Deloitte.

Risk governance spotlight

Global risk management survey, 11th edition

Reimagining risk management to mitigate looming economic threats and nonfinancial risks

Executive summary

Financial institutions are confronting a new environment marked by impending economic perils and growing nonfinancial risks, such as cybersecurity and conduct. Economic storm clouds remain on the horizon in the form of a slowing Chinese economy, trade tensions among major countries, and concerns that the world economy may be ready for another in a series of periodic crises that have hit markets and reduced growth over the last several decades. Although the pace of regulatory change has slowed, a number of important regulatory requirements remain to be finalized, while the full implications of those that have been recently implemented are still being assessed, such as final Basel III revisions to the capital framework, Solvency II, and the European Union's (EU) General Data Protection Regulation (GDPR).

Technological innovation is also altering business models and the competitive marketplace. Fintech competitors are leveraging technology capabilities to introduce innovative new products and directly target customers. These firms are not confined to startups but also include major technology and e-commerce companies that bring preexisting customers and strong brands.

The evolving economic and business environment will require financial institutions to rethink their traditional approaches to risk management and adopt fundamentally new approaches. Managing this transition successfully will depend on strong risk governance, including an active role for the board of directors in providing oversight and challenge, an effective risk appetite statement, and a well-defined three lines of defense risk governance model. The growing importance of nonfinancial risks, such as cybersecurity, conduct and culture, and reputational risk, raises additional governance challenges such as ensuring appropriate oversight by the board of directors, assigning clear management accountability, and defining risk appetite for these hard-to-quantify risks.

Deloitte's *Global risk management survey, 11th edition*, the latest edition in this ongoing survey series, is based on the responses of 94 financial institutions on their risk management practices and challenges on a range of issues. Five key takeaways emerged regarding management of nonfinancial risks:

- Clarifying the mandate of the board of directors
- Establishing an effective CRO position
- Assigning accountability for managing nonfinancial risks
- Meeting challenges in defining risk appetite
- Reassessing the three lines of defense risk governance model

