Deloitte.

Nonfinancial risk spotlight

Global risk management survey, 11th edition

Reimagining risk management to mitigate looming economic threats and nonfinancial risk

Executive summary

Financial institutions and their regulators have broadened their scope from a traditional focus on financial risks, such as market, credit, and liquidity, to encompass a broad range of nonfinancial risks. Many of the largest risk events in recent years have stemmed from nonfinancial, rather than financial, risk.

The category of nonfinancial risk is usually defined by exclusion—that is, as any risks other than financial risks—and leverages the operational risks as defined in the seven Basel operational risk event types and includes emerging risks such as cybersecurity, conduct, model, compliance, strategic, and third-party risk, among others.

These risks can not only have direct financial impacts but also damage an institution's reputation and brand. Yet, institutions typically have less well-developed methodologies and processes, and less access to relevant data, when it comes to nonfinancial risks. Institutions will benefit from adopting a holistic nonfinancial risk framework that offers an integrated approach to managing these risks. Such a framework should be based on a comprehensive inventory of nonfinancial risks and relevant controls, linked to the risk appetite framework, and employ a consistent assessment approach.

Nonfinancial risks are growing in size and importance. The focus has moved beyond traditional operational risks to risks like cyber, conduct and culture, and third-party risk management. Dealing with the challenges posed by these risks requires additional resources.

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

Financial institutions will need to adopt new approaches to meet the challenge of effectively managing nonfinancial risk. 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:

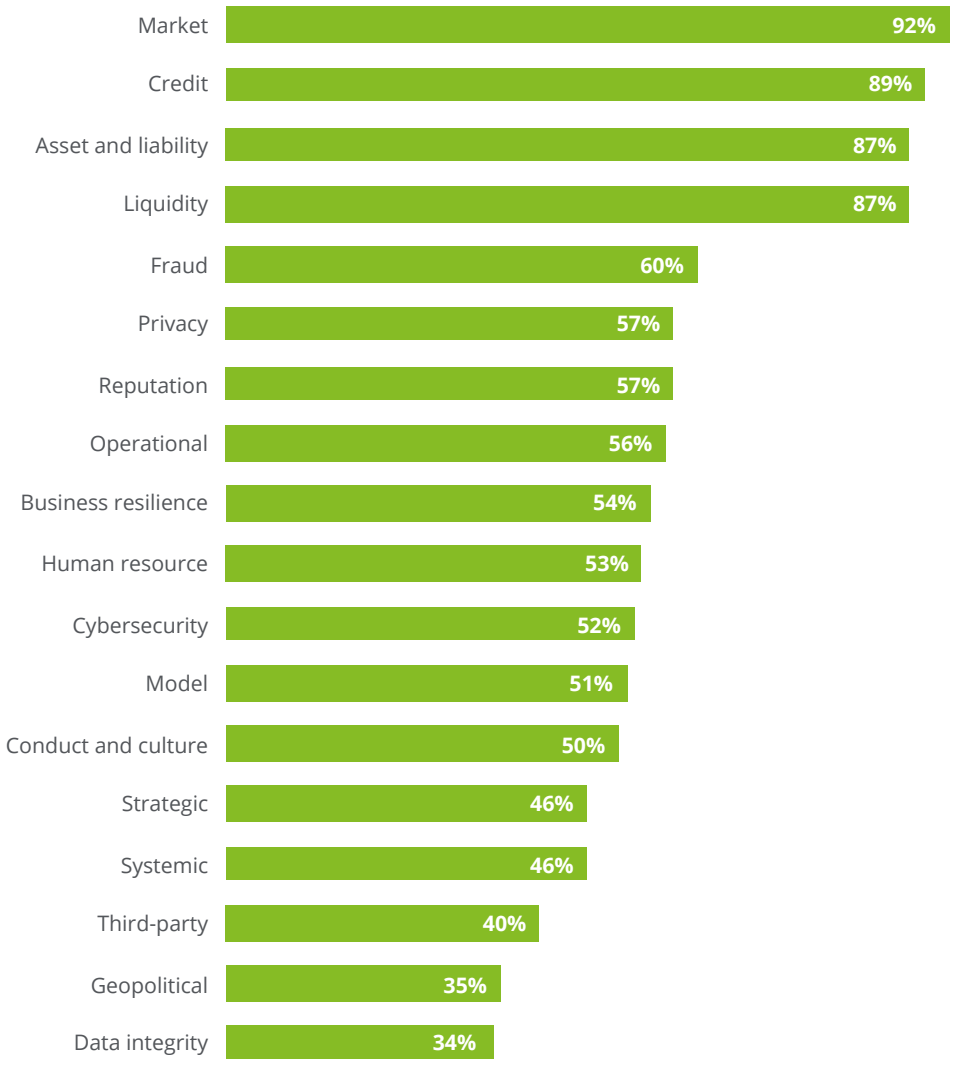
- Financial institutions are less effective in managing nonfinancial risks
- Growing importance of cybersecurity risk
- Increasing focus on conduct and culture
- Distinctive risks presented by third-party service providers
- Ongoing challenge of operational risk data and methodologies

