FEDERAL RESERVE BANK *of* NEW YORK *Serving the Second District and the Nation*

SPEECH

Keynote Address at the Institute for International Bankers Annual Seminar on Risk Management and Regulatory Examination/Compliance Issues

October 24, 2016
Posted November 01, 2016

F. Christopher Calabia

Keynote Address at the Institute for International Bankers Annual Seminar on Risk Management and Regulatory Examination/Compliance Issues

As prepared for delivery

Overview and Introduction

I'd like to thank our colleagues at the Institute for International Bankers for inviting me to participate in your seminar today. As representatives of internationally active banks, you are helping to bridge the gaps between regions and continents by promoting trade and investment between our countries. You play an integral role in enabling individuals and enterprises to conduct business far afield from their native lands; in some cases, you may also expand the choices that local customers in our market have for seeking credit and other banking services. You do so by conducting your business far afield from your firm's own home markets, through local offices here in the United States.

Banks doing business across borders accept a dual responsibility for compliance: they agree to do business within the laws and regulations in the home and host countries.

In thinking about how international bankers must adapt to the rules and expectations of a host country, I'm reminded of the words of one famous international banker, T.S. Eliot.

Now T.S. Eliot is actually not famous for being a banker. He was an American-born British subject who did indeed work in the international division of a bank in London from 1917-1925. We know him today because T.S. Eliot also wrote essays, plays, and poetry. Today he is recognized as one of the greatest English language poets.

In response to one interviewer's question about how he made the transition from writing poetry to writing plays, Eliot explained that he first worked hard to understand the technique of writing for the theater so that he could later forget those techniques. As he put it, Eliot felt "it's not wise to violate rules until you know how to observe them."[1]

I doubt you will ever hear a bank regulator encourage you to violate any rules. I'd like to stress that I'm not suggesting you should ever do so! Still, Eliot's remarks resonate with me when I think about the challenges some firms face when developing risk management or compliance programs.

If I might transform his words a bit, we are at the greatest risk of violating rules when we don't know how to observe them. And in my experience as a banking supervisor, I've found that one of the simple reasons that banks – both foreign and domestic – may fall afoul of rules and regulations can be that their managers did not understand or did not take the time to understand the purpose of those rules.

So I'd like to discuss some of the rules and expectations that we supervisors have for three sets of emerging issues that are of particular importance to foreign banking organizations operating in the United States.

First, cybersecurity has become one of the top concerns for all organizations in the public and private sectors that rely on information technology. I'd like to share some of the most common challenges we have seen in branches and agencies and our relevant expectations as supervisors.

Next, as part of the post-crisis regulatory reform in the United States, many branches and agencies are now expected to adopt even stronger controls and risk management processes as part of our enhanced prudential standards. Important standards have come into force this year, so I'll address the requirements to establish and report to a U.S. Risk Committee as my second topic and some of the requirements related to financial resilience as my third.

Most of my comments will focus on the U.S. operations of foreign banking organizations that maintain less than $50 billion in banking assets in the United States.

On all of these topics, I'd like to share my sense of the purpose of the underlying rules and regulations so that you may be better able to understand and observe those rules. Any opinions I share are my own and may not reflect those of the Federal Reserve

Bank of New York or the Federal Reserve System.[2]

Cybersecurity

Let's start with cybersecurity.

Our world in many ways is smaller, faster, and more accessible than ever before. Ever more sophisticated devices and networks have helped us to overcome the historical divisions between countries and continents created by distance.

Banking has certainly benefited from these advances: the same technology that allows a food blogger to share instantly a picture of a meal she is enjoying half way around the world enables that same person to deposit a paper check without visiting a branch or to pay a bill without speaking to a banker.

Yet our dependence on these technologies and infrastructure has exposed weaknesses that malevolent actors have learned to exploit. The motivations for attacks on banks in particular may vary from seeking to steal information or funds to simply creating embarrassment or havoc for the firm or for its customers and counterparties.

Branches and agencies operating abroad face special challenges in managing their cybersecurity in part precisely because they operate remotely from the head office. To simplify my discussion today, I'm going to use the word branch to relate to a firm's U.S. operations, but please note that my observations are relevant to agencies and often local U.S. subsidiaries of foreign banks as well. I'll mention two challenges that are unique to the structure of a local branch's operations, and I'll conclude this section with a glance at the future.

