Global risk management survey, ninth edition - select key insights

Operating in the new normal: increased regulation and heightened expectations

Edward T. Hida II, CFA
Global Risk & Capital Management Leader
Global Financial Services Industry
Deloitte Touche Tohmatsu Limited

We are pleased to share with you here a selection of key insights from current top of mind issues explored in DTTL's Global risk management survey, ninth edition. In this feature we have selected the current issues of regulatory risk, cybersecurity and risk data and technology systems for discussion. To view the full 56-page report and the accompanying infographic, please visit http://www2.deloitte.com/global-risk-management-survey. For any questions regarding the survey please contact the survey editor, Edward Hida, Global Risk and Capital Management Leader, DTTL, at ehida@deloitte.com.

The global financial crisis was the catalyst for an era of sweeping regulatory change that shows little sign of abating. Across the financial services industry, regulatory requirements are becoming broader in scope and more stringent. After new regulations are enacted, it can take years before their practical implications become clear. Although the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) in the United States and Basel III were introduced several years ago, their rules are still being finalized. New regulatory developments include the US Federal Reserve's Enhanced Prudential Standards (EPS), the European Central Bank (ECB) becoming the prudential supervisor of eurozone banks, a new Banking Standards Review Council in the United Kingdom, and Solvency II becoming effective for European insurers in 2016.

The new regulatory landscape is placing demands on financial institutions in such areas as corporate governance, risk appetite, capital adequacy, stress tests, operational risk, technology data and information systems, and risk culture, to name only some areas of focus. As institutions prepare to comply, they will need the flexibility, in both their business models and compliance programs, to respond to the seemingly inevitable next round of reforms.

DTTL's *Global risk management survey, ninth edition* assesses the industry's risk management practices and challenges in this period of reexamination. The survey was conducted in the second half of 2014 and includes responses from 71 financial services institutions around the world that operate across a range of financial sectors and with aggregate assets of almost US$18 trillion.

Key Findings

More focus on risk management by boards of directors. Reflecting increased regulatory requirements, 85 percent of respondents reported that their board of directors currently devotes more time to oversight of risk than it did two years ago. The most common board responsibilities are to approve the enterprise-level statement of risk appetite (89 percent) and *review corporate strategy for alignment with the risk profile of the organization* (80 percent).

Broad adoption of CRO position. During the course of this global risk management survey series, the existence of a Chief Risk Officer (CRO) position has grown to be nearly universal. In the current survey, 92 percent of institutions reported having a CRO or equivalent position, up from 89 percent in 2012 and 65 percent in 2002. Although it is considered a leading practice[1] for the CRO to report to the board of directors, only 46 percent of respondents said this is the case, while 68 percent said the CRO reports to the CEO.[2] In a positive sign, 68 percent of respondents said the CRO has primary oversight responsibility for risk management, an increase from 42 percent in 2012. Three responsibilities of the independent risk management program led by the CRO were cited by more than 90 percent of respondents: *develop and implement the risk management framework, methodologies, standards, policies, and limits; oversee risk model governance; and meet regularly with board of directors or board risk committees.* Yet only 57 percent of respondents said their risk management program had the responsibility to approve new business or products.

ERM becoming standard practice. It has become a regulatory expectation for larger institutions to have an Enterprise Risk Management (ERM) program, and this is reflected in the survey results. Ninety-two percent of respondents said their institution either had an ERM program or was in the process of implementing one, an increase from 83 percent in 2012 and 59 percent in 2008. Another positive development is that among these institutions, 78 percent have an ERM framework and/or ERM policy approved by the board of directors or a board committee.

Progress in meeting Basel III capital requirements. Eighty-nine percent of respondents at banks subject to Basel III or to equivalent regulatory requirements said their institution already meets the minimum capital ratios. The most common response to Basel III's capital requirements was to *devote more time on capital efficiency and capital allocation* (75 percent).

1 *About the term "leading practice": for the purposes of this paper, we consider industry practices to fall into a range, from leading to lagging. Some industry practices may be considered leading practices, which are generally looked upon favorably by regulators, industry professionals, and observers due to the potentially superior outcomes the practice may attain. Other approaches may be considered prevailing practices, which are seen to be widely in use. At the lower end of the range are lagging practices, which generally represent less advanced approaches and which may result in less-than-optimal outcomes. Items reflected as leading practices herein are based on survey feedback and the editor's and contributors' experience with relevant organizations*

2 *Percentages total to more than 100 percent since respondents could make multiple selections*

Increasing use of stress tests. Regulators are increasingly relying on stress tests to assess capital adequacy, and respondents said stress testing plays a variety of roles in their institutions; for instance, it enables forward-looking assessments of risk (86 percent), *feeds into capital and liquidity planning procedures (85 percent), and informs setting of risk tolerance* (82 percent).