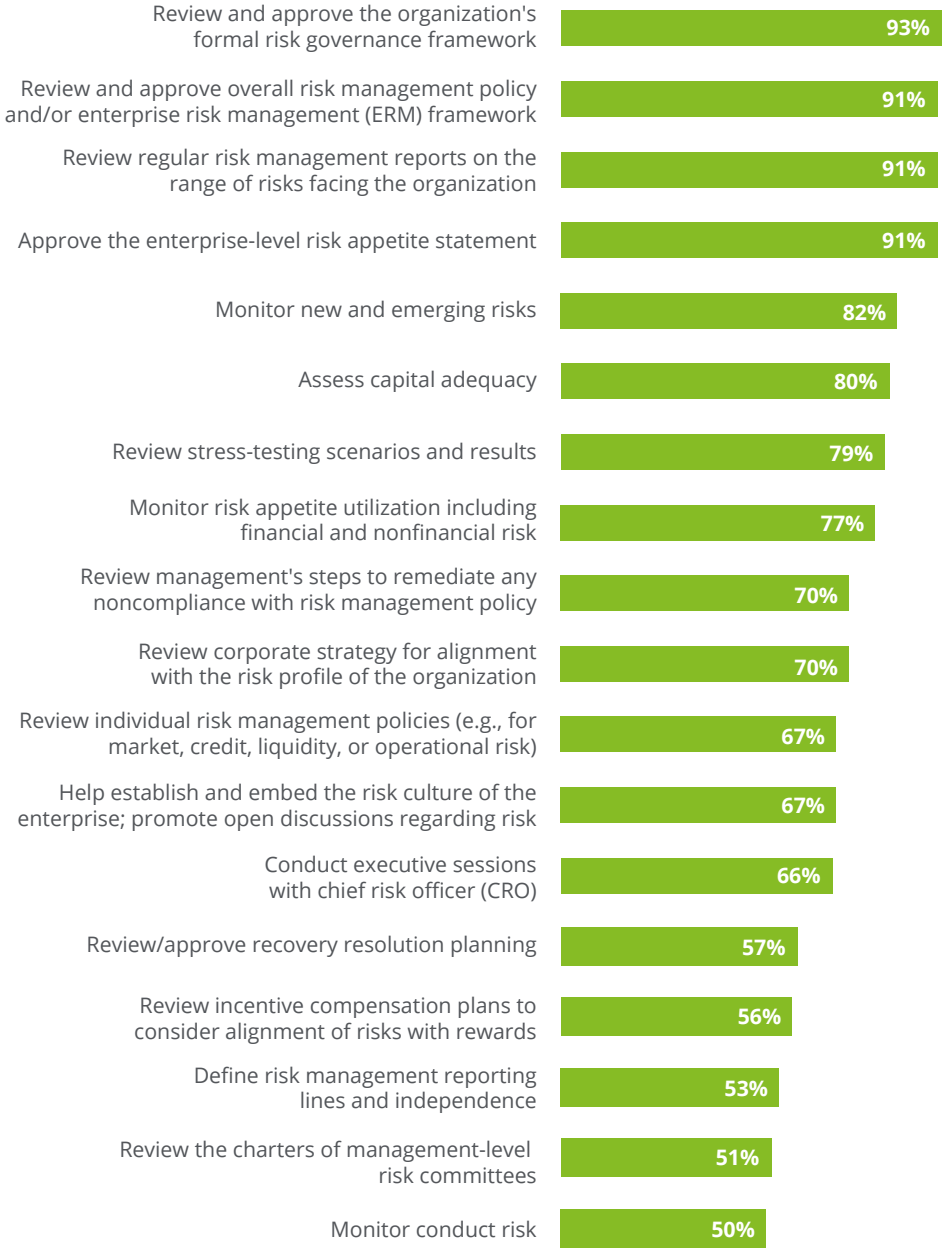
Clarifying the mandate of the board of directors

In the years since the global financial crisis, boards of directors have become much more active in providing oversight of the risk management programs at their institutions. Yet, often the lines have blurred between the oversight responsibilities of the board of directors and the operational responsibilities more appropriately the province of management. Financial institutions and regulatory authorities are now recalibrating the role of the board of directors to have it focus more clearly on providing oversight.

More than 90 percent of institutions reported that their board has a number of core risk management oversight responsibilities such as *review and approve the organization's formal risk governance framework* (93 percent), *review and approve overall risk management policy and/or enterprise risk management (ERM) framework* (91 percent), *review regular risk management reports on the range of risks facing the organization* (91 percent), and *approve the enterprise-level risk appetite statement* (91 percent) (see figure 1).

Boards less often have oversight responsibilities in other areas. Although business strategy can often drive an institution's risk profile, the role of the board in considering these impacts is far from universal, with 70 percent of respondents saying a board responsibility was to *review corporate strategy for alignment with the risk profile of the organization.* Despite the fact that conduct and culture risk is an increasing focus of regulatory authorities, only 50 percent of respondents said *monitor conduct risk* was a board responsibility, which may reflect the fact that many institutions see this as more of a management responsibility. In contrast, 67 percent said that a board responsibility was to *help establish and embed the risk culture of the enterprise/promote open discussions regarding risk.*

Figure 1
Which of the following risk oversight activities does your organization's board of directors or board risk committee(s) perform?



The percentage of respondents who said their board of directors had the responsibility to *monitor risk appetite utilization including financial and nonfinancial risk* was 77 percent, down from 89 percent two years ago. This is consistent with the trend that more institutions are having their boards concentrate on oversight, rather than activities more traditionally the province of management.

