5 evolving risks the audit committee should monitor in 2015

Prepared by:

Tyrone Beasley, Principal, RSM US LLP
tyrone.beasley@rsmus.com, +1 972 764 7016

Dan Shumovich, Principal, RSM US LLP
dan.shumovich@rsmus.com, +1 213 330 4668

Doug Underwood, Principal, RSM US LLP
doug.underwood@rsmus.com, +1 612 376 9210

Loras Even, Principal, RSM US LLP
loras.even@rsmus.com, +1 319 274 8541

Joe Benfatti, Partner, RSM US LLP
joe.benfatti@rsmus.com, +1 415 848 5344

February 2015

While no two financial institutions are exactly alike, all are affected to some degree by marketplace, legal and regulatory activities. During the production of this year’s Audit Committee Guide for Financial Institutions, we spoke with several RSM experts regarding what they perceive as “evolving risks” for the financial sector. Following are capsule summaries of those risks and quick action steps your financial institution can consider to address them.
Cybersecurity

For years, experts have warned about rising business vulnerabilities to cyberattacks, and 2014 was the year the issue exploded into public view after a number of prominent companies reported significant data breaches. Many of those incidents were credit card–related hacks that have driven many retailers and financial institutions to improve card security technologies. Due to this evolving risk, it’s more important than ever for companies to evaluate two key threats: cyberattacks facilitated in part by “social engineering” and attacks that can occur when online tools are built outside of the information technology (IT) department.

“Employees are the front–line defense against cyberattacks, and what we continually hear from CIOs (chief information officers) and CISOs (chief information security officers) is that many new hires and employees do not grasp how cyberattackers use social engineering to get valuable information,” said Doug Underwood, a principal in RSM’s risk advisory services group. “While managing these risks is important in any business, it is especially critical in financial services environments.”

Social engineering risk can take on many forms, and many recent, successful cybersecurity attacks have been facilitated in part through social engineering. The most well–known is phone or email communications from hackers to employees, posing seemingly innocent questions in order to secure system passwords or personal data. However, social engineering risk can also come from poorly considered development of online platforms. For example, in some financial institutions, websites and other external portals are designed, built and deployed by the marketing or communications area of the business, without involvement by internal security and IT staff. In many cases, this lack of cybersecurity awareness can create vulnerabilities in otherwise well–designed security systems.

Underwood and Loras Even, a principal in RSM’s risk advisory services group, said financial institutions can take a couple of simple steps to help reduce exposure to these threats. First, tighten hiring criteria for all hires in IT, compliance and data security roles, ensuring that successful candidates possess both technical ability and demonstrated “best practices” competence with social media. For the latter, this may mean reviewing a candidate’s Facebook, LinkedIn, Twitter or other social media accounts for obvious red flags, such as posted travel plans and dates, address or birthdate details or other information attackers could use to access personal accounts.

A second step is to ensure that all online activity—regardless of where it originated—is part of a regular technology risk assessment process. This means involving appropriate IT or data security partners during the design phase of any online project, which can help ensure the deployment of sound cybersecurity defenses that won’t compromise site functionality. This is especially critical for new cloud–based solutions or portals, since those reside outside an institution’s regular security systems.

A third and critical component is a sound vendor management program, the importance of which was underscored in some of the cybersecurity breaches that have occurred in the past couple of years. The security of any organization is directly affected by the online practices of its third–party partners. For instance, a bank that uses good password policies and user account reviews could still be at risk from a vendor that employs weak password policies and no account access reviews. In fact, cyberattackers often use social engineering to identify a financial institution’s vendors. That knowledge can then be used to position the attacker as a “trusted vendor,” making it easier to slip past a bank’s online defenses.

Bank Secrecy Act and anti–money laundering

The Currency and Foreign Transactions Reporting Act of 1970 (otherwise known as the Bank Secrecy Act or BSA) requires U.S. financial institutions to help government agencies uncover or prevent money laundering. The BSA, which is often referred to as the “anti–money laundering” law (AML), has been amended several times to help financial institutions and government agencies respond to changing trends in global money laundering activity. This includes financing for illicit drug traffic and terrorism.