Financial institutions are less effective in managing nonfinancial risks

More than three quarters of respondents considered their institutions to be extremely or very effective in managing traditional financial risks such as *market* (92 percent), *credit* (89 percent), *asset and liability* (87 percent), and *liquidity* (87 percent). In contrast, only 56 percent of respondents said the same about the nonfinancial risks grouped as *operational* (56 percent). Similarly, roughly half or fewer of the respondents felt their institutions were extremely or very effective at managing *cybersecurity* (52 percent), *business resilience* (54 percent), *model* (51 percent), *conduct and culture* (50 percent), *strategic* (46 percent), *third-party* (40 percent), and *geopolitical* (35 percent). See figure 1.

Institutions have long experience in managing financial risks, with well-developed models and analytics, and access to relevant data. In contrast, for nonfinancial risks; methodologies, risk assessments, and controls are less advanced and often fragmented; gaining access to relevant data is more difficult; and regulatory expectations are less well defined. In addition, it is inherently difficult to define and quantify some nonfinancial risk types and integrate them into the risk appetite statement. Respondents said their institutions found it to be extremely or very challenging to define and implement their enterprise-level risk appetite statement for nonfinancial risks such as *strategic* (51 percent), *cybersecurity* (44 percent), and *reputational* (39 percent).

Figure 1
How effective do you think your organization is in managing each of the following types of risks?
Selected risks
Percentage responding "extremely/very effective"



Growing importance of cybersecurity risk

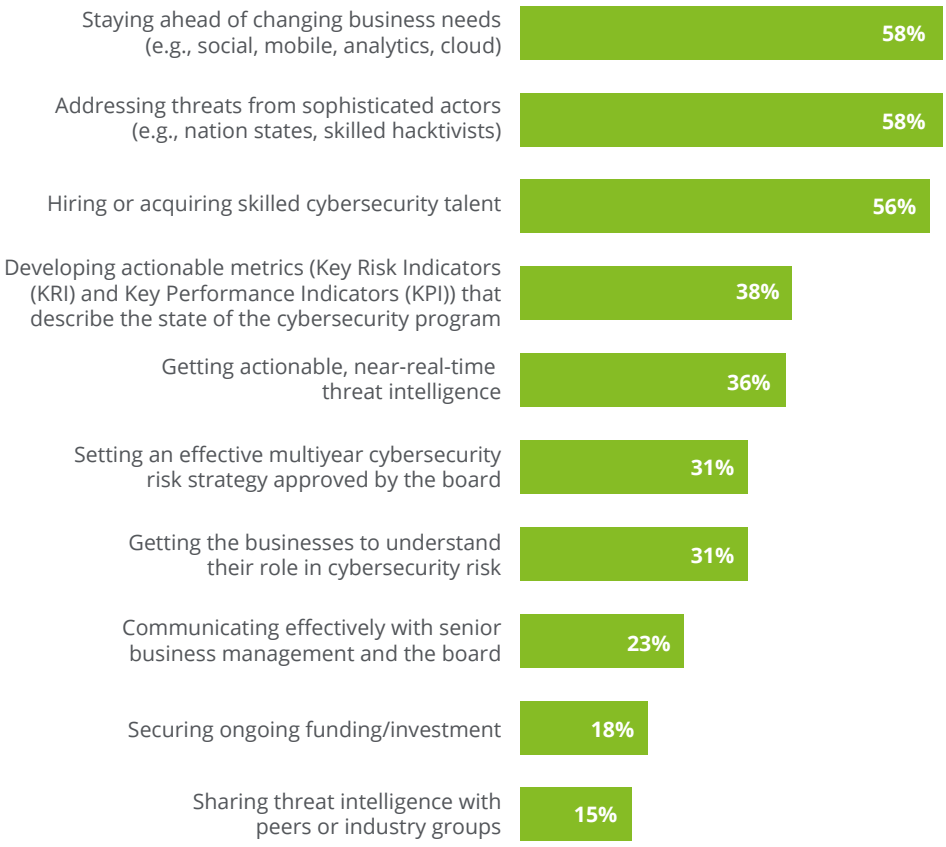
A series of cyberattacks against financial institutions and other companies has increased the attention of financial institutions and regulators on cybersecurity. Cyber threats continue to increase in sophistication, allowing hackers to obtain confidential information such as client data, install ransomware, initiate unauthorized payments, conduct espionage, and disrupt online systems, among other threats.