- *Insufficient head office oversight*
  First, many branches employ a decentralized model for information technology: a branch may rely on head office for core banking systems but still host its own information systems specific to U.S. requirements. For example, a branch may maintain locally a U.S. regulatory reporting systems or perhaps a filtering system used to help comply with U.S. sanctions against specific countries under the Office of Foreign Assets Control.

  Some head offices face challenges in overseeing these local systems. Often the local systems may not be familiar to head office auditors. We've found that, when head office auditors do visit their branches in our District, they may review solely general IT controls in place in the branch. They may not evaluate U.S. specific systems that the branch maintains or perform vulnerability tests of those systems. We would urge head office to develop capacity to conduct such audits of systems maintained at U.S. branches or, when necessary, to rely on appropriate external auditors who can help evaluate such systems on a head office's behalf.

- *Unclear division of responsibilities*
  Second, we've seen confusion over who is responsible for what in a branch when it comes to information technology. This may stem from the lack of clearly stated responsibilities for head office management versus branch management. When head office does provide information technology platforms and information security services, we've sometimes seen that a branch does not have an operational level agreement defining what local management is expected to oversee and what security incidents need to be reported back to head office.

  Conversely, when branch management outsources technology services to third party vendors, too often management has failed to clearly document the monitoring activities that they undertake to ensure that vendors adhere to contractual requirements and that vendors maintain acceptable security and performance levels. We supervisors expect firms to develop such documentation to ensure that all arrangements are well managed and well controlled.

- *Emerging standards for cybersecurity – the Advanced Notice of Proposed Rulemaking*
  The two challenges I've cited reflect the difficulty some branches face in operating remotely from a head office's information technology systems. Let me close my remarks on cybersecurity with some thoughts on what future rules might look like.

  As supervisors, our goal for U.S. branches is to transform their responses to cybersecurity challenges from ad hoc responses to more clearly defined and articulated processes and standards. While supervisors have already offered some tools to help in this regard – such as the interagency cybersecurity assessment tool[3] -- U.S. supervisors are proposing a more enforceable set of standards that go beyond the guidelines we have offered to date.

  In that vein, on October 19, the Federal Reserve, the Office of the Comptroller of the Currency, and the Federal Deposit Insurance Corporation issued a joint advanced notice of proposed rulemaking.[4] This notice solicits comments from the industry on ways the agencies might establish enhanced cyber risk standards for the largest and most interconnected firms subject to

their supervision. The agencies are contemplating such standards as a way to increase the operational resiliency of large firms and to reduce the potential damage to the financial system in the event of a cyber incident.

As discussed in the advanced notice, these new standards if approved would apply to larger firms, such as U.S. bank holding companies, savings and loan holding companies, and potentially state and nationally chartered banks and other institutions with more than $50 billion in total consolidated assets. The standards would apply as well to foreign banking organizations with $50 billion or more in total U.S. assets.

The proposed enhanced standards would set additional supervisory expectations within the current supervisory framework and are grouped into five categories:

- Category 1 describes standards for firms to create their internal cyber risk governance structures;
- Category 2 defines standards for cyber risk management;
- Category 3 discusses standards for managing internal dependency, which addresses how a firm uses its own business assets (such as its workforce, data, technology, and facilities) to deliver services;
- Category 4 addresses how a firm manages its external dependency, meaning its relationships with vendors, suppliers, customers, utilities, and so on; and
- Category 5 addresses incident response, cyber resilience, and situational awareness.

Together, these five categories would constitute the "first tier" of more enforceable expectations applicable to larger firms.

The advanced notice furthermore suggests that supervisors may propose a second tier of cyber requirements for those firms that have "sector-critical systems" – such as establishing a 2-hour "recovery time objective" to resume business after a cyber event.

The agencies have requested feedback on these initial proposals by January 17, 2017. I would encourage you to review these standards and offer comments for the agencies' consideration.

Enhanced Prudential Standards: U.S. Risk Committee

I'd like to turn now to my second and third area of focus and share observations on the enhanced prudential standards that now apply to the U.S. branches and agencies of foreign banking organizations.