Tyrone Beasley, who serves as a regional risk advisory services leader for RSM, says an evolving money laundering threat to financial institutions is the speed at which “bad actors” adjust and revise transaction schemes to avoid detection by existing anti–money laundering safeguards.

“Money launderers are getting very good at finding new ways to wipe out trails of suspicious activity, so financial institutions cannot rely on a static environment for monitoring and detecting this activity,” he said.

Clearly, regular risk assessments to monitor the effectiveness of anti–money laundering technology, staffing and training are important. However, Beasley said an additional step executives should consider is mapping that risk assessment to publicly available reports on major money laundering events and the steps taken by regulators or other financial institutions to handle the issue. By performing this extra level of due diligence, leaders can see if there are common “threat points” in their policies, technologies or training and use the information to make practical adjustments in their AML defenses.

Another way for financial institutions to improve their AML approach: Tighten the internal connections between AML and fraud detection. Too often, Beasley said, these areas operate in silos, despite the fact that each group may often uncover valuable information that would be useful to the other’s prevention activities.
Compliance

It’s no secret that the banks and financial institutions have been deluged by a series of regulations in recent years, ranging from the Dodd–Frank Wall Street Reform and Consumer Protection Act to new bank and nonbank supervision compliance requirements mandated by the Consumer Financial Protection Bureau (CFPB).

However, Beasley emphasized that one evolving risk may not lie in the sheer number of regulations, but in some financial institution's unwillingness to keep pace with constant change.

“A lot of institutions are not beefing up their knowledge with respect to the frequency and velocity of these changes,” Beasley said. “As a result, there are still boards and audit committees under the impression that their compliance staffing and knowledge base from a half–dozen years ago is still adequate today. And it’s not.”

While some financial institutions may well be understaffed for the challenges of a modern compliance environment, Beasley said simply assigning more bodies will not lessen the risk, unless the right personnel and skills are added to the mix. Instead, he suggested that leaders carefully assess the technical and regulatory needs in their specific compliance environment and make hiring and training decisions that close the gaps uncovered in that review.

Another evolving compliance issue is what can be described as the “not applicable risk” from regulations and guidance issued by the CFPB and the prudential regulators. For example, the Federal Deposit Insurance Corporation (FDIC) issued guidance for automated overdraft programs. While the guidance is specific to FDIC-regulated institutions, there are practices related to limits on the number of overdraft fees and other operational controls that can reduce an institution’s exposure to consumer claims of unfair, deceptive or abusive practices.

From a risk management viewpoint, executives shouldn’t simply say “this doesn’t apply to us” when faced with new or pending regulations designed for larger or smaller financial institutions or when guidance from other regulators are issued. Beasley said a better course is to become familiar with all of the upcoming rules and regulatory guidance and select items that can help demonstrably strengthen an institution’s risk or compliance environment. This sends a message to both regulators and stakeholders that a specific financial institution is taking a thoughtful, proactive approach to compliance.

Model governance

Increasingly, financial institutions are relying upon various modeling tools to manage risk and make informed business decisions. Common modeling tools are designed to address areas such as interest rate risk, liquidity forecasting, portfolio stress tests, bankwide stress tests, loan loss reserves, valuation issues and anti-money laundering systems.

In response to this trend, regulatory agencies have continued to raise governance expectations with regard to the use and scope of these models. In fact, the model governance umbrella has expanded beyond complex software programs to include tools as simple as internally developed spreadsheets. Due to this broadly defined governance area, regulators are now casting a wider net and looking more closely at model risks that may have been overlooked in the past.