The losses from cyberattacks were an estimated US$445 billion across all industries in 2016, up 30 percent from three years before, and banks and other financial institutions are prime targets of hackers.[1] The US Treasury Department has named cyberattacks one of the top risks facing the US financial sector.[2] Regulatory initiatives focused on cyber risk have been launched in the United States, the United Kingdom, Hong Kong, mainland China, Japan, Singapore, and Australia.

Sixty-seven percent of respondents named *cybersecurity* as one of the three risks that would increase the most in importance for their business over the next two years, with 40 percent naming it No. 1 —both figures far higher than for any other risk type. Yet, only 52 percent of respondents believed their institutions are extremely or very effective at managing this risk. Respondents least often considered their institutions to be extremely or very effective in addressing *threats from nation state actors* (37 percent), *threats from skilled hacktivists* (43 percent), and *insider threats* (44 percent).

Institutions face a variety of challenges in managing cybersecurity risk, with respondents most often considering *staying ahead of changing business needs* (e.g., social mobile, analytics, cloud) (58 percent), *addressing threats from sophisticated actors* (e.g., nation states, skilled hacktivists) (58 percent), and *hiring or acquiring skilled cybersecurity talent* (56 percent) to be extremely or very challenging (see figure 2). Institutions are likely to supplement their cybersecurity professionals with an increased use of predictive analytics and automation, which can handle the volume of incidents and also screen and identify potential breaches before they occur and take automated corrective actions.

Figure 2
In your opinion, how challenging is each of the following for your organization in managing cybersecurity risk?
Percentage responding "extremely/very challenging"



Increasing focus on conduct and culture

A series of instances of misconduct and unethical behavior at major financial institutions around the world has underscored the importance of managing conduct and culture risk. There have been legislative and regulatory initiatives around the world to strengthen risk management in this area including the European Union, Hong Kong, Australia, the United Kingdom, and the United States. Notably, in September 2018, Australia's Royal Commission into Misconduct in the Banking, Superannuation, and Financial Services Industry delivered an interim report that found widespread misconduct among financial institutions as well as inadequate supervision by the regulators.

Advanced technologies—such as cognitive analytics, machine learning, and natural language processing—can play an important role in managing conduct risk by automatically analyzing the sentiment and tone of unstructured data (such as emails, texts, and chat messages) to detect, and potentially prevent, instances of misconduct before they occur.

> From a conduct risk perspective, it's very important that we continue to educate people and reinforce the culture. One informal way our CRO assesses conduct risk is by seeing how risk is brought up at town halls and management discussions and how it is cascaded down to all levels of the organization.
>
> — **Senior risk management officer**
> **Large financial services company**

Only half the respondents believed their institutions were extremely or very effective at managing conduct risk, placing it 25th out of 31 risk types ("stripes"). While 55 percent of respondents said *help establish and embed the risk culture of the enterprise/promote open discussions regarding risk* is an extremely or very high priority for their institutions, only 28 percent named *establishing a formal conduct and culture program* as a top priority. Institutions may find they need to formalize their activities into a defined conduct and culture program in order to communicate its importance and detail the specific steps that should be taken to manage this risk.

