ADVISEN
Insurance Intelligence

Financial Institution Risk Management Issues

January 2014

SPONSORED BY: AIG

Financial Institution Risk Management Issues

Introduction

As a consequence of the global financial crisis, politicians, regulators, and many financial industry executives agree on the need for comprehensive risk management reform in the financial sector. While their preferred solutions may differ, most acknowledge that the lack of sound, industry-wide risk management policies and procedures was one of the primary enablers of the crisis.

In the not too distant past, "risk management" for many types of financial institutions principally meant managing the financial aspects of risk such as the portfolio risk of a bank for example. Many financial institutions now are viewing risk from more of a holistic, enterprise-wide perspective. The damage that can be inflicted by other categories of risk has gained mindshare among regulators and executives. Additionally, forward-thinking executives now recognize that integrating risk management into the strategic planning process can be a source of competitive advantage.

As a percentage of total revenue, the average total cost of risk is less for financial institutions than for companies in most other industry segments, according to the 2013 RIMS Benchmark Survey. This is because financial institutions typically have comparatively benign employee health and safety exposures, no product liability or recall exposures, and no large investments in plants, machinery, warehouses, inventory or fleets. Nonetheless, even without these common exposures, financial institutions pose an abundance of risk management challenges.

The current risk profile of financial institutions is shaped not only by the credit crisis and its regulatory fallout, but also by technology, globalization, demographic shifts, and changing customer expectations. Increasingly, financial institutions view risk as something to be managed across the entire organization, and many are open to innovative ways to finance risk issues. Near the top of many financial institution risk managers' lists of significant issues are the implementation of enterprise risk management programs; cybercrime; reputation damage; the changing exposures of directors and officers; anti-corruption and anti-money laundering laws; and alternative risk financing and transfer strategies.

Enterprise Risk Management and the Evolving Role of the Risk Manager

The financial crisis that led to waves of bank bailouts and failures forced the industry to reconsider its approach to risk. Most of the nation's largest financial institutions now have implemented an enterprise-wide risk management approach to ensure that sound risk management is being applied to operations and decisions at every level within the company. In fact, according to a survey of business executives from predominantly large companies conducted by a leading consulting firm, 79 percent of financial service firms have enterprise risk management programs as compared to 67 percent of the survey participants overall.[1] While not as widespread, enterprise risk management adoption also is gaining traction with smaller, less complicated institutions.

The impetus for enterprise risk management programs predates the credit crisis, but the financial crisis and continued economic instability have accelerated the drive towards this change

As opposed to traditional risk management practices, enterprise risk management requires a comprehensive institutional process that addresses all areas of risk including market risk, credit risk, operational risk, business risk, reputation risk, audit, and governance. The impetus for enterprise risk management programs predates the credit crisis, but the financial crisis and continued economic instability have accelerated the drive towards this change. New rules and regulations that have been implemented in an effort to prevent another financial meltdown have encouraged a more holistic view of risk. But these rules also have resulted in increased regulatory expectations and scrutiny of risk management practices by investors and other stakeholders such as rating agencies and analysts. These new rules - while critical in avoiding a repeat of the 2008 financial crisis – can offer new litigation pathways for plaintiff attorneys. Added regulation oversight and scrutiny create additional areas of potential non-compliance for management to consider.

An example of legislation with both direct and indirect risk management implications is the Dodd-Frank Wall Street and Consumer Protection Act of 2010. While not mandating enterprise risk management in its broadest sense, proposed regulation implementing Dodd-Frank does require that larger institutions have a risk committee of the board of directors that is responsible for oversight of enterprise-wide risk management.[2] The regulation, however, only applies to a small group of large financial institutions that likely already have some sort of enterprise risk management in place or in the works. It likely will not have a strong impact on the adoption of enterprise risk management more broadly in the financial sector at least in the near term. If history is a reliable guide, however, a regulation designed for a few can become the standard for many over time.

On the other hand, Basel III applies to almost all U.S. banks, regardless of size. While the primary focus of Basel III is capital and liquidity standards, risk management has a central role. Although focused principally on financial and operational risk, Basel III encourages the creation of an enterprise-wide risk management framework that can accommodate all categories of an organization's risk.

