Deloitte.

Insurance spotlight

Global risk management survey, 11th edition

Reimagining risk management to mitigate looming economic threats and nonfinancial risk

Executive summary

Insurance companies today are facing a series of impending threats that will require a reexamination of their traditional approaches to risk management. Global growth has been uneven, slowed by weak economic performance in Europe coupled with a Chinese economy saddled with increasing debt levels and slower growth. Tensions over tariffs between the United States, China, the European Union (EU), and other jurisdictions raise the possibility that the volume of global trade could shrink. Many issues remain to be resolved in the Brexit negotiations regarding the United Kingdom's exit from the European Union. Hovering over all these developments are concerns that the world economy may be poised for another in a series of periodic crises that have occurred over the last several decades.

Although the speed of regulatory change has slowed from the breakneck pace of recent years, a number of important regulatory requirements are yet to be finalized, while insurers are still assessing the impact of others that have recently taken effect such as the EU's Solvency II, the Insurance Distribution Directive, and the General Data Protection Regulation (GDPR).

"From an insurance perspective, one of the biggest challenges in managing risk is whether you are getting paid for those hard-to-model risks—specifically, cyber risk and terrorism risk. As a commercial writer of coverage, those are perils that your policyholders are looking to insure but where the models are just not as developed as, say, a hurricane model, because you don't have the same level of historical claims data."

— **Senior risk executive**
Major insurance and asset management company

Insurers will need to take new approaches to respond to this rapidly evolving environment. Deloitte's *Global risk management survey, 11th edition,* the latest edition in this ongoing survey series, includes responses from 43 insurance companies on their risk management practices and challenges. Five key takeaways emerged for insurers:

- Growing focus on nonfinancial risk
- Leveraging advanced technologies
- Enhancing risk data and IT systems
- Retooling the three lines of defense model
- Keeping pace with ongoing regulatory change

Growing focus on nonfinancial risk

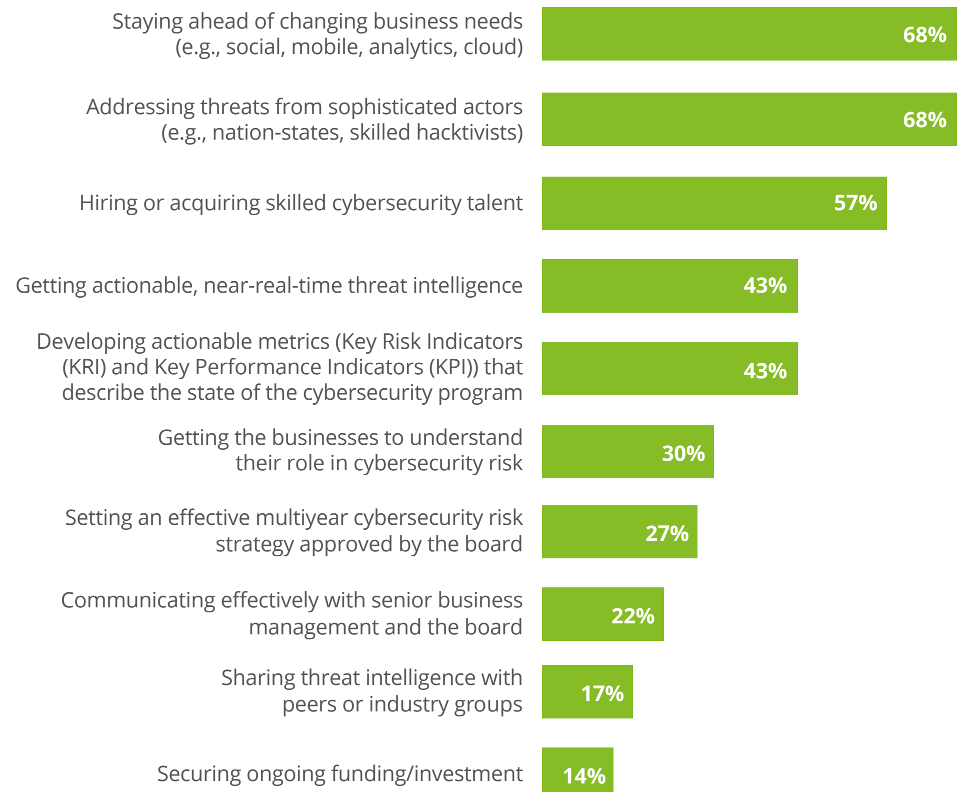
Both insurance companies and regulators have recognized the need for increased attention on nonfinancial risks, which can cause substantial financial and reputational damage.

