, such as the importance of maintaining strong audit functions, and ensuring robust governance and oversight when they are leveraging third parties . The environment is challenging for all banks, and all banks will need a healthy risk culture for the industry to prosper. There are a great number of factors that make today's operating environment difficult.

First, the current operating environment is challenging because of the volume and velocity of change occurring within individual banks and across the industry. Banks—and their supervisors—are going through a period of tremendous adjustment that began a half decade ago. Obviously, part of that change is a direct result of the financial crisis. The losses from legal judgments, regulatory fines related to foreclosure processing, BSA/AML and business practices, and lapses in the oversight of trading activities—caused banks to address internal flaws in oversight, operational controls and processes, and incentive compensation schemes. Another important driver of that change is that the economy, while improving, remains challenging. Loan growth appears to be improving, but banks are still struggling with compressed margins and fewer opportunities to increase noninterest income. Banks and thrifts continue to grapple

with ways to control expenses. Nonbank entities provide significant competitive pressures on a number of fronts by providing innovative products, state of the art technology, and aggressive pricing models. Regulatory change is another challenge in the current environment—driven in part by new laws such as Dodd-Frank that were passed to address some of the hard lessons from the recent financial crisis.

Banks are responding to these drivers—internal adjustments and a challenging operating environment—in a number of ways. Many banks are rethinking their strategy and business models. A number are launching new products or entering into new business lines. Some are deciding to divest non-core assets. Banks also are overhauling business processes and legacy technology to address new and emerging business demands and to meet heightened internal and regulatory requirements for better risk management information.

A change in strategy or in core business process often is vital to success, and in some instances is essential to survival. However, change of this magnitude sometimes has unintended or unforeseen consequences. Consider the originate-to-distribute business model. It seemed like an innovative way to generate noninterest income, manage balance sheet size, meet a burgeoning demand from consumers, diffuse risk to avoid concentration, and meet investor demand for new securities that could be customized to meet risk and yield requirements. The model worked for a while. Then some unintended consequences began to appear. The drive for revenue led to compensation plans that didn't align behavior with risk management requirements and led to underwriting processes that ceased focusing on quality and borrower capacity. The tranching and repackaging of cash flows into new types of securities, combined with inadequate data architecture and poorly linked systems, made it harder to know where the risk was and whether it had concentrated in some new way. When those poorly underwritten loans began to stumble, the

failure to supervise third-party law firms and collection companies led to abuse of customers and numerous lapses in controls and violations of law.

Increasingly, banks are addressing operational challenges by turning to third parties for expertise they lack internally, for expense control and for faster time to market with products or services. For some, this has become a new business model in which they handle only the most core parts of the business and turn the rest over to third parties. They are able to source staff and processes from the lowest cost provider. They can leverage higher levels of expertise from a menu that includes options from around the world. The Internet and software-as-a-service solutions enable banks to implement mix-and-match systems that are customizable with the best of breed choices. The marketplace offers an outsourced, third-party solution to almost every backroom process—including customer acquisition, underwriting, collections, litigation, payments, payroll, Web management and Internet banking, backup and disaster recovery, and quality assurance activities like loan review and audit.

However, as the level of outsourcing proliferated across all sizes of institutions, we observed some unintended consequences. Due diligence required greater breadth and depth, intellectual property challenges arose more frequently, and dispute resolution with third parties—sometimes on the other side of the world—became more complicated. We also began to see misaligned compensation and incentive schemes in some of the third-party relationships involving direct marketing activities to bank customers. Risk management became more daunting because the level of expertise around systems and processes waned as reliance on third parties increased. These trends are precisely why the OCC issued updated guidance on the risk management of third-party relationships. That guidance states clearly that a bank's use of third parties does not diminish the responsibility of its board and senior management to ensure that the

activity is performed in a safe and sound manner and in compliance with applicable law. It outlines our expectation that banks should adopt risk management processes commensurate with the level of risk and complexity of their third-party relationships and ensure comprehensive risk management and oversight of third-party relationships involving critical activities.

That's a significant amount of change as banks make internal adjustments coming out of the financial crisis and cope with a difficult economic and changing regulatory environment. But wait, there's more.