In the past, risk management often was viewed as a process bolted onto a financial institution's core operations to help keep bad things from happening. As enterprise risk management becomes more ingrained throughout more firms, risk management is increasingly viewed as a core operation itself: banks "have an opportunity to turn good risk management into a competitive advantage," in the words of consulting firm McKinsey & Company.[3] An Accenture survey of business executives from a cross section of industries, including financial services, found "risk management capabilities are high on the executive agenda and now seen as a critical business driver and source of sustained growth and long-term competitive advantage."[4]

In order to comply with current and future regulations, and to meet the expectations of stakeholders, the role of financial institution risk manager is evolving. Increasingly risk managers are responsible for – or at least involved with – a broader range of risks, and perform in roles that often have much greater strategic significance. As a risk manager accumulates knowledge of the institution's risk and exposure, he/she is in a position to assist senior management in identifying where best to focus their core growth strategies. Deeper skills in a wider array of risk issues are becoming essential for risk managers to succeed and add value in this new environment.

Malware/Cyber-Crime

Today's criminals are increasingly sophisticated and use leading edge techniques to stay a step ahead of business defenses

Financial institutions have long been a target of criminals. The difference today is that guns and masks have been replaced with malware and the anonymity of the internet and personal computers where attacks can be carried out from miles or oceans away from their intended targets.

This was the case in a series of politically motivated attacks that repeatedly targeted some of the nation's largest financial institutions. A hacktivist group located in the Middle East, Izz ad-Din al-Qassam Cyber Fighters, claimed responsibility for the distributed denial-of-service attacks that disrupted the websites of dozens of U.S. banks. U.S. intelligence officials, however, have continually claimed that due to the sophistication of the attacks, the hacker groups are likely being backed by a nation-state and all signs point to the Iranian government. Although the attacks to date have been seen mostly as a nuisance, there is concern that they are being used as a cover for bank and data theft. There is also concern that in the future enough firepower could be gathered to crash any website. As a result, a coordinated response among industries, companies and the government has been initiated.[5]

Today's criminals are increasingly sophisticated and use leading edge techniques to stay a step ahead of business defenses. Potential attackers include thieves seeking to steal customer data, trade secrets, and money; social agitators (aka hacktivists) interested in causing a disruption to make social or political point; and cyber terrorists, often sponsored by nation states, who are intent on bringing down an institution and/or causing havoc within the financial sector.

Because all have different agendas, different mechanisms are used to achieve a particular goal. For example, thieves may deploy malware in attempt to takeover customer accounts, breach third party payment processors, and exploit securities and market trading services; hacktivists may use denial of service attacks, publish private information, and deface websites; and cyberterrorists may deploy malware to attack a country by bringing down critical infrastructure including its financial system. Recently, denial of service attacks resulting from international events caused some major financial institutions to address the issue independently. This type of event is not only a nuisance, but can potentially disrupt business and negatively impact reputation. While many larger institutions spend in the hundreds of millions of dollars on data security, there is often a need for additional funds in order to bolster and continue security measures. These threats are growing, and as a result according to some estimates, require financial institutions to spend approximately 8 percent more year-over-year on data and privacy security.[6]

Financial institutions often find themselves in a precarious situation. Banks increasingly face pressure to comply with regulatory mandates, strengthen balance sheets and meet customer demands.[7] Accomplishing these objectives can put a strain on the resources needed to address and stay ahead of threats targeting their networks, applications, and data. For example, online banking now is a competitive necessity, but providing these services presents abundant security challenges, especially via often less secure mobile devices.

Failure to provide adequate security can have dire consequences for a financial institution. Not only can a breach be costly, it can result in significant penalties for non-compliance with data security and privacy regulations and most importantly cause significant damage to its reputation. Risk managers therefore need to maintain a comprehensive understanding of the threats along with their institutions exposures and vulnerabilities.