While more than 80 percent of insurance respondents believed their companies were extremely or very effective in managing financial risks such as market, credit, and liquidity, they gave their companies much lower ratings when it came to nonfinancial risks such as cybersecurity, conduct and culture, data integrity, fraud, and third-party risk.

Cyber threats continue to proliferate and can result in hackers obtaining confidential information, installing ransomware, initiating unauthorized payments, conducting espionage, and disrupting online systems, among other threats. Sixty-five percent of insurance respondents named *cybersecurity* as one of the three risk types that would increase the most in importance, with 37 percent ranking it first, far more than any other risk type. Yet, only 49 percent said they are extremely or very effective at managing this risk. Insurers most often said the issues that were extremely or very challenging were *staying ahead of changing business needs* (e.g., social, mobile, analytics, cloud) (68 percent) and *addressing threats from sophisticated actors* (e.g., nation-states, skilled hacktivists) (68 percent) (figure 1). This is one of several instances where the insurer's risk function sees a healthy tension with growth of the business.

There have been a number of well-publicized instances of misconduct at major financial institutions, and only 49 percent of insurance respondents considered their company to be extremely or very effective at managing *conduct and culture risk*.

Figure 1
In your opinion, how challenging is each of the following for your organization in managing cybersecurity risk?
Base = Respondents at insurance companies
Percentage "extremely/very challenging"



Although not under an insurer's direct control, if a third-party service provider fails to perform or engages in misconduct, an insurer brand and reputation could suffer. Only 32 percent of insurance respondents felt their company was extremely or very effective at managing *third-party risk*.

Insurers will need to adopt a holistic approach, and some insurers have begun to group management of their nonfinancial risks, which have in the past (and are still sometimes) referred to as operational risks, within a nonfinancial risk function under the chief risk officer (CRO).

Leveraging advanced technologies

Advanced technologies and digital tools—such as big data, cloud computing, robotics and process automation, cognitive analytics, and natural language processing—have the potential to reengineer risk management. Beyond reducing expenses by automating manual tasks, machine learning and cognitive analytics tools can make predictions and take decisions without the need for explicit programming. When combined with natural language processing applications, these technologies can interpret unstructured data such as emails and texts and transform them into structured data that can be analyzed to identify emerging threats and take preventive action before they occur, while offering insight into their causal factors. By automating risk management processes, they provide the ability to automatically review 100 percent of a set of transactions, rather than rely on human review of only a sample.

Many insurers expect significant benefits from these technologies, especially in *enhance risk analysis and detection* (67 percent), *increase operational efficiency/reduce error rates* (64 percent), and *improve timely reporting* (62 percent) (figure 2).

While the benefits of new technologies promise to be substantial, institutions will need to be ready to manage the increased risks these technologies can create. Although automated solutions will reduce the potential for human error, their speed could increase the impact when errors or control breakdowns do occur. Further, institutions will need to monitor automated applications for potential instances of inadvertent bias or inaccurate results.

"We are embracing AI and predictive analytics, for example, in areas like monitoring customer behavior and potential fraud issues as well as applying robotics to automate manual policy processing tasks."

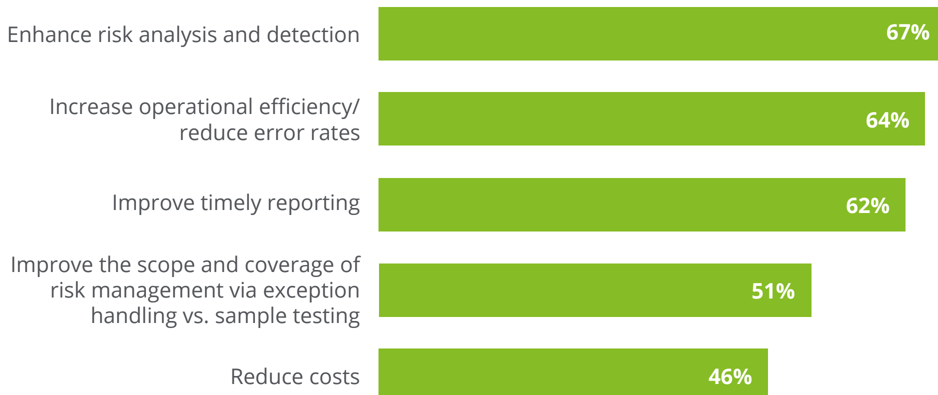
— **Senior risk executive**
Major insurance and asset management company

Figure 2

How much potential benefit do you believe that your organization could gain in each of the following risk management areas from the application of emerging technologies?

