

Global risk management survey, 12th edition

A moving target: Refocusing risk and resiliency amidst
continued uncertainty

Deloitte Risk & Financial Advisory


We don't believe that risk is simply managed—it is confronted. In Advisory, we do not take a defensive crouch. We move forward, defining the unknowns and framing the issues before you encounter them. Whether your challenge is cyber, transactional, regulatory, or internal controls, we can help prepare you to preempt the threat, define what's vital, and aggressively secure it. So that you can keep pace, get back to the business at hand—and move on what matters.

To learn more, visit [Deloitte.com](https://www.deloitte.com).

Contents

Foreword	2
Executive summary	4
Introduction: The COVID-19 era	9
About the survey	11
Risk management governance	13
Management of individual risk types	26
Risk management technology and data	38
Sector risk topics	42
Conclusion	47
Endnotes	49

Foreword

 ON BEHALF OF the Deloitte member firms, I am pleased to present the 12th edition of *The Global Risk Management Survey*, the latest installment in Deloitte's ongoing assessment of the state of risk management in the global financial services industry. The survey findings are based on the responses of 57 financial services institutions around the world across multiple financial services sectors, representing a total of US\$27.2 trillion in aggregate assets. In addition, this report is based on in-depth interviews conducted with a number of senior risk executives to gain deeper insight into the issues highlighted in the survey. We wish to express our appreciation to all the survey and interview participants for their time and insights.

The survey was conducted in an extraordinary period, as countries, businesses, and citizens around the world were responding to the COVID-19 global pandemic. In an effort to contain the novel coronavirus, governments across the globe imposed a series of lockdowns and other restrictions on economic activity; even when permitted to open, many businesses either closed their operations voluntarily or had many employees work remotely; and consumers quickly and dramatically changed their behavior and spending patterns. The resulting sharp economic downturn and the changes to working practices had broad implications for risk management.

With economies contracting and unemployment rising, credit risk rose significantly regarding lending both to consumers and businesses. Many banks have allowed borrowers to defer payments or have offered loan modifications, but they have also tightened credit standards for new lending.

Institutions have increased their focus on nonfinancial risks in recent years, and the COVID-19 pandemic has further highlighted both their importance and the challenges they present. While most respondents believed their institutions are extremely or very effective at managing financial risks, substantially fewer said the same about nonfinancial risk types and aspects such as operational resilience, cybersecurity, and conduct and culture, which have become more prominent in the COVID-19 period.

The pressure on revenues from the economic downturn has only increased the desire to reduce risk management expenses, which have been growing continually since the global financial crisis. Institutions are looking to the potential of emerging technologies to slash expenses by automating manual tasks while simultaneously increasing the effectiveness of risk management by improving testing, reducing errors, and identifying potential risk events before they occur, among other benefits.

Yet, while their potential benefits are clear, implementation of these technologies is proceeding slowly at many institutions. One of the obstacles is that many institutions lack the comprehensive, high-quality risk data that these technologies require, and more institutions are likely to increase their focus in this area.

Institutions reported that they have made progress in laying strong foundations for risk management governance in such areas as having a board-approved risk management framework and risk appetite

statement, having a board risk committee with independent directors and risk management experts, having an enterprise risk management (ERM) program in place, and employing the three lines of defense risk governance model. Yet, challenges remain, especially in clearly defining the roles and responsibilities of the first line (business units and functions) and second line (risk management) of the model, as well as ensuring that the first line has access to the required risk management talent.

The COVID-19 pandemic has changed the environment for risk management. Uncertainty remained at the close of 2020 as it was unclear how long the economic downturn would last and how long many employees would continue to work remotely. With the COVID-19 era approaching the one-year mark, financial institutions should focus on addressing such longer-term issues as maintaining morale, communicating their culture and values, and continuing to foster innovation in an environment where employees are interacting virtually.

The disruption caused by COVID-19 presents financial institutions with an extraordinary set of new challenges. Institutions will need strong risk management governance while having the agility and willingness to rethink their traditional approaches in a fundamentally altered business environment.

We hope that this view of risk management at financial institutions around the world provides you with helpful insights as you work to further enhance your organization's risk management program.

Sincerely,

J.H. Caldwell
Global Financial Services Risk Advisory Leader
Partner, Deloitte & Touche LLP

Executive summary

IN 2020, RISK management at financial institutions faced challenges of a scale and scope not seen in living memory as the world responded to a global health crisis caused by COVID-19. The measures taken by governments, businesses, and consumers to restrain the spread of the virus triggered a sharp economic downturn and far-reaching social impacts. Although promising results on the trials of several vaccines were announced as the year drew to a close, the numbers of cases and hospitalizations were again rising rapidly. The outlook for 2021 and beyond remains uncertain, depending largely on the ability to control the spread of COVID-19.

The Deloitte risk management survey was conducted from March through September 2020 during unprecedented times globally. When asked about the top trends that will increase the most in importance for their institutions over the next two years, respondents most often named issues that are inextricably linked in the current period: *global financial crisis* (48%) and *global pandemics* (42%).