While it takes years to develop a good reputation, it can vanish literally in a matter of hours in an environment where information travels across the globe at lightning speed

In the not-too-distant past, data security was seen as principally an IT department issue. Most financial institutions now recognize that firewalls, encryption, and other software security solutions are vitally important, but that privacy and data security require enterprise-wide involvement. Many also are recognizing the benefits of insurance protection. Risk Managers should acknowledge that sometimes the sophistication of their internal IT groups may not be sufficient enough to protect their institution from all the threats that exist today. It is a best practice to seek external consultation regarding loss control efforts, risk mitigation, and other methods that can help avoid a breach in security or aid in the response to a crisis situation in order to mitigate reputational damage. As a result, the role of the risk manager in this realm continues to grow.

Reputational Risk

As a whole, the financial industry has had a black eye since the financial crisis. But at the institutional level, in an industry as competitive as financial services, a tarnished reputation can be catastrophic.

As defined by the Board of Governors of the Federal Reserve System:

> *Reputational risk is the potential that negative publicity regarding and institution's business practice, whether true or not, will cause a decline in the customer base, costly litigation, or revenue reductions.*[8]

For this reason, protecting the institution's reputation is one of the most significant challenges faced by financial institution risk managers, executive management, and board of directors. While it takes years to develop a good reputation, it can vanish literally in a matter of hours in an environment where information travels across the globe at lightning speed.

A variety of circumstances can lead to a tarnished reputation for a financial institution. For starters, negative publicity of any type in local or national media could adversely impact its image. A number of banks and other financial firms suffered reputation damage as result of their subprime lending and subsequent foreclosure practices, London Interbank Offer Rate (Libor) rate rigging scandal, and from their involvement with the Bernie Madoff Ponzi scheme to name a few. Additionally, misinterpretation of public data such as an institutions Home Mortgage Disclosure Act (HMDA) data and Community Reinvestment Act (CRA) ratings could impact a current or future customer's opinion of the institution. Data security breaches and leaks of confidential information (i.e. insider trading information) also are issues that could have reputational consequences.[9] One study found that announcements of 'pure' operational losses can result in substantial reputational losses, and that fraud is the event type that generates the most damage.[10]

Safeguarding an organization's reputation is impossible to accomplish with 100 percent effectiveness. A company can, however, minimize the potential damage with proper planning, policies, and procedures. A crisis management plan is essential to quickly respond to an event that threatens to undermine a company's reputation. Insurance coverage also may be available to cover the cost of crisis response and assist in connecting the insured with a network of crisis management professionals.

Changing Exposures of Directors and Officers

Executives and board members face heightened scrutiny by regulators, investors, and other stakeholders, putting them under the microscope as they navigate a shifting risk landscape

More than five years after the collapse of the subprime mortgage market, which triggered the credit crisis that plunged the world economy into recession, financial institution directors and officers continue to be named in newly-filed subprime and credit crisis-related lawsuits. Even as some directors and officers remain at risk for decisions and actions of years past, those same events also have resulted in an array of new exposures as lawmakers and regulators erect new regulatory frameworks, and plaintiffs' attorneys test new legal theories.

Executives and board members face heightened scrutiny by regulators, investors, and other stakeholders, putting them under the microscope as they navigate a shifting risk landscape. At the same time, and for the same reasons, underwriters of directors and officers liability have tightened underwriting standards and increased the amount of required underwriting information for some classes of financial institutions. Some troubled institutions have found it more difficult to assemble adequate limits of insurance.

Risks faced by financial institution directors and officers in the current environment include:

- **Actions by regulators.** Recently-enacted regulations create potential compliance and liability headaches for directors and officers. The Dodd-Frank Act, for example, includes provisions that address executive compensation and corporate governance, both of which have regulatory enforcement implications. Other sections of Dodd-Frank require the registration and regulation of swap dealers and major swap participants, and of security-based swap dealers and security-based major swap participants, making these activities more likely to be subject to enforcement actions. Additionally, the FDIC has authorized suits in connection with 120 failed banking institutions against 962 individuals for Directors & Officers liability as a result of the credit crisis.
- **Shareholder suits.** Publically traded financial institutions have long been a favorite target of shareholders and plaintiff's attorneys, with the number of suits skyrocketing in the wake of the credit crisis. While the frequency of securities class action fell in 2012,[11] regulations passed in the wake of the credit crisis may provide plaintiffs' lawyers abundant new opportunities to ply their craft. The "say on pay" provision of Dodd-Frank, for example, has led to a slew of suits against financial institutions and other companies. Privately-held financial firms also are at risk for investor suits. In one representative example, two credit crisis-related suits filed by shareholders of failed California bank against its directors allege the bank was brought down by unnecessarily risky lending activity.[12] Additionally, Shareholder Derivative actions are a major concern for financial institutions based on certain officers and directors decisions that may have affected certain bank failures. Historically, Derivative litigation settlements were small in comparison to securities class action suits. However, that is not the case today based on some of the recent larger derivative settlements that are out there and moreover, the costs to defend these cases today has increased dramatically.
- **Suits by borrowers and other customers.** Suits against banks by borrowers also have increased since the credit crisis and recession. Many of these suits – some of which continue to be filed – relate to subprime mortgage lending practices or foreclosures. A new round of suits allege that borrowers overpaid for loans because of manipulation of Libor.