In a recent Supervisory Insights newsletter, the FDIC noted that while modeling was a useful advance for financial institutions, “the models themselves represent a new source of risk—the potential for model output to incorrectly inform management decisions.” While the article was focused primarily on interest rate risk, the same principals and expectations are being applied equally to other modeling processes beyond interest rate risk. That is why many financial institutions have proactively embraced the concept of model governance to address overall control responsibilities in a framework that can be applied equally without regard to the underlying modeling tool or objective.

Dan Shumovich, a RSM principal and national financial institutions consulting leader, agreed with the FDIC’s assessment of modeling as an evolving risk and the migration of these concepts to other business processes. “Regardless of what a specific model is intended to accomplish, there are certain processes, controls and validation steps that a financial institution needs to employ to make sure the modeling process is conceptually sound for the task at hand, that assumptions are justified, that controls over user access and data inputs are in place and that secondary independent audit or validation routines are in place to periodically measure the integrity of underlying management processes,” he said. “In addition to meeting regulatory expectations, improved modeling governance practices can increase the reliability of information and ultimately lead to better business decisions.”

To achieve this objective, organizations should deploy a series of “model governance” procedures in proportion to the size, complexity and materiality of their underlying objectives for modeling. For example, many financial institutions are now developing board–approved modeling governance policies and procedures. These rules seek to define the process for selecting third-party modeling tools, while setting management guidelines for internally developed models. These internal standards also seek to define the governance framework in areas such as user access controls, justifying key assumptions, ensuring data integrity, establishing routines for data backup, storage and security and enabling a risk–based approach to independent audit and validation activities.

Independent validation of the modeling process remains an especially vital guideline. For example, if financial models were developed by in–house staff, validation from a qualified third party provides a level of assurance to boards, audit committees and regulatory agencies about the integrity of the
Vendor management

For years, vendor management for many financial institutions was operated via an in-house list or external software tools that could be customized for specific workflows and processes. However, greater regulatory oversight in financial services has raised the bar on both the quality of vendor information and the level of formality in which it is presented. For example, recent guidance from the Office of the Comptroller of the Currency (Bulletin 2013–29) specifically outlined the need for more documented management of third parties that provide “critical activities,” such as consumer compliance, debt collection or loan origination and servicing providers.

Joe Benfatti, a partner in RSM’s technology risk advisory services group, said the tighter rules have created an evolving risk for some small and midsize financial institutions, where existing vendor management processes and tools may not be enough to help them meet modern compliance standards.

“Some firms have a relatively informal vendor management protocol, which may be managed by a single person or a small group with a “one-size-fits-all” approach, while most large financial institutions have a very strict set of processes,” he said. “But there are technology solutions now available, where even the smallest financial institution can gain access to broader, more robust tools to help them stay in compliance with leading vendor management guidelines while maximizing the return on their vendor relationships.”

Today, several leading cloud-based solutions deliver a one-stop shop on key vendor performance benchmarks, such as benefit–cost ratios, customer ratings, analytics related to regulatory compliance, information security and reliability. Those tools also help financial institutions track key “critical vendor” criteria, such as significance of transaction volume, relevance of core business processes and the average length of time to find and onboard a replacement vendor (should the relationship fail). The key advantage to this solution? Many solutions come pre-populated with data, and it provides data from thousands of businesses, providing a much broader sampling through which to evaluate current or prospective suppliers—the institution doesn’t have to spend nearly the time it used to gather, populate and update these data elements for each vendor. The value of such tools provides a unique opportunity to scale the nature and depth of an institutions vendor management requirements on a risk-ranked basis. Doing so better aligns with regulatory intent while reducing focus on administrative vendor management functions allowing for more time and efficient expenditure of effort and analysis where it is needed most.

These new vendor data management solutions are readily available at a relatively modest price-point, often on a subscription basis. But Benfatti said financial institutions would get the most value from such tools if they first retain expert help to analyze the vendor pool, identify critical suppliers, review service-level agreements and prioritize all of that data against the relative significance each vendor has with respect to its core operations and latest regulatory requirements. That way, business leaders know precisely where to invest time on vendor monitoring activities for maximum return on their compliance investment.