Distinctive risks presented by third-party service providers

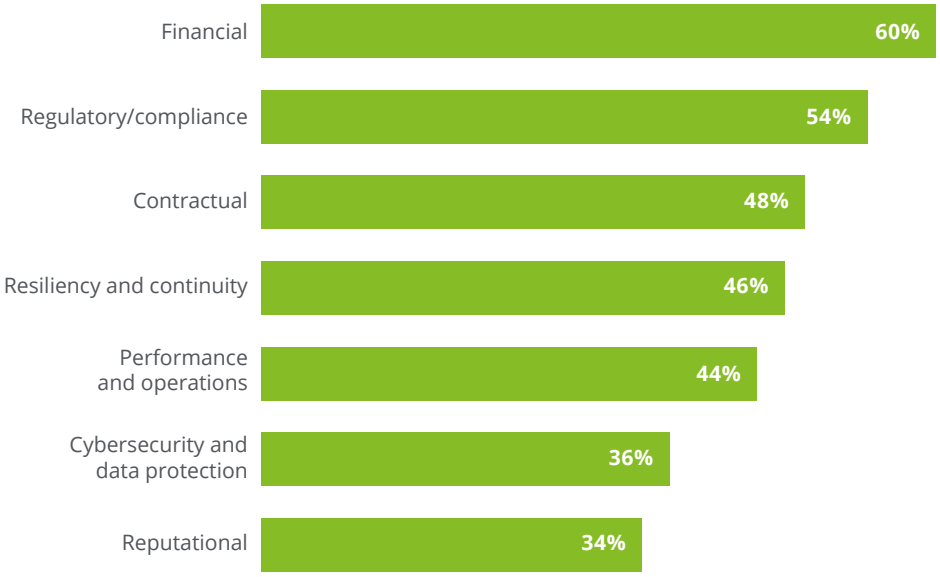
Many institutions rely on third-party service providers, but these relationships present a distinctive set of risks including nonperformance, theft of intellectual property, violations of laws, unethical conduct, data breaches, and the inability to provide services in case of an infrastructure breakdown or disaster. These providers themselves may subcontract a portion of the work to additional vendors. Although third-party service providers are not under the direct control of the financial institution, if they fail to perform or engage in illegal or unethical conduct, their actions can cause significant financial and reputational damage to the institution. Regulators have made clear that financial institutions are responsible for managing the risks posed by their third parties.

Only 40 percent of respondents felt their institutions were extremely or very effective at managing the overall risks from their relationships with third-party service providers. In specific areas, just 34 of respondents said their institutions were extremely or very effective in managing the *reputational* risk from these relationships, and 36 percent said the same about the risk related to *cybersecurity and data protection* from its third-party relationships (see figure 3).

Figure 3

When managing risk from third parties, how effective do you think your organization is in managing each of the following risk types?

Percentage "extremely/very effective"



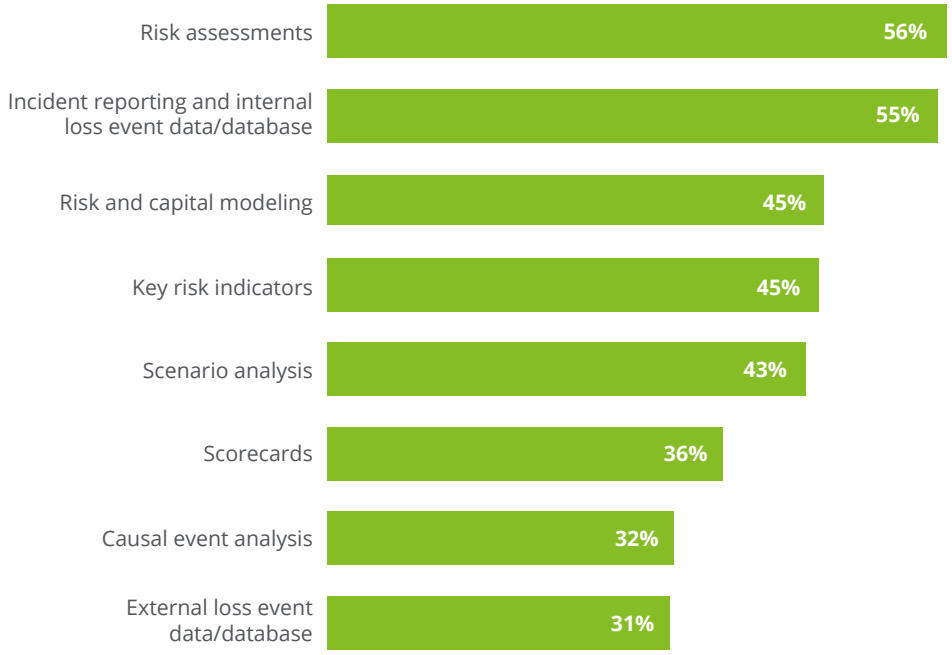
Ongoing challenge of operational risk data and methodologies