Many of the most significant new exposures to directors and officers of financial institutions are a consequence of an increasingly complex regulatory environment. In a setting where exposures are continuously evolving as new legislation and regulation bring increased scrutiny of management practices and oversight, non-compliance or inadequate compliance can have serious liability implications. For this reason it has never been more important for risk managers to understand the regulatory-driven exposures faced by directors and officers and financial institutions, and to stay current with the rapidly-developing regulatory risk landscape.[13]

Foreign Corrupt Practices Act, UK Bribery Act, and Anti-Money Laundering Laws

Increased scrutiny by regulators and law enforcement agencies call for financial institutions to be more transparent by identifying customers and sources of funds, monitoring account activity, conducting inquiries into transactions, and reporting suspicious transactions to government entities among other requirements

Companies in all industry groups, including financial institutions, have been subject to a rapidly growing number of investigations by the Department of Justice and the Securities and Exchange Commission for violations of the Foreign Corrupt Practices Act. The Foreign Corrupt Practices Act (FCPA) makes it illegal for a company, its employees, its directors or officers, or agents to make a bribe or unlawful payment, or give anything of value to any foreign government official in order to obtain business with that government.

In recent years more cases resulting in large settlements have been brought than at any time in the history of the FCPA. Since 2005, the Department of Justice has instituted more prosecutions than in the previous 28 years of the statute's existence.[14] While financial institutions have thus far largely escaped the attention of the Securities and Exchange Commission and the Department of Justice, that situation may be changing.

Financial institutions also have been subject to increased scrutiny for violations of anti-money laundering laws. Under various anti-money laundering regulations, financial institutions are required to identify customers and the sources of funds. One high-profile example is a recent case that resulted in a $340 million payment to New York's banking regulator by Standard Chartered, a British-based bank, to settle money laundering allegations that it hid transactions with Iran. Institutions conducting business globally also need to remain compliant with anti-bribery laws elsewhere such as the UK Bribery Act.

Increased scrutiny by regulators and law enforcement agencies call for financial institutions to be more transparent by identifying customers and sources of funds, monitoring account activity, conducting inquiries into transactions, and reporting suspicious transactions to government entities among other requirements. Effective loss control practices are essential to avoid FCPA and money laundering losses since insurance coverage may be largely limited to coverage for investigation costs.

Alternative Risk Financing and Transfer Strategies

Financial institutions are experts at hedging strategies and capital market solutions, and a growing number are looking into these strategies as alternatives or supplements to traditional insurance. Insurance linked securities have proven successful for various categories of non-financial institution risks, such as accumulations of property exposures on insurance company balance sheets. More companies are using hedging tools such as weather derivatives as a compliment to traditional insurance coverage. Savvy risk managers will continue to explore the use of these types of approaches for financial institution-related risks as part of their overall risk management strategies.

Conclusion

For almost all companies, risk management is a higher priority today than it was a few years ago. Not many industries have seen the impact of that observation more profoundly than the financial services industry. Challenges frequently necessitate change and, in the case of the financial services industry, the global financial crises presented challenges not seen since the Great Depression. The concept of "risk" has taken on new meaning and garnered more attention from executives and regulators alike. As became evident as a result of the crisis, failure to address risk from a more holistic, enterprise-wide perspective can have adverse consequences for the institution, the industry, and the economy as a whole. Savvy executives, however, recognize that a focus on risk management is not only a way to avoid bad things from happening, but also can be a source of competitive advantage. As a result, the role of the financial institution risk manager has never been important or more challenging than it is today.