As you know, the Dodd-Frank Wall Street Reform and Consumer Protection Act introduced a host of new standards for capital, liquidity, and governance especially for large U.S. firms, but also for foreign banks active in the United States. Congress enacted this law in response to some of the lessons learned from the recent financial crisis. Our overarching goal is to strengthen resilience and to reduce the risk that a significant disruption or outright failure of a large U.S. or foreign bank might threaten the stability of the financial system or hinder the growth of the broader economy.

For branches of foreign banking organizations, one of the most interesting lessons learned through the crisis is how much their risk profiles, activities, and strategies have evolved recently.

When T.S. Eliot wore pinstripes in London, a bank's overseas offices might have served largely to facilitate trade and commerce between countries. Internationally active banks supported customers engaged in global commerce by offering letters of credit and other forms of trade finance; by offering international payments or correspondent banking services; or perhaps by facilitating a customer's access to credit in overseas markets or to foreign exchange.

In contrast, even just over the last 20 years in the United States, we have witnessed a dramatic progression in the role that some foreign banks play in our markets.

- The change is most pronounced in foreign banks' increasingly deep participation in U.S. capital markets activities. As an example, some of the largest broker/dealers in the United States are now operated by foreign banking organizations.
- In addition, we saw through the crisis that some branches' profiles have changed from depending on their parent banks for funding to becoming themselves a major source of U.S. dollar funding to service the firm's needs worldwide.
- In some cases, this effort to raise U.S. dollar funding for head offices and affiliates worldwide made the U.S. branches of those firms significantly more dependent on wholesale overnight funding sources that proved to be far more volatile in the crisis than anticipated. These trends furthermore made branches in the United States more interconnected with other financial service organizations, but also more concentrated in risks, and more exposed to a sudden loss of liquidity.

The enhanced prudential standards applicable to foreign banks are intended to strengthen their resilience and reduce the need to access emergency funding sources, such as the Discount Window or other facilities in the future. Many of those regulations became effective this past July.

Regulations arising from the Dodd Frank Act that are relevant to foreign banks include the requirement for banks with the largest U.S. operations – those with over $50 billion in U.S. assets held outside of a branch structure – to establish intermediate holding companies that will be subject to capital and liquidity requirements similar to those expectations set for domestic holding companies of that size.

Today, I'd like to focus mainly on the requirements imposed on a broader set of foreign banking organizations, including those with smaller U.S. operations that were not required to establish a holding company, which would apply to most of the firms represented at this conference. The requirements relate to governance on the one hand and to financial resilience on the other.

U.S. Risk Committee

The first requirement I'd like to discuss is for qualifying foreign banking organizations to establish a U.S. Risk Committee. For firms not subject to the intermediate bank holding company requirement, this committee must be established at the board of directors back home.

This requirement applies to foreign banking organizations with more than $10 billion in global assets if publicly traded, as well as to other foreign banking organizations with total global consolidated assets of $50 billion or more.

In my view, the intention for this rule is to ensure that a head office plays an active role in overseeing the firm's activities in the United States and that it has board members and other senior executives with sufficient focus on and understanding of U.S. markets.

For organizations with less than $50 billion in U.S. assets, the U.S. Risk Committee must conduct two tasks under the new regulation.

- First, it must oversee the risk management policies of the combined U.S. operations.
- Second, it must include at least one member who has experience in identifying, assessing, and managing the risk exposures of large, complex firms. (The rules are more prescriptive for firms with more than $50 billion in U.S. assets and also specify that such larger firms must have a U.S. chief risk officer, for example.)

As supervisors, we expect that the home country banks are taking appropriate measures to ensure that U.S. operations implement the policies created by the U.S. Risk Committee. In addition, we expect that the U.S. operations provide sufficient information to the U.S. Risk Committee so that it can carry out its responsibilities.

With regard to this latter point, one open question remains exactly what it means to provide sufficient information to the U.S. Risk Committee. The final rule doesn't specify the type, frequency, or quality of information that would satisfy the "sufficiency" requirement outlined above. The Board of Governors has not defined this expectation further.

However, our experience supervising other kinds of firms, such as domestic bank holding companies, might lend some insight into what a U.S. Risk Committee might find useful to receive from a bank's U.S. operations. Again, these represent my views only.