Base = Respondents at insurance companies

Percentage responding "extremely/very large benefit"



Enhancing risk data and IT systems

Employing advanced technology tools will require access to relevant high-quality, timely data and robust IT systems. Regulatory developments are also increasing the importance of strong data governance. GDPR, which took effect in May 2018, places new obligations on all financial institutions that have the data of EU citizens to secure consumer consent for its use, among other requirements. Insurers will need to work to ensure their data governance models comply with GDPR regarding such issues as data privacy and the extent to which data can be used to generate value for customers. Solvency II and International Financial Reporting Standard (IFRS) 17 will place additional demands on access to high-quality data across the organization.[1]

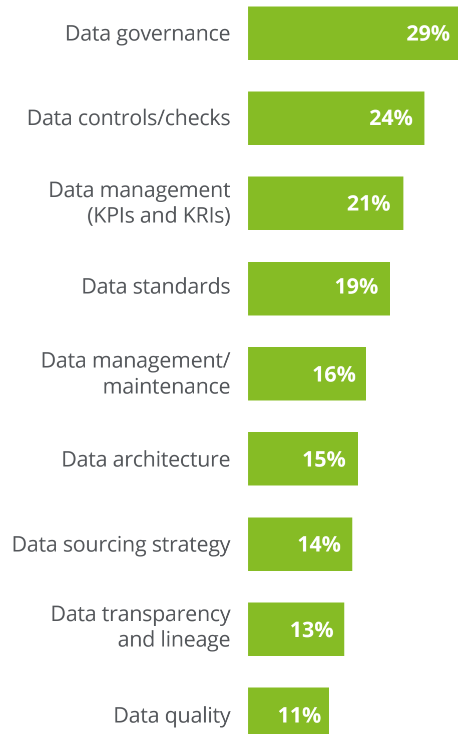
Insurers recognize that this is an area where improvements are required. Fewer than one-third of insurance respondents considered their companies to be extremely or very effective in areas such as *data governance* (29 percent), *data standards* (19 percent), and *data quality* (11 percent) (figure 3). Reflecting these assessments, the issues cited most often by insurers as being extremely or very high priorities over the next two years concerned data and IT systems: *enhancing the quality, availability, and timeliness of risk data* (77 percent) and *enhancing risk information systems and technology infrastructure* (67 percent).

Insurance companies will need to invest in building an integrated data architecture and an effective data controls framework. Many insurers are coming to see data—and how they can leverage its power within regulatory boundaries—as one of the critical assets for their future success. Rather than leaving data to be housed in the business units, more insurers are placing management of this enterprise asset within the C-suite, with some creating a chief data officer (CDO) position.

"Cyber risk has become a standing agenda item on every board risk committee meeting. Our biggest challenge in cyber is the all-out sprint to continually manage patches and updates to stay ahead of vulnerabilities. We also have ongoing contingency planning to manage potential incidents."

— **Chief risk officer**
Large multinational insurance company and financial services provider

Figure 3
How effective do you think your organization is in each of the following aspects of risk data strategy and infrastructure?
Base = Respondents at insurance companies
Percentage responding "extremely/very effective"