The changed environment due to the pandemic has raised the importance of effectively managing a number of key issues, especially nonfinancial risks:

- **Operational resilience** plans received a real-life stress test as financial institutions suddenly instructed their employees to work from home.
- **Cybersecurity** has been a growing problem in recent years and has increased further in the COVID-19 period with employees working on devices that sit outside their institution's firewall and being more subject to cyberattacks.

- **Conduct and compliance** risk may increase since conversations with customers may not be subject to the same level of controls, such as the application of artificial intelligence (AI) and natural language processing technologies, which are designed to identify potential instances of inappropriate behavior and lack of compliance with regulatory requirements.
- **Risk-aware culture** is key to managing conduct risk, but this becomes more difficult if employees are working remotely. Institutions should consider how they can create a sense of community and engender their culture and values as they hire new employees, who have never met their colleagues in person either in the office or in social settings.
- **Innovation** is another concern. Will institutions be able to keep pace with innovation while working virtually for an extended period? Institutions may need to explore new approaches, such as virtual innovation labs, recognizing that these may be more difficult, especially at the outset, and may require different skills.
- **Environment (including climate), social, and governance risk (ESG)** became more prominent in 2020, with widespread demonstrations in favor of increased racial justice and equity and greater attention to the broader social responsibilities of business.

COVID-19 has also had direct financial impacts on financial institutions. The economic contraction significantly increased credit risk from both retail and commercial customers, and many institutions responded by tightening credit standards. In

addition, there may be greater potential for fraud such as from misuse of customer data, invoicing for work not completed, or collusion with disreputable third parties.

The pressure on revenues is likely to intensify the drive at many institutions to reduce ever-increasing expenditures on risk management. One promising approach is leveraging emerging technologies—such as cognitive analytics, robotic process automation (RPA), machine learning, natural language processing, and digital tools—to cut expenses by automating manual tasks. But the benefits of so-called “digital risk management” go far beyond cost reduction to enhancing risk management effectiveness by reducing errors, improving controls, and identifying potential risk events in real time so that preventive action can be taken, among other benefits.

One challenge for many institutions in implementing digital risk management is a lack of the comprehensive, timely, and high-quality risk data these technologies require. The data challenges have only grown in the COVID-19 period, with more data being generated from more sources than before as employees work remotely.

Deloitte’s *Global risk management survey, 12th edition* is the latest edition in this ongoing survey series that assesses the industry’s risk management practices and the challenges it faces. The survey was conducted from March to September 2020 and was completed by 57 financial institutions around the world that operate in a range of financial sectors and with aggregate assets of \$27.2 trillion.

“The infrastructure works, so you can work from home. But the behavior, of course, is very different if everyone sits at home—you don’t see anyone, and you can only communicate online. It’s a whole different atmosphere. How do you work together as colleagues? How do you stay effective? How do you ensure sufficient accountability? How do you innovate and start new projects when everyone is at home? I think that’s far more difficult.”

— Integrated Risk Manager, Major diversified financial services company

Key findings

Increasing credit risk. Concerns over credit risk typically peak during economic contractions and, not surprisingly, 20% of respondents named credit risk as the risk type that will increase the most in importance for their institutions over the next two years, more than for any other risk type, compared with only 3% in 2018. Sixty-two percent of respondents said that *credit risk measurement* will be an extremely or very high priority for their institutions over the next two years with this being further iterated during the interviews. Respondents said that many areas of credit risk management will be extremely or very challenging for their institutions over the next two years, including *collateral valuation* (48%), *commercial credit* (48%), *commercial real estate* (43%), *unsecured credit* (43%), and *leveraged lending* (41%).

More focus on nonfinancial risks. Institutions have recognized that nonfinancial risk types can have wide-ranging financial and reputation impacts. While almost all respondents rated their institutions as extremely or very effective at managing financial risks, the figure dropped to 65% for *nonfinancial risk* overall and was even lower for specific types and aspects of nonfinancial risk such as *conduct and culture* (55%), *geopolitical* (42%), and *data quality* (26%). Forty-four percent of institutions reported having a single individual who is accountable for oversight of the general category of nonfinancial risk. Many institutions have worked to do to enhance their capabilities in this area. No more than one-third of respondents said that several methodologies for managing nonfinancial risk are extremely or very well developed at their institutions, including *causal event analysis* (33%), *scenario analysis* (25%), *risk and capital modeling* (25%), *scorecards* (23%), and *external loss event data/database* (21%). None of the respondents rated their institutions even this highly when it came to *use of alternative data such as unstructured data*.

Continuing concerns over cybersecurity.

Institutions have faced cyberattacks for a number of years, but the threat has only grown with many employees working at home due to COVID-19. Thirty percent of respondents named *cybersecurity* as one of the three risks that would increase the most in importance for their institutions over the next two years, the second most highly rated risk. Only 61% of respondents considered their institutions to be extremely or very effective at managing cybersecurity risk, and 87% said that improving their ability to manage cybersecurity risk will be an extremely or very high priority over the next two years. Respondents most often considered *staying ahead of changing business needs* (e.g., social, mobile, analytics) (67%) to be extremely or very challenging in managing cybersecurity risk, which may be due to the changes in working practices, the business environment, and consumer behavior in 2020. There has also been keen competition for talent across all industries in this area, and 57% of respondents said that *hiring or acquiring skilled cybersecurity talent* is extremely or very challenging.