A third risk driver is the increasingly interconnected and interdependent world that includes a growing number of dependencies and concentrations. The chain of relationships is getting longer and more complicated. At the same time that banks are providing their customers with quick and easy access to account information and products, their own information systems are becoming increasingly linked to those of third parties. It's worth noting, too, that the risks associated with interconnectedness are further amplified by dependencies on other industry sectors, such as telecom and energy, and by the continued buildup of service provider concentrations. One can't help but notice the ongoing consolidation among the firms that provide core transaction processing services. A smaller number of technology service providers are providing a greater amount of services for an increasing number of banks. Those concentrations, and the potential magnitude of impact exposure, warrant close attention, both from the banks that are the clients of these firms as well as the supervisory agencies. Finally, as demonstrated by the recent and ongoing merchant breaches, banks are connected—and exposed—indirectly to vulnerabilities over which they have no direct control.

This brings me to the fourth risk driver I want to highlight today—something that has the attention of nearly every C-suite in America—the evolving and increasingly sophisticated cyber

threats. I want to spend some additional time on this operational risk driver in particular, because the threats often target the weaknesses posed by the interconnections and interdependencies throughout the banking sector.

Distributed Denial of Service (DDoS) attacks targeting banks have been sporadic for a year and a half. More attacks can occur at any time as cybercriminals continue to change their tactics. A number of firms that monitor and report on information security issues indicate that DDoS attacks are increasing in intensity, as measured by the number of packets directed at target firms per second, resulting in significant waves of Internet traffic to Web sites. In addition, the attack vectors are shifting from the application layer to the infrastructure layer. For non-technical types like me, this means that the attack focus is changing from customer-facing software to the platforms and operating systems on which that software runs. As you well know, a successful attack on a bank's infrastructure layer could have far-ranging consequences on a bank's core systems. Fortunately, banks have successfully defended against these attacks, which up to this point have been mostly designed to disrupt operations and the availability of Web-facing applications. Information sharing among institutions has helped banks respond to shifting tactics. That success certainly hasn't been without some cost. It takes significant resources to mitigate an attack, often involving both internal staff and external service providers. In addition, the increased time and resources spent fending off DDoS attacks have an impact on banks' ability to attend to other core activities, such as performing normal maintenance or overhauling legacy systems. Importantly, during a time where bottom lines aren't growing as fast as expected, these attacks can diminish banks' ability to support the development of new products and services. We're also seeing instances of DDoS attacks being used as a diversion for

attempted fraud, which is one of the reasons the OCC issued an alert on *Distributed Denial of Service Attacks and Customer Account Fraud*.

The cyber threats aren't just focused on disrupting operations. We know that other cyber attackers are attempting to install malicious software to gain permanent footholds in networks so that they can monitor the activity and steal intellectual property. These cybercriminals are persistent and innovative. They work hard to exploit vulnerabilities in the banking, customer, and third-party systems to steal credentials, initiate account takeovers, reset security controls, introduce malicious software, and conduct other illicit activity. Whether the objective is disruption, fraud, theft, or something else, an attack can not only damage the reputation of a single institution; it can undermine overall confidence in the entire financial system. While the banking industry has a good track record in warding off these attacks, other industries have not been as successful.

Given the risk drivers internally and in the environment, and the volume and velocity of the change that's occurring, we—banks and supervisors—need to maintain heightened awareness and make sure banks remain sufficiently agile and forward-looking in their risk management and governance to ensure safe and sound operations. The breadth of change will not narrow soon. The level of business environment complexity will not become simpler. While complacency has its own risks, the risks associated with change can be even greater. In fact, risks associated with change are among the top challenges identified in the OCC's *Semiannual Perspective on Risk.*

Managing the process of change is an important and fundamental principle embedded in risk management frameworks. Appropriate policies, people, processes, and systems must support the framework. When the risks associated with change are not well understood and

when the execution of strategies and plans are not well managed, the consequences can be substantial. A poorly managed change process is a risk to your business and it can increase both strategic and reputation risks. That's how the change process should be handled: as a real business risk, not as a regulatory-driven compliance exercise or process.