Placing oversight responsibility for risk management in a board risk committee is a regulatory expectation and has become a widely accepted practice. Sixty-three percent of respondents reported that the primary responsibility for risk oversight lies with a risk committee of the board of directors. An additional 21 percent of respondents said that oversight responsibility is placed with other committees, such as jointly with the combined risk and audit committees (7 percent). Only 14 percent of institutions said that the full board of directors has risk management oversight responsibility.

There has also been a trend among regulators to expect risk committees to include independent directors that have risk management expertise and skills—and these expectations have had an impact. Seventy percent of respondents said their board's risk committee comprises either entirely or a majority of independent directors, while 6 percent said it does not contain any independent directors. In addition, 84 percent of respondents said their institution has one or more risk management experts on its board risk committee, up from 67 percent in Deloitte's survey two years ago. Overall, the move toward independent directors is most pronounced in the United States/Canada, where 87 percent of respondents reported their board risk committee was composed of either entirely or a majority of independent directors, compared to 67 percent in Europe and 58 percent in Asia-Pacific.

"Due to regulatory and other pressures, over time the roles of the board and management had become blurred. Recently, there has been a reorientation to get the board and the board risk committee focused on strategic issues and oversight and not the day-to-day management of the business."

— **Senior risk executive**
Large global financial services company

Establishing an effective CRO position

Over the course of Deloitte's global risk management survey series there has been progress in meeting the regulatory expectation that financial institutions have an independent risk management function, with 95 percent of respondents in the most recent survey reporting that their institution has a chief risk officer (CRO) position or equivalent.

Institutions can benefit by having the CRO report both to the CEO and also to the board of directors, but this is not always the case. Seventy-five percent of respondents said their CRO reports to the CEO, which means that in one quarter of institutions the CRO does *not* report to the most senior management executive. Similarly, only 52 percent of respondents said that their CRO reports to the board of directors or a board committee. However, 97 percent of respondents said that their independent risk management group headed by the CRO meets regularly with the board of directors or with the board committees responsible for risk management oversight.

"The strategic planning process is a joint exercise between the business and risk management. Dedicated senior risk leaders are also responsible for providing advice and oversight pertaining to a business risk."

— Senior risk executive
Large diversified financial services company

There remains room for improvement. While the percentage of institutions that reported a responsibility of their board of directors was to *conduct executive sessions with the chief risk officer (CRO)* increased to 66 percent from 53 percent in the previous survey two years ago, more institutions should consider having their boards adopt this practice. Having the board of directors meet with the CRO, ideally sometimes without the CEO or other members of senior management present, can allow the board to receive an unvarnished assessment of the institution's risk management program.