Addressing risk from third parties. Third-party relationships present a distinctive set of risks including data privacy, nonperformance, unethical conduct, and the loss of business continuity, and have received increased attention from regulatory authorities. Only 44% of respondents rated their institutions as extremely or very effective in managing *third-party risk*, placing it 30th out of 33 risk types assessed. Not surprisingly, 64% of respondents said improving management of risks from third parties will be an extremely or very high priority over the next two years for their institutions.

Spotlight on environment, social, and governance risk. With growing concern over climate risk and increasing attention to the social responsibility of business, ESG concerns—including climate change—are receiving greater attention from financial institutions. ESG was named by 38% of respondents as being one of the

three risk types that will increase the most in importance for their institutions over the next two years, more than for any other risk type. Yet, only 33% of respondents considered their institutions to be extremely or very effective at managing this risk. Consistent with this result, 47% of respondents said it will be an extremely or very high priority for their institutions to improve their ability to manage ESG risk. Institutions will need to monitor carefully how expectations regarding ESG evolve among regulators, investors, and customers.

The potential for digital risk management.

There has been increasing recognition of the potential to leverage AI and digital technologies to reduce risk management expenses while simultaneously boosting effectiveness. Fifty% of respondents reported that *efficiency tools* (such as RPA, cognitive intelligence, AI/machine learning) will be an extremely or very high priority for their institutions over the next two years. Yet, despite their expected benefits, most institutions have not yet implemented these technologies. *Cloud computing* (46%) was used most often, with fewer institutions saying they use RPA (29%), *machine learning* (27%), or *cognitive analytics* (13%).

Substantial challenges in risk data

management. Leveraging emerging technologies requires comprehensive, high-quality, and timely risk data. But many institutions continue to face challenges in achieving this, especially for nonfinancial risks. In this regard, most respondents said their institutions found two issues to be extremely or very challenging: *maintaining reliable data to quantify nonfinancial risk and drive risk-based decisions* (74%) and *ability to leverage and source alternative data such as unstructured data* (74%). Notwithstanding the fact that the Basel Committee's principles for effective risk data aggregation and risk reporting (BCBS 239) were issued in 2013, 49% of respondents said they are extremely or very concerned about *risk data quality and*

management in their institutions' risk management information technology systems.

"The impact of climate change is a top 10 risk, both on us as an organization and on our clients as well."

— Head of Risk Management, Large diversified financial services company

Clarifying the three lines of defense model.

All the institutions surveyed reported using the three lines of defense risk governance model, but many reported significant challenges. The challenges cited most often concerned the responsibilities and capabilities of the first line, such as *getting buy-in from line 1* (business and functions) (58%), *defining the roles and responsibilities between line 1* (business and functions) *and line 2* (risk management) (53%), *executing first-line responsibilities* (42%), and *having sufficient skilled personnel in line 1* (39%). The business units and functions in line 1 should own the risks they assume and have responsibility for enterprise control testing, yet only 33% of respondents said this is *embedded within business-unit first line of defense*, and only 34% of respondents said that line 1 handles internal controls quality assurance.

Greater focus on stress testing. Large majorities of respondents reported that their institutions employed stress tests for capital (83%) and for financial risks such as related to liquidity (92%), market (81%), and credit (77%). However, regulators are now expanding stress tests to include nonfinancial risks, such as climate, and only 38% of institutions reported conducting stress tests for nonfinancial/operations risk.

Continued progress on risk governance.

At the level of the board of directors, 72% of respondents said that one or more board committees are responsible for risk oversight, which is a sign of progress in effective governance. Eighty-seven% of institutions reported that their

board risk committees have independent directors, and 82% said these committees have one or more identified risk management experts.

Universal adoption of the chief risk officer (CRO) position. The percentage of institutions with a CRO position or equivalent has increased over the course of Deloitte’s global risk management surveys, and all the institutions participating in the current survey reported having this position. Although the CRO is the highest level of management responsible for risk management at 70% of institutions, 21% named the CEO. In

addition, the CRO is not always given the appropriate authority to effect change. Seventy% of respondents said the CRO reports to the CEO, although one might have expected this to be virtually universal, and 53% named the board of directors. Although 63% of respondents said a responsibility of their boards of directors is to *conduct executive sessions with the CRO*, the remaining institutions could benefit from adopting this practice.

“We understand that to serve clients and serve those relationships, we need a much stronger, more digital experience. Like virtually all major insurers, we are trying to drive toward a more accelerated underwriting approach that’s reliant on a broader set of data, so the decisions can be made in minutes, not weeks.”