Operational risk has received significant attention in recent years from financial institutions and regulators. The Basel Committee made fundamental changes, to be implemented by January 1, 2022, in how operational risk capital is calculated by replacing the model-based Advanced Measurement Approach (AMA) with the Standardized Measurement Approach (SMA). The SMA is based on two variables: the Business Indicator Component, which is, in turn, based on selected financial data intended to be representative of the bank's business volume in different aspects, and the Internal Loss Multiplier, which is, in turn, based on the bank's actual operational risk loss history. As a result, banks will need to ensure that their internal loss databases are as accurate as possible and supported by robust IT systems, processes, and controls.

Despite the regulatory focus, only 56 percent of respondents felt their institutions were extremely or very effective when it came to managing operational risk. Less than half the respondents said their institutions' operational risk management methodologies were extremely or very well developed in such areas as *external loss event data/database* (31 percent), *causal event analysis* (32 percent), *scorecards* (36 percent), and *key risk indicators* (45 percent) (see figure 4).

Much work also remains to be done to develop the internal loss data that will be needed to employ the SMA. Fewer than 40 percent of respondents considered a number of important data issues to be extremely or very well developed at their institutions: *quality of loss data information* (34 percent), *sufficiency and granularity of legal loss data information* (34 percent), *consistency of loss event capture across different organizational units* (36 percent), *completeness of loss data events* (37 percent), and *sufficient duration of internal loss data* (39 percent).

Figure 4
How well developed is each of the following operational risk management methodologies at your organization?
Percentage responding "extremely or very well developed"



Conclusion

In the wake of a series of major nonfinancial risk events, financial institutions and regulators are devoting considerably more attention to the broad range of nonfinancial risks, such as cybersecurity, conduct and culture, and third-party risk. Effectively managing these risks will require institutions to rethink how risk management operates and the issues it addresses, and many will need to develop new methodologies and processes for these risks. Financial institutions may benefit from adopting a comprehensive framework for nonfinancial risk to allow an integrated approach.

Advanced technologies, such as cognitive analytics, machine learning, big data, and natural language processing, have the potential to automatically identify potential nonfinancial risk events before they occur to allow preventive action to be taken. Investments in risk data governance and IT systems will be needed to provide access to the high-quality, timely data required to quantify these risks and align them with the enterprise-wide risk appetite statement.

Beyond these steps, institutions are well advised to enhance their governance structure as well, such as grouping their nonfinancial risk management activities within a nonfinancial risk function under the chief risk officer (CRO).

The growing threats from nonfinancial risks is a central element of a new landscape that is requiring new risk management approaches. Financial institutions will need to consider new approaches to managing these risks—from leveraging advanced technologies to adopting a nonfinancial risk framework—if they are to thrive in this new environment.

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 it 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 James Lewis, *Economic impact of cybercrime—No slowing down,* McAfee, February 2018, https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/economic-impact-cybercrime.pdf; Stacy Cowley, "Banks adopt military-style tactics to fight cybercrime," *New York Times*, May 20, 2018, https://www.nytimes.com/2018/05/20/business/banks-cyber-security-military.html.

2 Office of Financial Research, US Department of the Treasury, *2017 Annual Report to Congress*, December 5, 2017, https://www.financialresearch.gov/annual-reports/2017-annual-report/.

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

Gerhard Schroeck, Frankfurt, Germany
gschroeck@deloitte.de

Michael Pieper, Frankfurt, Germany
mipieper@deloitte.de

Francisco Porta, Madrid, Spain
fporta@deloitte.es

Ricardo Martinez, New York, New York, US
rimartinez@deloitte.com

Deloitte.