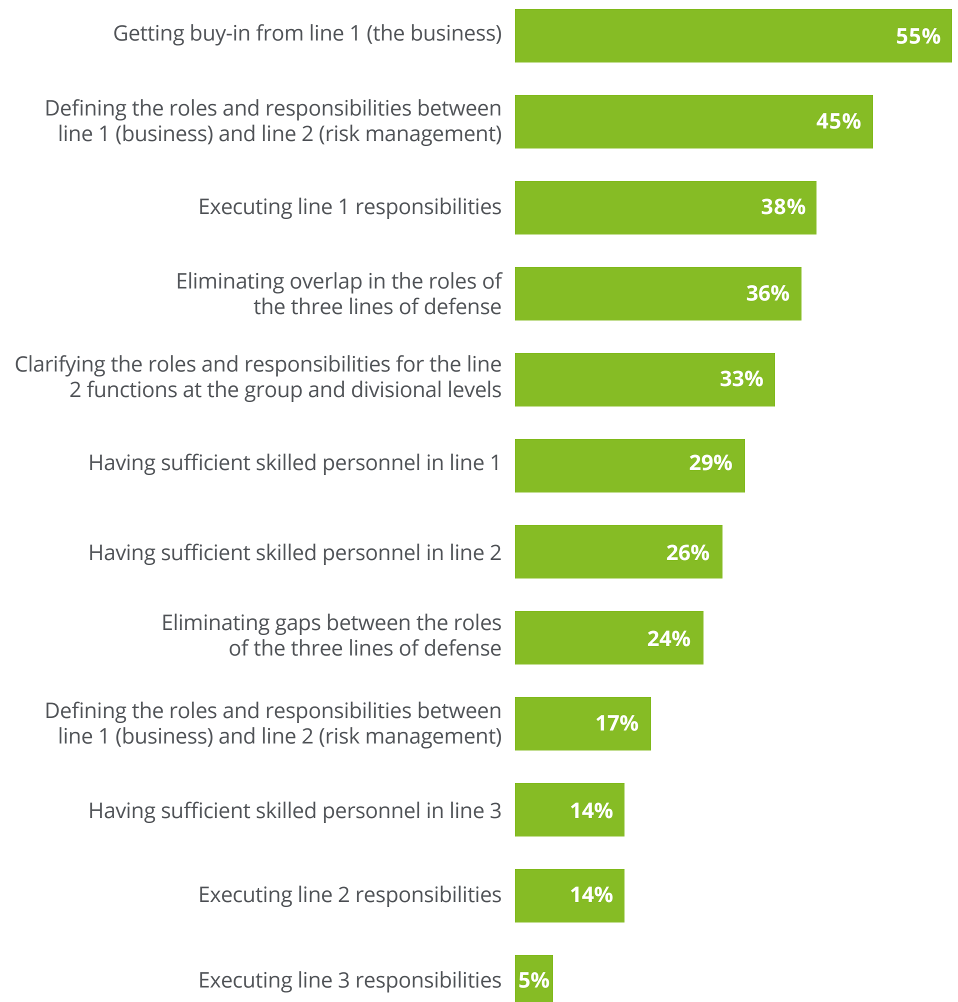
Retooling the three lines of defense model

All insurers reported employing the "three lines of defense" risk governance model, but many have found it difficult to operate effectively. The increasing use of advanced technologies has exacerbated these challenges. The introduction of digital solutions by the business units comprising Line 1 has accelerated the introduction of new products and services, which is requiring Lines 2 and 3 to keep pace. Insurers are also employing advanced analytics and automated solutions in their risk management (Line 2) and internal audit (Line 3) functions, which is changing how these lines function and their relationship to Line 1.

The three lines of defense model is based on the premise that the business units in Line 1 are responsible for managing the risks they assume, but this has not been easy to achieve. Although risk management is a central element of the mission of business units, many insurance companies find it difficult to specify the risk management role of Line 1 and how it should coordinate with Line 2. When asked about the three lines of defense risk governance model, insurance respondents most often said their companies faced significant challenges in *getting buy-in from line 1 (business)* (55 percent) (figure 4). One reason may be that many insurance companies find it difficult to clarify how Line 1 and Line 2 should coordinate, with 45 percent of insurance respondents saying that *defining the roles and responsibilities between line 1 (business) and line 2 (risk management)* presented a significant challenge.

Despite these and other challenges, only 30 percent of insurers said they had either revised their three lines of defense model or were planning to reassess it, compared to 51 percent for banks and 52 percent for investment management firms in the survey. To help ensure the three lines of defense model is working as intended, with each line fully accepting and executing its role, more insurance companies may find they need to undertake a reexamination of their model. Such reassessment and renewal programs should consider how to recalibrate the roles of each line of defense to align with operating models that have been transformed by digital technologies, while also taking account of evolving regulatory requirements.

Figure 4
What are the most significant challenges your organization faces in maintaining a "three lines of defense" risk governance model?
Base = Respondents at insurance companies



Keeping pace with ongoing regulatory change

Insurance companies are facing a variety of changes to regulatory requirements and accounting standards.

Consumer privacy. The EU's GDPR, which took effect in May 2018, placed new data protection requirements on all institutions that hold the data of EU citizens, wherever the institutions are located, including the need to obtain consumer consent before collecting personal data and providing consumers with more control over how their data is used. Other jurisdictions are also implementing new consumer privacy regulations including India and China. Among regulatory issues, insurance respondents most often said they were extremely or very concerned about *data privacy requirements* (51 percent).

Risk-based capital standards. Insurance regulators around the world are moving to introduce risk-based capital standards. Solvency II has been implemented in the EU, and other countries have drawn lessons from it. In the United States, the National Association of Insurance Commissioners (NAIC) is developing a risk-based group capital calculation for US insurance groups.[2] The International Association of Insurance Supervisors (IAIS) is working to develop a global insurance capital standard (ICS). Under the ICS, important issues remain to be resolved such as defining the valuation bases, the role of internal models in determining capital requirements, and resolving the purpose of Margin Over Current Estimate (MOCE), which is analogous to risk margin under Solvency II.