Assigning accountability for managing nonfinancial risks

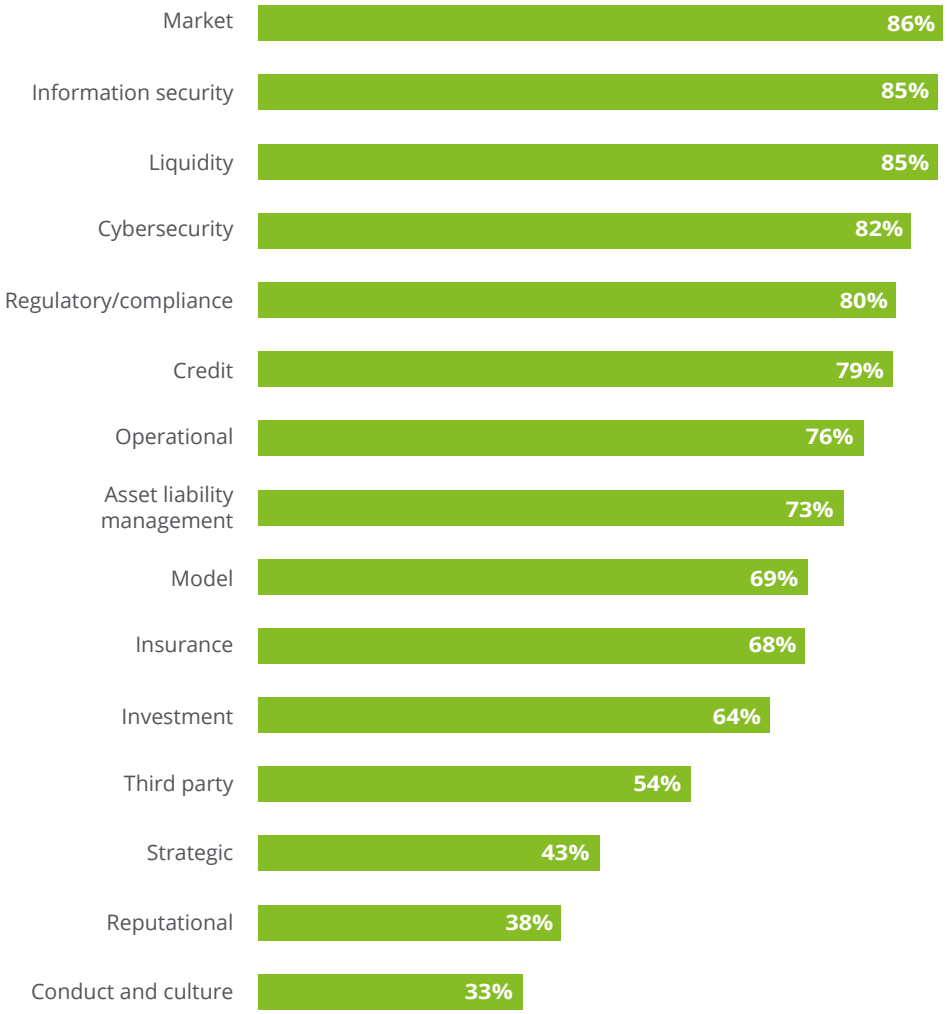
An important governance decision is how to assign responsibility for each risk type (or "stripe"), in particular whether there should be a single individual responsible for oversight of the risk across the organization, or instead have responsibility decentralized by business units or geographies. Having a single individual accountable has become common for financial risks such as *market* (86 percent), *liquidity* (85 percent), and *credit* (79 percent) (see figure 2).

When it comes to nonfinancial risks, there is much less consistency. With some nonfinancial risks, most institutions reported that a single executive is responsible, such as *regulatory/compliance* (80 percent), *information security* (85 percent), and *cybersecurity* (82 percent). In contrast, it is much less common to centralize responsibility for other risks such as *third party* (54 percent), *strategic* (43 percent), *reputational* (38 percent), and *conduct and culture* (33 percent). Institutions may want to consider centralizing accountability for some of these nonfinancial risks to raise their profile in the organization and clarify accountability.

Figure 2

For each of the following risk types, does your organization have a single individual who is specifically accountable for risk oversight?

Percentage responding "Yes"



Meeting challenges in defining risk appetite

A written risk appetite statement approved by the board of directors provides guidance to senior management when setting business strategy and for the lines of business when making business decisions, and should be periodically revisited.[1] The importance of a risk appetite statement has received greater attention from regulatory authorities in recent years, such as the Financial Stability Board and the Basel Committee.[2] Ninety percent of respondents said their institutions either have a risk appetite statement that has been approved by the board of directors (84 percent) or are developing a statement for approval (6 percent).

Yet, institutions face a variety of challenges in defining and implementing an enterprise-level risk appetite statement, especially with defining risk appetite for hard-to-quantify nonfinancial risks. The risk types that were cited most often as being extremely or very challenging in defining risk appetite were *strategic* (51 percent), *cybersecurity* (44 percent), *reputational* (39 percent), *operational* (36 percent), and *conduct* (33 percent) (see figure 3).

Figure 3

How challenging is each of the following in defining and implementing your organization's enterprise-level risk appetite statement?