Low effectiveness ratings on managing operational risk types. Roughly two-thirds of respondents felt their institution was extremely or very effective in managing the more traditional types of operational risks, such as legal (70 percent), *regulatory/compliance* (67 percent), and *tax* (66 percent). Fewer respondents felt their institution was extremely or very effective when it came to other operational risk types such as third party (44 percent), *cybersecurity* (42 percent), *data integrity* (40 percent), and *model* (37 percent).

More attention needed on conduct risk and risk culture. There has been increased focus on the steps that institutions can take to manage conduct risk and to create a risk culture that encourages employees to follow ethical practices and assume an appropriate level of risk, but more work appears to be needed in this area. Sixty percent of respondents said their board of directors works to *establish and embed the risk culture of the enterprise and promote open discussions regarding risk*, and a similar percentage said that one of the board's responsibilities is to review incentive compensation plans to consider alignment of risks with rewards, while the remaining respondents said these were not among the board's responsibilities. Only about half of respondents said it was a responsibility of their institution's risk management program to review the compensation plan to assess its impact on risk appetite and culture.

Increasing importance and cost of regulatory requirements. When asked which risk types would increase the most in importance for their institution over the next two years, regulatory/compliance risk was most often ranked among the top three, and 79 percent felt that *increasing regulatory requirements and expectations* were their greatest challenge. The most important impact of regulatory reform was *noticing an increased cost of compliance*, cited by 87 percent of respondents.

A closer look at select current issues

Regulatory risk

The wave of change since the global financial crisis has constituted the most far-reaching revision of regulatory requirements in decades, significantly increasing compliance requirements. The era of regulatory reform is far from over, with additional proposals from the Basel Committee and with final rules still to be established for many provisions of the Dodd-Frank Act in the United States and for the CMU and the EU regulations and directives in Europe.

The impacts of these more-stringent regulatory requirements are significant for many institutions, including higher capital requirements, restrictions on business activities, additional documentation for regulators, and new standards on risk data and infrastructure. Regulators are also turning their attention to qualitative issues, such as risk culture and the effectiveness of internal controls.

One result of all these regulatory requirements has been increased costs. When asked about the impacts of regulatory reform on their institution, respondents most often mentioned noticing an increased cost of compliance (87 percent up from 65 percent in 2012). Other impacts cited often were maintaining higher capital (62 percent up from 54 percent in 2012) and adjusting certain products, lines, and/or business activities (60 percent up from 48 percent).

Many respondents are concerned that compliance costs will continue to escalate. Considering the potential impact on their organization of supervisory and regulatory processes, respondents were most often extremely or very concerned about issues related to cost: *tighter standards or regulations that will raise the cost of doing existing business* (72 percent) and *growing cost of required documentation and evidence of program compliance* (60 percent).

The impacts of examinations and enforcement actions were also mentioned by many respondents: *regulators' increasing inclination to take formal and informal enforcement actions (53 percent) and more intrusive and intense examinations* (49 percent).

New regulatory requirements have not only increased costs, they have also limited the ability of many institutions to generate revenues. Reflecting this new reality, 43 percent of respondents said they were extremely or very concerned about *new restrictions or prohibitions on profitable activities that will require a significant change in business model or legal structure*.

Cybersecurity

Cybersecurity is an operational risk type that has become a high priority for financial institutions and regulators. The number and extent of cyber-attacks have shown "exponential growth"[3] according to one corporate security chief, with the financial services industry as a top target.[4] In response, double-digit increases in bank security budgets are expected in the next two years.[5] Once seen as only an IT issue, the impacts of cyber-attacks can spread across the organization and affect business lines, operations, legal, and communications, among other areas. With their widespread impacts, cybersecurity events also pose significant reputational risks to a company.

With the increase of major hacking incidents from both criminal enterprises and potentially state-sponsored actors, cybersecurity has been a major focus for regulators. In February 2015, the SEC's Office of Compliance Inspections and Examinations released the results of its examinations in 2014 of cybersecurity practices at more than 100 registered broker-dealers and investment advisers.[6] In the same month,

FINRA published its recommendations on effective cybersecurity practices, based on its 2014 examinations of financial services firms.[7] FINRA has announced that cybersecurity will again be one of its examination priorities in 2015.[8]

Given the increasing regulatory requirements and the potential reputational damage that can result from a data breach, financial institutions need a comprehensive cybersecurity program. Among the leading practices for such a program are that it places a priority on threats with the greatest potential impact and on safeguarding sensitive data and critical infrastructure; it implements a formal written plan to respond to cybersecurity incidents; it conducts penetration testing; has dedicated personnel; and it periodically reviews the firm's cyber insurance strategy.