— *VP Enterprise Risk Management, Major life insurance company*

Introduction

The COVID-19 era

Economic environment

In 2020, the COVID-19 global pandemic caused far-reaching economic and social impacts. There were already concerns about the economic outlook at the beginning of 2020, but it's safe to say that no one anticipated a severe worldwide downturn triggered by a global pandemic.

In its October 2020 *World Economic Outlook*, the International Monetary Fund predicted that world economic activity would decline by 4.4% in 2020 after growth of 2.8% in 2019.¹ The contraction was expected to be even greater in some major economic centers. GDP was predicted to contract by 4.3% in the United States, 8.3% in the Euro area, 9.8% in the United Kingdom, and 5.3% in Japan. Economic growth in China was projected to remain positive in 2020 at 1.9%, down from 6.1% in 2019.

Governments and monetary authorities responded to the downturn triggered by COVID-19 with a variety of initiatives designed to stimulate the economy and stabilize financial markets.

In the second half of 2020, the world experienced a K-shaped recovery, with some sectors and countries posting rapid growth, while others continued to experience flat or negative growth. Some economic sectors were especially hard hit, including travel and tourism, hospitality, and commercial real estate. Others, like technology, have seen their revenues increase as businesses and consumers relied more heavily on digital tools. Similarly, some economies appeared to be recovering more quickly, with the United States and China reporting strong growth in the third quarter.

Concerns over the global economy led to a flight to safety for investors, with the 10-year US Treasury yield dropping from 1.9% at the beginning of 2020 to a yield of 0.7% on October 2, 2020.²

Although the future course of COVID-19 is the principal uncertainty clouding the economic outlook for 2021 and beyond, there are others as well. There remains significant geopolitical risk due to the ongoing US-China trade tension. For institutions operating in Europe, the end of the Brexit transition period will have important impacts. Beginning in 2021, UK-based firms will no longer have the automatic right to sell their financial services across the EU.³

“We expect to see more stress come through next year as the true impact of the downturn really starts to hit our business.”

— Chief Risk Officer, Major diversified financial services firm

Regulatory response

As of the beginning of 2020, the period of regulatory reform resulting from the global financial crisis in 2008 was drawing to its end, and regulators were focused on implementing the final elements. Given the economic downturn and market volatility caused by COVID-19, however, regulators have postponed the implementation of various requirements.

On April 16, 2020, the European Central Bank announced a temporary reduction in capital requirements for market risk by allowing banks to

reduce the qualitative market risk multiplier.⁴ The International Association of Insurance Supervisors (IAIS) delayed the deadline for submitting data for its review of the insurance capital standard. The Basel Committee announced it would delay the implementation of the final phase of the Basel III rules for one year. Some banking authorities have gone further, with the US and Swiss authorities allowing banks to exclude sovereign bond exposures from their leverage ratios.⁵

As the pandemic continues, the focus of regulators is expected to shift from quickly responding to the crisis to ensuring the medium-term resilience of financial institutions, including recovery and resolution planning, capital management, and stress testing.

The new environment for risk management

Financial institutions should remain vigilant and proactively monitor how the ongoing COVID-19

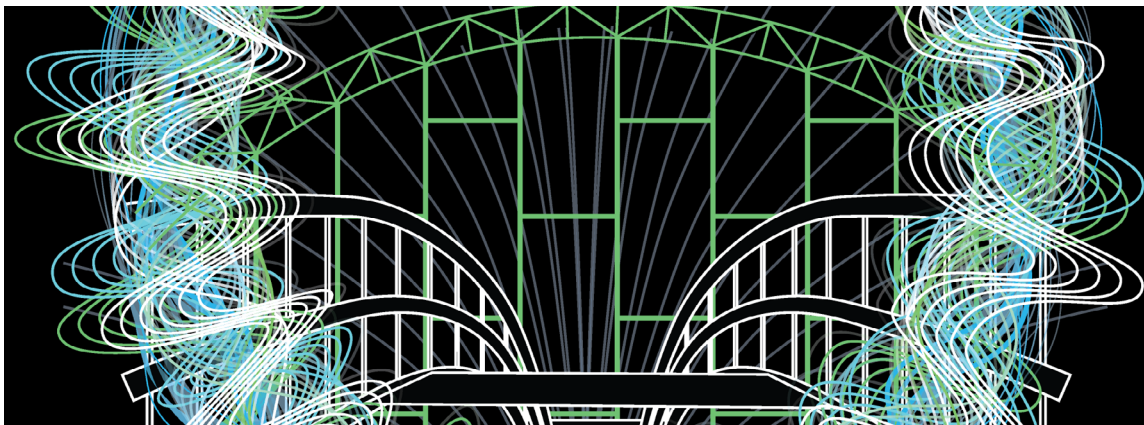
pandemic is impacting both the size and nature of a range of financial and nonfinancial risks. The rapid economic downturn, coupled with abrupt changes in consumer and business behavior, may mean that models based on pre-COVID-19 data may no longer accurately reflect the post-COVID-19 reality.