Base: Organizations that have a written enterprise-level statement of risk appetite

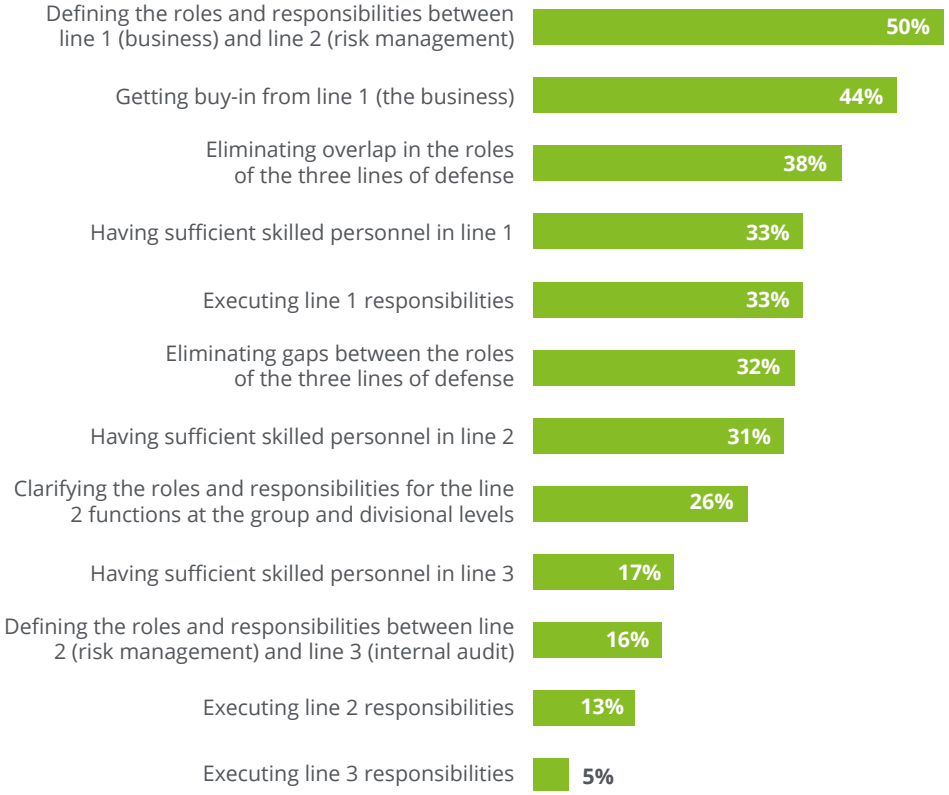
Percentage responding "extremely/very challenging"

Reassessing the three lines of defense risk governance model

Virtually all institutions (97 percent) reported employing the three lines of defense risk governance model, but many said they face significant challenges in deploying it. The issues most often cited as significant challenges typically involved the role of line 1 (business units) including *defining the roles and responsibilities between line 1 (business) and line 2 (risk management)* (50 percent), *getting buy-in from line 1 (business)* (44 percent), *eliminating overlap in the roles of the three lines of defense* (38 percent), *having sufficient skilled personnel in line 1* (33 percent), and *executing line 1 responsibilities* (33 percent) (see figure 4). There is also the related issue of *eliminating overlap in the roles of the three lines of defense,* which was considered to be a significant challenge by 38 percent of respondents. To address these challenges, 43 percent of institutions said they either have revised their three lines of defense model, reassessed their model, or plan to reassess it.

Many institutions have been focusing on the role of the first line of defense but have found it difficult to have their business units always assume full responsibility for actively managing the risks they assume. Some business units may resist accepting their responsibility for risk management, seeing it as outside their core mission of generating revenues and profits. Beyond securing buy-in, many business units will find they need to hire or develop a sufficient number of professionals that bring both risk management expertise and experience in the specific business.