42 percent of respondents felt their institution is extremely or very effective in managing cybersecurity, roughly similar to the percentage of respondents that said the same about managing third-party risk (44 percent). Third-party and cybersecurity risk are sometimes closely related since there have been security breaches involving third parties that have affected the confidentiality of customer information.

Respondents at large institutions (63 percent), which have more resources to devote to safeguarding their data and information systems, were more likely to consider their organization to be extremely or very effective in this area than those at mid-size (35 percent) or small institutions (25 percent).

Risk data and technology systems

The global financial crisis underscored the need for risk data that are accurate, timely, consistent, and aggregated across the enterprise. Since then, risk data has been a priority for regulators.

In 2013, the Basel Committee issued its BCBS 239 paper, which emphasizes that banks need systems capable of producing aggregated risk data for all critical risks during times of stress or crisis.[9] Banks must also fully document and validate their aggregation capabilities and reporting practices. G-SIBs must comply by 1 January 2016, and BCBS 239 suggests that supervisors apply the same rules to domestic systemically important banks (D-SIBs).

CCAR's stress tests require banks to aggregate risk data across regions and lines of business.[10] There are also stricter requirements for data quality and aggregation in various capital and liquidity requirements, Solvency II, the OCC's heightened standards, and MiFIR, among other regulations.

Complying with these requirements is an arduous task for some institutions. For example, many eurozone banks encountered difficulties in providing the accurate, timely data required by the ECB's asset quality review.[11] When asked about the challenges facing their institution, many respondents said that *risk information systems and technology infrastructure* (62 percent) and risk data (46 percent) are extremely or very challenging.

3 *Vikram Bhat and Lincy Francis Therattil, "Transforming cybersecurity: New approaches for an evolving threat landscape," Deloitte LLP, 2014, http://www2.deloitte.com/us/en/pages/financial-services/articles/dcfs-transforming-cybersecurity.html*

4 *Mandiant, "Not Your Average Cybercriminal: A Look at the Diverse Threats to the Financial Services Industry," 23 September 2013, as cited in Deloitte US's infographic "Transforming cybersecurity: New approaches for an evolving threat landscape"*

5 *Daniel Huang, Emily Glazer, and Danny Yadron, "Financial Firms Bolster Cybersecurity Budgets," Wall Street Journal, 17 November 2014, http://www.wsj.com/articles/financial-firms-bolster-cybersecurity-budgets-1416182536*

6 *"Cybersecurity Examination Sweep Summary," Office of Compliance Inspections and Examinations, Securities and Exchange Commission, 3 February 2015, http://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf*

7 *"SEC and FINRA Issue Results of Cybersecurity Examinations," The National Law Review, 18 February 2015, http://www.natlawreview.com/article/sec-and-finra-issue-results-cybersecurity-examinations*

8 *"2015 Regulatory and Examination Priorities Letter," Financial Industry Regulatory Authority, 6 January 2015, https://www.finra.org/web/groups/industry/@ip/@reg/@guide/documents/industry/p602239.pdf*

9 *"From principles to practicalities: Addressing Basel risk data aggregation and reporting requirements," Deloitte US, 2013, http://www2.deloitte.com/us/en/pages/regulatory/basel-risk-data-aggregation-and-reporting-requirements.html?nc=1*

10 *Joe Rennison, "Stress, tested," Risk Magazine, August 2014*

11 *"Top 10 for 2015: Our outlook for financial markets regulation", Deloitte EMEA Centre for Regulatory Strategy, 2015, http://www2.deloitte.com/global/en/pages/financial-services/articles/regulatory-top-ten-for-2015.html*

In response to these stricter requirements, many financial institutions have undertaken major data remediation and infrastructure programs. Progress has been made, but significant work remains to be done at many institutions.

Less than half of the respondents rated their institution as extremely or very effective in any area of risk data and infrastructure, although the ratings improved since 2012: *data management/maintenance* (39 percent compared with 20 percent in 2012), data process architecture/workflow logic (35 percent compared with 23 percent), *and data controls/checks* (31 percent roughly similar to 33 percent in 2012).

The pace of regulatory change places additional demands on risk technology systems. 48 percent of respondents said they are extremely or very concerned about *risk technology adaptability to changing regulatory requirements*, an increase from 40 percent in 2012, while 46 percent of respondents said the same about lack of integration among systems, up from 31 percent in 2012.

Most of the survey participants are multinational institutions, with 68 percent having operations outside their home country

About the survey

The full report presents the key findings from the ninth edition of Deloitte's ongoing assessment of risk management practices in the global financial services industry. The survey gathered the views of CROs or their equivalents at 71 financial services institutions around the world and was conducted from August to November 2014.