With COVID-19 case numbers continuing to rise rapidly in many countries around the world at the end of 2020, the prognosis for when companies and economies would be able to return to a semblance of normality remains unclear. The extended duration of the crisis has blurred the lines between “business-as-usual” risk management and crisis management. Coming a decade after the global financial crisis, the COVID-19 pandemic has raised the question of whether severe disruptions often described as “once-in-a-lifetime” events are now destined to recur every decade or so.

“One of my biggest issues has actually been getting my people to work less hard. We’ve provided an enormous amount of focus on people’s mental health and people’s physical health, you know, ergonomics. Making sure we’re providing them with a working environment from home where they can be safe and productive while ensuring they don’t burn out.”

— *Chief Risk Officer, Property and casualty insurance company*

About the survey



THIS REPORT PRESENTS findings from the 12th 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 57 financial services institutions around the world and was conducted from March to September 2020.

The survey gathered the views of CROs or their equivalents at 57 financial services institutions around the world representing a total of US\$27.2 trillion in aggregate assets.

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 67% having operations outside their home country.

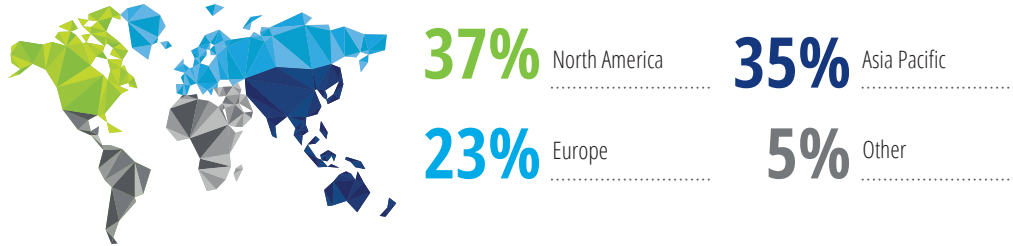
The participating institutions most often described themselves as diversified financial institutions (44%) that provide a range of services, while smaller percentages said their principal business was insurance (19%), banking (16%), or investment management (9%) (figure 2). When asked which financial services they provide, substantial percentages of the participating institutions reported offering investment management (53%), banking (51%), and insurance (33%) services (figure 2).

The institutions surveyed have total combined assets of US\$27.2 trillion and represent a range of asset sizes (figure 3). Institutions that provide asset management services have a total of US\$16.1 trillion in assets under management.

FIGURE 1

The institutions participating in the global risk management survey represent the major economic regions of the world

Participants by headquarters

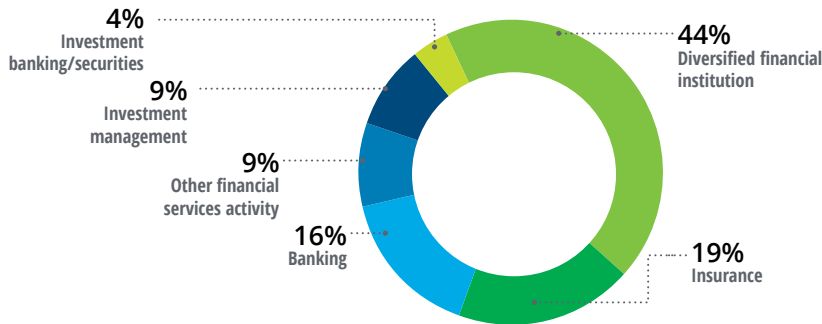


Source: Deloitte Global Risk Management Survey, 12th ed.

FIGURE 2

Participants by primary business

Participants by financial services provided

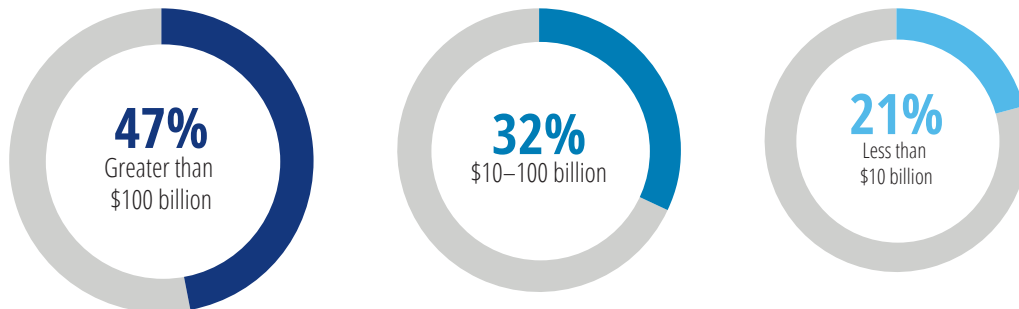


Note: Percentages may not total to 100 due to rounding.
Source: Deloitte Global Risk Management Survey, 12th ed.

FIGURE 3

The institutions surveyed represent a range of asset sizes

Participants by asset size



Source: Deloitte Global Risk Management Survey, 12th ed.

Risk management governance

Role of the board of directors

The central role of the board of directors in exercising effective oversight of risk management has been a focus of attention from regulatory authorities around the world. There have been a variety of regulatory initiatives focused on corporate governance in general and in particular on the role and responsibilities of the board of directors. Institutions that operate in multiple jurisdictions will need to keep abreast of these developments and the implications of differences in the regulatory approaches adopted in each locality.