Figure 4
What are the most significant challenges your organization faces in maintaining a "three lines of defense" risk governance model?
Percentage responding "Yes"



Conclusion

To successfully confront the array of economic threats and growing nonfinancial risks in today's shifting business environment, financial institutions will need to reengineer their risk management programs and adopt fundamentally new approaches—from increased attention to cybersecurity, conduct and culture, and other nonfinancial risks to leveraging the power of AI technologies to gain the ability to automatically identify and address potential risks before they occur.

As they introduce new methods, institutions will need to make parallel enhancements to the governance of their risk management programs. The three lines of defense risk governance model will need to be reassessed to clarify the roles and responsibilities of each line of defense, especially the business units comprising the first line. The second line of defense should have a reporting connection to the board's risk committee and in many cases, a "dotted line" connection to the CEO. Accountability for managing nonfinancial risks, such as conduct and culture risk and third-party risk, will need to be reexamined. Institutions will need to develop more robust methodologies and gain access to relevant data to allow them to quantify their risk appetite for nonfinancial risks.

Boards of directors should play a key role in fostering new approaches to risk oversight. At many institutions, boards will need to expand their focus to encompass oversight of the nonfinancial risks, such as conduct and culture, third party, and strategic risk, while ensuring that they truly concentrate on oversight rather than duplicate management responsibilities. In their oversight of the risk appetite framework and statement, boards should also assess if management has sufficiently tied risk to strategy and incorporated hard-to-quantify nonfinancial risks into their risk appetite statement. Finally, as companies try to push more risk management responsibility into the business units comprising the first line of defense, boards will need to make sure that they understand and are comfortable with those changes as their oversight role continues to evolve.

Global risk management survey, 11th edition

Global risk management survey, 11th edition is the latest edition in Deloitte's ongoing survey series that assesses the state of risk management in the financial services industry and the challenges the industry faces. The 2018 survey findings are based on the responses of chief risk officers or their equivalents at 94 financial institutions around the world. The institutions participating in the survey have total combined assets of US$29.1 trillion and represent a range of asset sizes: 26 percent with less than US$10 billion, 36 percent with US$10 billion to less than US$100 billion, and 37 percent with US$100 billion or more.[3] The participating institutions provide a range of financial services including banking (61 percent), investment management (49 percent), and insurance (46 percent).[4] To view the full report, please visit https://www.deloitte.com/insights/globalrisksurvey.

Endnotes

1 See Deloitte's report, *Directors' Alert 2018: Linkages to success*, Global Center for Corporate Governance, https://www2.deloitte.com/global/en/pages/risk/articles/deloitte-risk-directors-alert-2018.html.

2 Financial Stability Board, P*rinciples for an effective risk appetite framework*, November 18, 2013, http://www.financialstabilityboard.org/wp-content/uploads/r_131118.pdf; Bank for International Settlements (BIS), Guidelines: Corporate governance principles for banks, Basel Committee on Banking Supervision, July 2015, https://www.bis.org/bcbs/publ/d328.pdf.

3 Note: In this report, some percentages may not total to 100 percent due to rounding.

4 Note: The percentages total to more than 100 percent because some institutions provide more than one type of financial service.

Contacts

Global financial services industry leadership

Bob Contri
Global leader | Financial Services Industry
Deloitte Global
+1 212 436 2043
bcontri@deloitte.com

J.H. Caldwell
Global Financial Services leader | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
+1 704 227 1444
jacaldwell@deloitte.com

Survey editor

Edward T. Hida II, CFA
Partner | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
+1 212 436 4854
ehida@deloitte.com

Acknowledgments

This report is the result of a team effort that included contributions by financial services practitioners from member firms of Deloitte Touche Tohmatsu Limited around the world. Special thanks are given to Bayer Consulting for administering the survey and assisting with the final document.

Subject matter advisors

Mike Rossen, Jericho, New York, US
mrossen@deloitte.com

Irena Gecas-McCarthy, New York, New York, US
igecasmccarthy@deloitte.com

Deloitte.