NOTES:

[1] Accenture, "Report on the Accenture 2011 Global Risk Management Study: Risk management as a source of competitive advantage and high performance", (2011), http://www.accenture.com/SiteCollectionDocuments/Microsites/risk-research-report/Accenture_Global_Report.pdf

[2] "The Dodd-Frank Act: Size matters," Westlaw Journal Derivatives, (2012) http://newsandinsight.thomsonreuters.com/Securities/Insight/2012/04_-_April/The_Dodd-Frank_Act__Size_matters/

[3] Turning risk management into a true competitive advantage, McKinsey Working Paper on Risk, (2008) http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CD4QFjAA&url=http%3A%2F%2Fwww.mckinsey.com%2F~%2Fmedia%2Fmckinsey%2Fdotcom%2Fclient_service%2FRisk%2FWorking%2520papers%2F5_Turning_risk_management_into_a_true_competitive_advantage_lessons_from_the_recent.ashx&ei=wiSmUOLxJKqq2QXK04GgDw&usg=AFQjCNF6_I-8U4Sv6-9fqmdh0vER2eOtGQ

[4] Accenture, "Report on the Accenture 2011 Global Risk Management Study: Risk management as a source of competitive advantage and high performance", (2011), http://www.accenture.com/SiteCollectionDocuments/Microsites/risk-research-report/Accenture_Global_Report.pdf

[5] Joseph Menn, Insurance Journal, "Cyber Attacks on Banks More Serious Than Public Realizes,' (2013), http://www.insurancejournal.com/news/national/2013/05/20/292573.htm

[6] AntoneConsalves, PC World, "Cyberattacks victimizing the largest banks, feds say," (2012) http://www.pcworld.com/article/2013502/cyberattacks-victimizing-largest-banks-feds-say.html

[7] Peggy BresnickKendler, Dell SecureWorks, "Staying Ahead of Cyberthreats: Recommendations for Financial Institutions", (2011), http://docs.bankinfosecurity.com/files/whitepapers/pdf/562_Staying_Ahead_of_Cyberthreats_Recommendations_for_Financial_Institutions.pdf

[8] Section 1000.1 pg. 8 of the Federal Reserve System's commercial Bank Examination Strategy and Risk Focused Examinations, (2011), http://www.federalreserve.gov/boarddocs/supmanual/cbem/1000.pdf

[9] William J. Brown, Enforcement Specialist, Federal Reserve Bank of Philadelphia, "Understanding Reputational Risk: Identify, Measure and Mitigate the Risk", (2007), http://www.philadelphiafed.org/bank-resources/publications/src-insights/2007/fourth-quarter/q4si1_07.cfm#one

[10] Jason Perry, Measuring Reputational Risk: The Market Reaction to Operational Loss Announcements, Barclays, quoted in "Banking on a reputation," Financial Risks Today, (2011) http://www.financialriskstoday.com/reputation_june.php

[11] Securities Suits Remain Off Recent Highs, Advisen, (2012) http://corner.advisen.com/advisen_webinars_2012_Q2_Sec_Lit.html

[12] Guy Kovner," Investors file new lawsuit against Sonoma Valley Bank," The Press Democrat, (2011) http://www.pressdemocrat.com/article/20110817/BUSINESS/110819548?p=1&tc=pg

[13] Michael Dandini, The Hartford Financial Services Group, Risk & Insurance Online, "The Evolving Landscape: Financial Crisis adds to complexity of D&O market, which demands more vigilance from buyers," (2010), http://www.riskandinsurance.com/printstory.jsp?storyId=533327124

[14] Michawel B. Himmel & Melissa Toner Lozner, FCPA Regulators Set Sights On Private Equity, VCExperts, Lowenstein Sandler, (2012) http://www.lowenstein.com/files/Publication/84c001cf-8cc4-444f-857c-0ce442f36bf4/Presentation/PublicationAttachment/b98ed255-6d96-4f52-9eed-1035ca2b4c79/FCPA%20Regulators%20Set%20Sights%20on%20Private%20Equity%20VC%20Experts.pdf