Eighty-two percent of respondents reported that their boards of directors are spending more time on risk management compared with two years ago, including 27% who said they are spending *considerably* more time.

The survey identified notable observations in board risk oversight responsibilities and reporting (figure 4).

- **Conduct risk and risk culture.** Managing conduct risk and creating a risk-aware culture have become areas of greater focus by regulators, and 70% of institutions reported that a board responsibility is to *help establish and embed the risk culture of the enterprise and promote open discussions regarding risk*. Yet, only 54% of institutions said that *monitor conduct risk* was a board responsibility, and 44% *cited review incentive compensation plans to consider alignment of risks with rewards*.
- **Operational resilience.** All institutions said that *operational resilience monitoring and conduct and culture monitoring* are included in

their periodic board-level risk management reporting packages (figure 5). Monitoring operational resilience has increased in importance during the COVID-19 crisis.

- **Environmental, social, and governance issues.** Forty percent of institutions said that *ESG updates* (including climate) are included in risk reports to the board; it is likely that this figure will grow over time.

BOARD RISK COMMITTEES

It has become a preferred practice for the full board of directors to delegate the primary responsibility for oversight of risk management to a board risk committee. However, this was the case at only 58% of institutions participating in the survey.

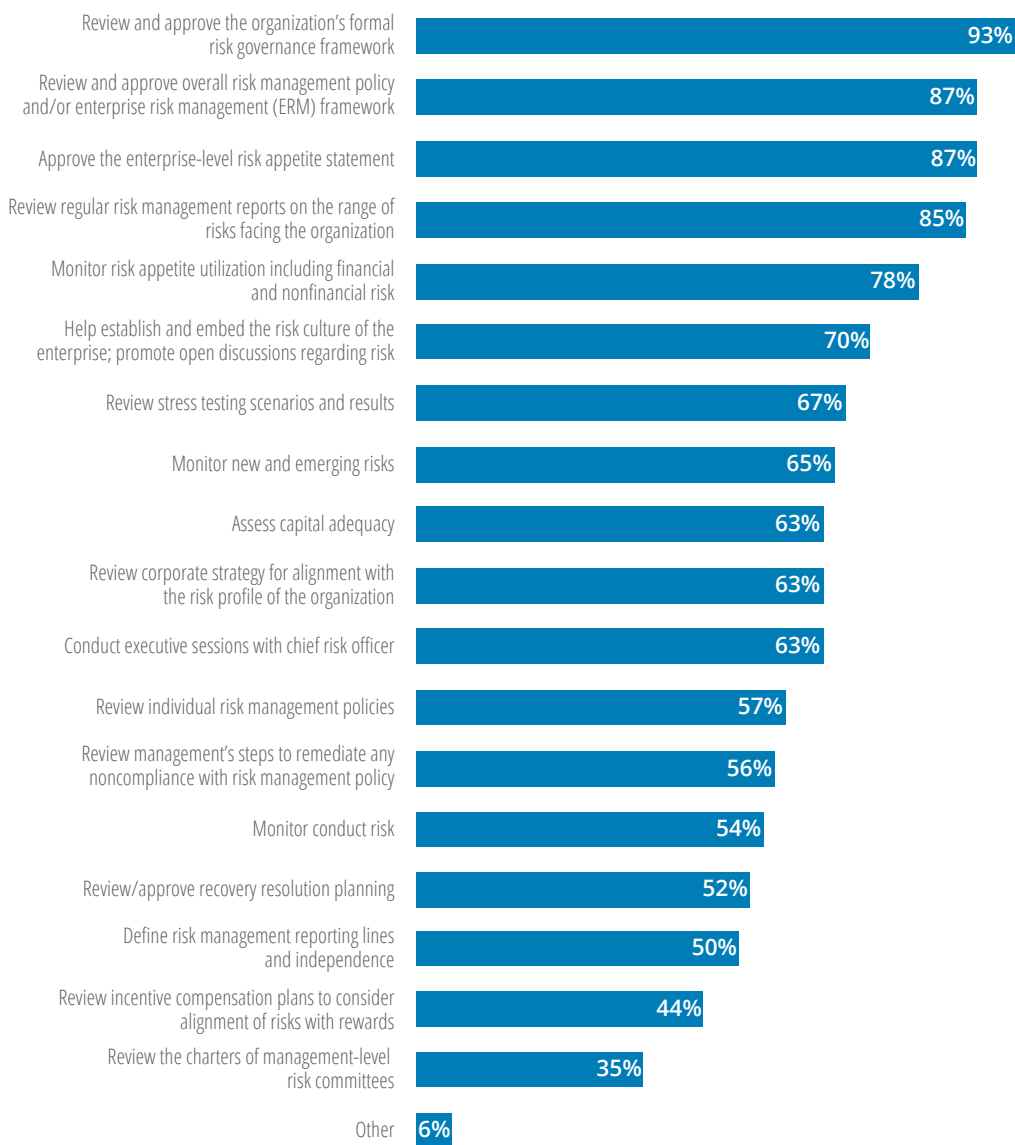
Regulatory authorities also expect risk committees to include independent directors who possess risk management expertise and skills. Eighty-nine percent of respondents said the risk committee of their boards has independent directors, with 32% saying the risk committee is composed entirely of independent directors and 37% saying that a majority of its members are independent directors. An independent director chairs the board risk committee at 86% of institutions.