"It's sometimes hard for us to assess and keep pace of the overall regulatory environment given the constant drumbeat of changing regulatory expectations."

— **Chief risk officer**
Large multinational insurance company and financial services provider

Evolving accounting standards. IFRS 17, currently slated to take effect in 2022, will require insurance liabilities to be measured at a current fulfillment value. The Financial Accounting Standards Board (FASB) issued Accounting Standards Update (ASU) 2018-12, which amends the US Generally Accepted Accounting Principles (GAAP) for certain long-duration insurance contracts and requires insurers to provide additional disclosures.[3] Insurers will need to make significant changes across operating models, processes, and technology to comply with these new standards.

Eighty percent of insurance respondents expected the regulatory requirements on their companies would increase over the next two years, with one-third expecting a significant increase. These and other regulatory developments will entail substantial work to revise systems and processes as insurers transition to the new rules and then comply with additional reporting requirements, and potentially higher capital standards, going forward. All these developments have the potential to increase costs, and the regulatory issue cited second most often about which respondents were extremely or very concerned was *standards or regulations that will raise the cost of doing existing business* (50 percent).

Conclusion

Insurance companies will need to transform their risk and capital management programs to manage a variety of economic threats and changing regulatory requirements. Rather than remain content with traditional approaches, the new environment will require a more intense focus on nonfinancial risks such as cybersecurity, investments in improving risk data governance and IT systems, and the reassessment and retooling of the three lines of defense risk governance model.

Perhaps the most significant break with current approaches will be ushered in by digital technologies. These technologies are allowing insurers to develop innovative new products, while also freeing risk professionals from repetitive tasks to instead focus on identifying emerging risks and adding value. The more rapid pace of product introduction made possible by digital technologies, however, can be out of sync with the more deliberate pace of regulatory response. Insurers will need to determine how close to the leading edge of innovation they want to place themselves, while at the same time closely monitoring evolving regulatory requirements.

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 94 financial institutions around the world, including 43 insurance companies. These insurers represented a range of sizes as measured by their consolidated assets: 16 percent with less than US$10 billion, 40 percent with US$10 billion to less than US$100 billion, and 44 percent with US$100 billion or more. To view the full report, please visit https://www.deloitte.com/insights/globalrisksurvey.

Endnotes

1 For a discussion of the impact of Solvency II on data governance, see Deloitte's article "The impact of Solvency II and data management in insurance," written by Jean-Pierre Maissin and Ronan Vander Elst, *Inside* magazine, Issue 1, June 2013, https://www2.deloitte.com/lu/en/pages/risk/articles/impact-solvency-ii-data-management-insurance.html; for a discussion of data management and IFRS 17, see Deloitte's report, *Data management in the new world of insurance finance and actuarial,* written by Francesco Nagari and Angela Muriithi, 2017, https://www2.deloitte.com/content/dam/Deloitte/cn/Documents/financial-services/deloitte-cn-fs-data-management-in-new-world-of-insurance-finance-and-actuarial-en-171207.pdf.

2 "Risk-Based Capital," National Association of Insurance Commissioners, July 12, 2018, https://www.naic.org/cipr_topics/topic_risk_based_capital.htm; "NAIC update: Summer 2018," Deloitte, https://www2.deloitte.com/us/en/pages/financial-services/articles/naic-update.html.

3 "FASB makes targeted improvements to the accounting for certain long-duration insurance contracts," Deloitte's *Insurance Spotlight*, August 2018, https://www2.deloitte.com/content/dam/Deloitte/us/Documents/audit/ASC/IndPub/us-aers-ins-fasb-makes-targeted-improvements-to-the-accounting-for-certain-long-duration-insurance-contracts-august-2018.pdf

Contacts

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

Neal Baumann
Global leader | Insurance
Deloitte Global
+1 212 618 4105
nbaumann@deloitte.com

J.H. Caldwell
Global Financial Services leader | Deloitte Risk 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
Eric Clapprood, Hartford, Connecticut, US
eclapprood@deloitte.com

Markus Salchegger, Munich, Germany
msalchegger@deloitte.de

David Sherwood, Stamford, Connecticut, US
dsherwood@deloitte.com

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms and their related entities. DTTL (also referred to as "Deloitte Global") and each of its member firms are legally separate and independent entities. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our network of member firms in more than 150 countries and territories serves four out of five Fortune Global 500®companies. Learn how Deloitte's approximately 264,000 people make an impact that matters at www.deloitte.com.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms or their related entities (collectively, the "Deloitte network") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

© 2019. For information, contact Deloitte Touche Tohmatsu Limited.