- First, as we would always expect, management of the U.S. operations should ensure that it is providing data that is accurate, timely, and accessible for U.S. Risk Committee members.
- Second, the report that the U.S. operations provides should be presented in a format that is easily read and understood by a senior manager or director with little first-hand knowledge of the actual businesses.
- Finally, the system should be audited independently by internal and external staff with sufficient expertise to understand the issues.

These requirements are all intended to ensure that large, internationally active firms that conduct banking activities in the United States have a good understanding of those activities. We want senior leaders at head office to review material events and supervisory issues that occur within their U.S. operations so that they can best support their businesses here. That, in turn, should reduce the likelihood of significant disruptions or losses that could affect the U.S. financial system. As always, we expect that head office will be a source of strength to its U.S. offices. The U.S. Risk Committee requirement helps to make that expectation tangible.

Enhanced Prudential Standards: Financial Resilience

Another way that head office serves as a source of strength to its overseas offices is by possessing adequate financial resources to withstand unexpected losses in its global operations. So I'll turn now briefly to the requirements related to financial resilience for

organizations that maintain less than $50 billion in U.S. assets.

Let's begin with capital. Under the enhanced prudential standards, firms with U.S. assets below $50 billion must be subject to capital standards at home that are equivalent to those set by the Basel Committee on Banking Supervision.

Such firms are also required to be subject to one of the most important tools to emerge from the financial crisis, namely stress testing, in which firms imagine how economic conditions might change in the future and evaluate whether they have sufficient capital and liquidity to withstand future potential losses.

The largest and most systemically important U.S. and recently foreign banking organizations are now subject to the most comprehensive U.S. stress testing requirement, the Comprehensive Capital Analysis and Review ("CCAR"). So today I'd like to address instead requirements that apply to smaller foreign banking organizations.

Under the enhanced prudential standards, foreign banking organizations with greater than $10 billion in global assets that maintain U.S. operations are required to be subject to a stress test by their home country supervisor and provide it to their supervisor for review.

We don't intend to subject foreign banks with less than $50 billion in U.S. assets to a CCAR-like process. Instead, we want the firm to submit only the stress test results, and not the actual stress test. The Federal Reserve would review only whether the firm passed a supervisory stress test and would not comment on the process or methodology. We are still developing a process for how firms will submit their stress test results to us.

If the bank is not subject to a home country stress test, its U.S. branch/agency network would be subject to asset maintenance requirements, and any U.S. subsidiary banks would be subject to a U.S. stress test.

With regard to liquidity stress testing, foreign banking organizations with more than $50 billion in global assets will be required to submit the annual results of a global liquidity stress test or of a combined U.S. operations stress test. The test should consider the Basel Committee's standards that cover scenarios for 30 and 60 days, plus a one year scenario. We are still developing the procedures through which firms will submit this information.

Our goal for capital and liquidity stress testing is to have a better understanding of how well the global parent organization can withstand future potential economic downturns or shocks such that it can continue to serve as a source of strength to its U.S. operations.

Closing Remarks

I set out to offer some remarks today on emerging issues that the U.S. operations of foreign banking organizations face and how U.S. supervisors expect firms to be best prepared to address them.

We've discussed the most current thinking ranging from how a branch should protect its systems from cyber attacks to how we'll ensure that the parent organization back home is best able to understand the risks and issues facing its U.S. operations and how well prepared it is to continue to serve as a source of strength to its businesses here throughout the business cycle.

With that, I've come to the end of my prepared remarks.

Yet, as T.S. Eliot wrote, "the end is where we start from."

Banks and supervisors alike have a lot of work ahead of us as we strengthen the resilience of firms and of the broader financial system. To do so well, we need to remain in close dialogue. We supervisors need to understand the challenges that you face. In turn, we'd like to be sure that you understand the purpose of our rules and expectations and so that your firms can best observe those rules.

In that vein, I'd like to express my thanks to our colleagues at the Institute for International Bankers for hosting this dialogue today.

---

[1] T. S. Eliot, The Art of Poetry No. 1

[2] I would like to thank especially Eric Caban, David Fenton, Amy Man, and Peter Truong, all of the Federal Reserve Bank of New York, who provided input and advice for these remarks. Any remaining errors are mine.

[3] Cybersecurity Assessment Tool.

[4] Agencies Issue Advanced Notice of Proposed Rulemaking on Enhanced Cyber Risk Management Standards