Let me bring our discussion today around to where I see opportunities to strengthen operational risk management in the industry. Frankly, as a supervisor, I've seen numerous examples where the quality of risk management simply hasn't always kept pace with the velocity and breadth of change and the rapidly evolving threats in the environment. For one thing, too often the knowledge and awareness of these risks and threats are siloed in the operational risk management area. That approach is too narrow. Risk awareness, risk identification, risk assessment, and controls need to be pervasive in your organizations. Let me use cyber threats as an example. Cyber threats are more than an information security risk and more than an operational risk. They pose a risk to every element of your business model, a risk to your strategy, and a risk to your reputation. Cyber threats are not just a technology issue. If managed only from a technology perspective, a bank misses the opportunity to identify and plug holes and vulnerabilities. The breach at Target was the result of criminals gaining access through compromised vendor credentials. Whether its spear-phishing e-mails, social engineering phone calls, or the flash drive found in the parking lot, there is a human component to the vulnerability, and it can exist anywhere in your firm, or at any of your third-party relationships, or with your customers. This type of threat requires a comprehensive business—not just an operational risk—response.

In a world where the velocity of change is accelerating, the breadth of that change is widening, and the resulting complexity is mounting, it's appropriate for banks and supervisors to

ask whether existing organizational structures are sufficiently agile, and whether the tools, techniques and technologies being used are sufficient for the changing environment. Those are areas that our supervisory strategies are set to explore in the coming year. Those are the same areas where opportunities exist to improve operational risk management. Business lines—increasingly recognized as the organization's first line of defense—are not always exhibiting the needed robustness in risk-control self-assessments and emerging risk identification. In a number of operational models, technology is being developed at, deployed from, and managed by the business lines. Where this is the case, the first line of defense must understand the risks and be held to the same standards for risk management as technology units.

The second line of defense—the independent risk management functions—is increasingly being stretched thin. More worrisome, in too many instances second lines of defense are inadequately staffed, experience high turnover in critical leadership positions, or are insufficiently engaged with identifying, assessing, and monitoring the risks associated with strategic and business model change. The second line of defense needs adequate resources, stable and strong leadership, and extensive rather than narrow engagement.

In keeping with our historical approach, in January of this year, the OCC issued for comment proposed formal enforceable guidelines establishing heightened standards for large insured institutions with $50 billion or more in average total consolidated assets. These heightened standards build on lessons learned from the financial crisis and would require the establishment of a risk governance framework that covers all risks, including operational risk. It also addresses the roles of the frontline units, independent risk management, and internal audit in implementing the framework into all aspects of a bank's operations.

In the search for solutions to make your bank stronger, don't overlook the opportunity to embrace the foundational guidance provided by the Basel Committee on Banking Supervision's *Principles for the Sound Management of Operational Risk*, issued in June 2011. The principles are certainly a great foundation for any operational risk framework. If your bank has implemented all of these principles, if it rigorously assesses the quality and robustness of that implementation, and if it continuously seeks out emerging better practices and implements them in a way that fits your organization, then you'll have a strong base.

Finally, an important building block is embedding operational risk management solidly into your bank's risk management culture. One way to do this is to ensure that for every significant business decision your bank has a holistic understanding of the operational risk implications of that strategic direction. In all likelihood, you already have programs in place to review and approve new products, services, and individual business activities. These programs are critically important in today's environment given the amount of change underway; they ensure that risks are well identified, understood, and appropriately managed. These review and approval processes, and the risk assessment approaches that they use, are working fairly well. We know this because we've been looking at them in our examinations. I would encourage you to apply this same approach and discipline to your process of assessing strategic and business model change. If you're thinking about significant changes and new directions, you need to look across initiatives and understand how they interact, how the change in the risk profile of one activity cascades through and across other activities. In simple terms, you need a means to identify and assess the impact of change across the enterprise, a firm-wide approach for looking not just at the immediate risks and impacts, but also at the potential or probable risks and their impact down the road.

In the end, sound operational risk management isn't something a bank does. It's more than that. It's something so embedded in a bank's culture and its DNA that the thought of "cutting corners" to be first to market isn't even a consideration. It's the ingrained guiding principles that recognize that defense against cyber threats and ensuring information security are more than the technology, more than firewalls, more than perimeter protection. It's an inherent and automatic understanding that the best defense against the risks associated with managing change is central to identifying and mitigating the operational, strategic, and reputational risks facing institutions today. It's individuals who understand and own the risks, and it's the necessary controls and incentive schemes that do not encourage employees to compromise the control environment. Moreover, it's the tone from the top that promotes and ensures that this can all happen at your organizations.

Thank you. I think we have some extra time, and I'd be happy to use it to respond to some of your questions.