Having one or more risk management experts as members of the risk committee is becoming a regulatory expectation, which can pose challenges for institutions to identify individuals with appropriate expertise. While 82% of respondents reported that they have one or more identified experts on the board committees overseeing risk management, the remaining institutions could benefit by also following this practice.

FIGURE 4

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

Base: Institutions at which risk management oversight is a board responsibility

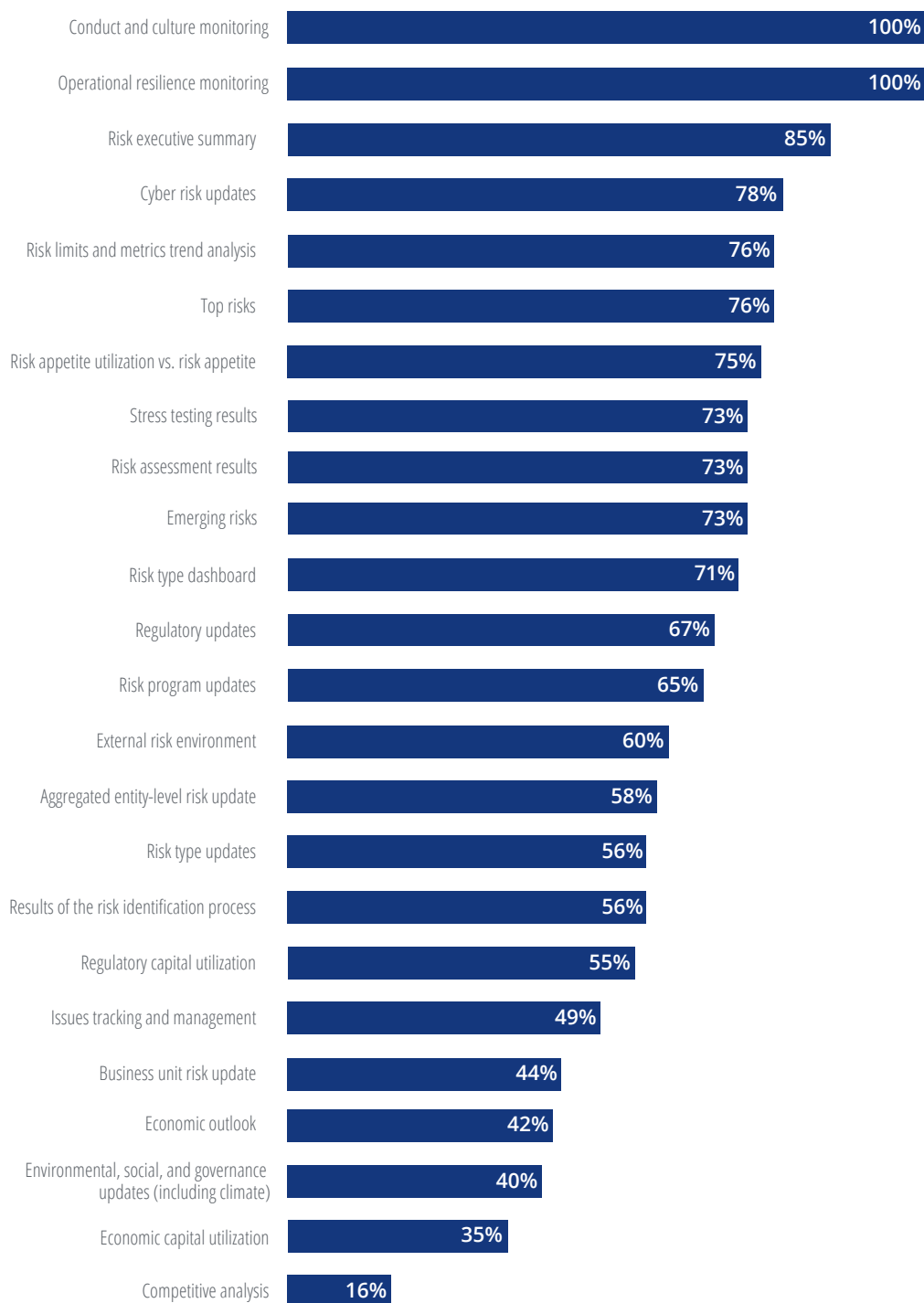


Note: Percentages total to more than 100% because respondents could make multiple selections.
 Source: Deloitte Global Risk Management Survey, 12th ed.