The institutions participating in the survey represent the major economic regions of the world, with most institutions headquartered in the United States/Canada, Europe, or Asia Pacific (Figure 1). Most of the survey participants are multinational institutions, with 68 percent having operations outside their home country. The survey participant companies provide a range of financial services offerings, including insurance (58 percent), banking (55 percent), and investment management (48 percent) (Figure 2).[12]

The institutions have total combined assets of US$17.8 trillion and represent a range of asset sizes (Figure 3). The survey participants that provide asset management services represent a total of US$5.6 trillion in assets under management.

Where relevant, the report compares the results from the current survey with those from earlier surveys in this ongoing series. Deloitte's *Global risk management survey* is conducted biennially.

Analysis by asset size

In this report, selected survey results are analyzed by the asset size of participating institutions using the following definitions:

- Small institutions - Institutions with total assets of less than US$10 billion
- Mid-size institutions - Institutions with total assets of US$10 billion to less than US$100 billion
- Large institutions - Institutions with total assets of US$100 billion or more

12 *Percentages total to more than 100 percent since some institutions provide more than one type of service. In the report, institutions that provide insurance services will sometimes be termed "Insurers" (even if they also provide other types of financial services) and institutions that provide investment management services will sometimes be termed "investment management companies" (even if they also provide other types of financial services)*

Figure 1: Participants by location of headquarters

39% US & CANADA

33% EUROPE

14% ASIA PACIFIC

8% LATIN AMERICA

6% AFRICA

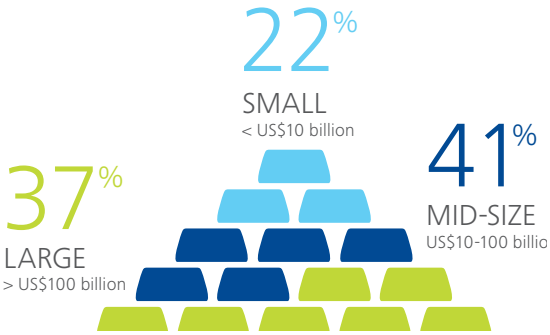
Figure 2: Participants by financial services provided

58% INSURANCE

55% BANKING

40% INVESTMENT MANAGEMENT

Figure 3: Participants by asset size



Note: percentages do not total 100% since respondents could make multiple selections.

Conclusion

The era of regulatory reform sparked by the global financial crisis has become the new normal. There have been an ongoing series of new regulations affecting risk governance, capital adequacy, liquidity, stress testing, and prohibitions on proprietary trading, among other areas. Institutions are being required to enhance their capabilities for managing operational risk, with both regulators and management especially concerned about the impacts of hacking and other types of cyber-attacks. Regulators are also focusing on the qualitative aspects of risk management. They are looking beyond quantitative measures of market, credit, and liquidity risk to assess whether institutions have created a culture that encourages employees to take appropriate risks and that promotes ethical behavior more broadly. In this effort, it is essential that incentive compensation schemes are aligned with an institution's risk appetite.

Success in all these areas depends on quality risk data and effective information systems. Yet, developing accurate, aggregated risk data on a timely basis remains a challenge. Measurement can be especially difficult for some risk types, such as operational risk, and for qualitative issues, such as risk culture. DTTL's Global risk management survey indicates there has been progress in many of these areas. But with the regulatory expectations being ratcheted up continually, institutions will need to keep pace by regularly upgrading their risk management capabilities:

- Many institutions have implemented strong risk governance at the level of their board of directors and senior management, including implementing an ERM program and creating a CRO position. They will now need to broaden their perspective to consider how they can manage conduct risk by embedding a risk culture throughout their organization that encourages ethical behavior by employees. Keys to this effort will be the board of directors and senior management communicating the value the organization places on treating customers fairly and also having incentive compensation practices that reward ethical behavior and appropriate risk-taking
- As regulators rely more on stress tests to assess capital adequacy and liquidity, institutions will need to improve their stress-testing capabilities and attract personnel with the required skills and experience. The talent shortage noted in the survey will make this an ongoing challenge
- More effective management of operational risks, especially cybersecurity, will be essential. Institutions will not only need to improve their IT security processes, but also their processes for selecting vendors and assessing their security procedures
- Institutions will need to reassess their risk data and information systems. Many institutions will need to improve their access to high-quality and timely risk data as well as their ability to quickly aggregate risk data across lines of business and geographies

Financial institutions are adjusting to the new environment for risk management. Most institutions will need to enhance their risk management programs to stay current—improving analytical capabilities, investing in risk data and information systems, attracting risk management talent, fostering an ethical culture, and aligning incentive compensation practices with risk appetite. They will find that business strategies and models must be reassessed in response to changed regulations more often than before. Perhaps most important, institutions will need to develop the flexibility to respond nimbly to the "new normal" risk management environment of unceasing regulatory change.

The era of regulatory reform sparked by the global financial crisis has become the new normal

To view the full 56-page report and the accompanying infographic, please visit http://www2.deloitte.com/global-risk-management-survey.