FIGURE 5

Topics addressed in periodic board-level risk management reporting package

Base: Institutions with periodic risk management reporting to the board



Note: Percentages total to more than 100% because respondents could make multiple selections.
Source: Deloitte Global Risk Management Survey, 12th ed.

Role of the CRO

Over the course of Deloitte’s global risk management surveys, there has been continual progress toward meeting the regulatory expectation that institutions have a CRO. For the first time in our survey series, all the institutions participating said they have a CRO or an equivalent position (figure 6).

The CRO was reported to be the highest level of management responsible for the risk management program at 70% of institutions, while 21% of institutions placed this responsibility with the CEO.

There are benefits in having the CRO report both to the CEO as well as the board of directors. Reporting directly to the CEO indicates the seniority of the CRO position, and reporting to the board of directors provides the board with an independent assessment of the organization’s risk management program and any issues it faces. However, these reporting relationships are not always in place.

Seventy percent of institutions said the CRO reports to the CEO. In addition, only 53% of respondents said the CRO reports to the board of directors or a board-level committee,⁷ and 63% said that *conducting executive sessions with the*

CRO is a board responsibility. These results suggest that many institutions may be considering strengthening the position by elevating the CRO’s reporting relationships.

As the CRO works closely with other C-suite executives to help them address the risks in their areas of responsibility, a strong level of mutual trust is key to success.

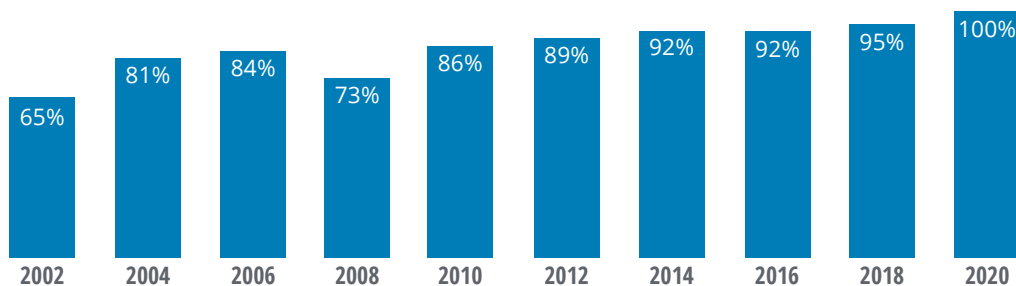
Responsibilities of the independent risk management function

There has been a trend for institutions to allocate more resources to risk management. Forty-five percent of respondents expected their institutions’ annual spending on risk management would increase over the next two years, likely in response to the additional risks engendered by COVID-19. Over time, however, there is likely to be pressure to constrain risk management budgets.

A wide range of responsibilities is assigned to the risk management function at most institutions. Notably, 75% of institutions said that *operational resilience monitoring*, is a responsibility of the risk management group.

FIGURE 6

Organizations with a chief risk officer or equivalent position



Source: Deloitte Global Risk Management Survey, 12th ed.

Striking the appropriate balance between centralization and decentralization

Institutions need to decide to what extent risk management activities should be centralized across the organization, and to what extent they should be decentralized to individual business units, functions, and geographies. They also need to decide how to strike an appropriate balance for each of their specific risk management activities.

Respondents were asked whether the business units and functions at their institutions have their own risk management functions led by business unit/functional CROs, or do they instead rely on an enterprise-wide function. Business units have had an independent risk management group embedded for a longer time than functions, and this was reflected in 40% of institutions reporting that business units have their own independent risk management group compared with 26% for functions.

Regulators have encouraged institutions to establish independent risk management groups at business units and more recently to extend this practice to their functions. Over time, we would expect more institutions, especially larger institutions, to follow this approach at their business units and functions.

Among institutions that do have independent risk management groups within their business units or functions (or both), there was no consensus on their reporting relationships. Forty-six percent said the business unit/functional CRO reports with a *solid line to the overall corporate CRO* (sometimes with a dotted line to the business unit or functional head). Other institutions have adopted a more decentralized model, with 54% saying their CROs report with a *solid line to the business unit/functional head* (sometimes with a dotted line to

the overall corporate CRO). Over time, a better practice to migrate toward would be to have risk management groups in business units and functions strengthen their reporting to the corporate CRO, since this enhances independence.

Business units have had an independent risk management group embedded for a longer time than functions, and this was reflected in 40% of institutions reporting that business units have their own independent risk management group compared with 26% for functions.

Institutions also face the decision whether to centralize responsibility across the organization for each risk type (or “stripe”) or instead take a more decentralized approach. Almost all institutions reported having a single individual responsible for cybersecurity (91%), information security (89%), liquidity (87%), regulatory/compliance (87%), market (85%), and asset liability management (84%) (figure 7).

Third-party risk has received recent attention from the regulators, and 58% of institutions reported having a single individual responsible for risk oversight in this area. Regulators have also been addressing conduct and culture, and 50% of institutions reported having a single individual responsible, up from 33% in 2018.

The results for two new risk stripes are notable. ESG has become a greater concern of both regulators and business executives recently, as highlighted both during the interviews and in the survey with 52% of

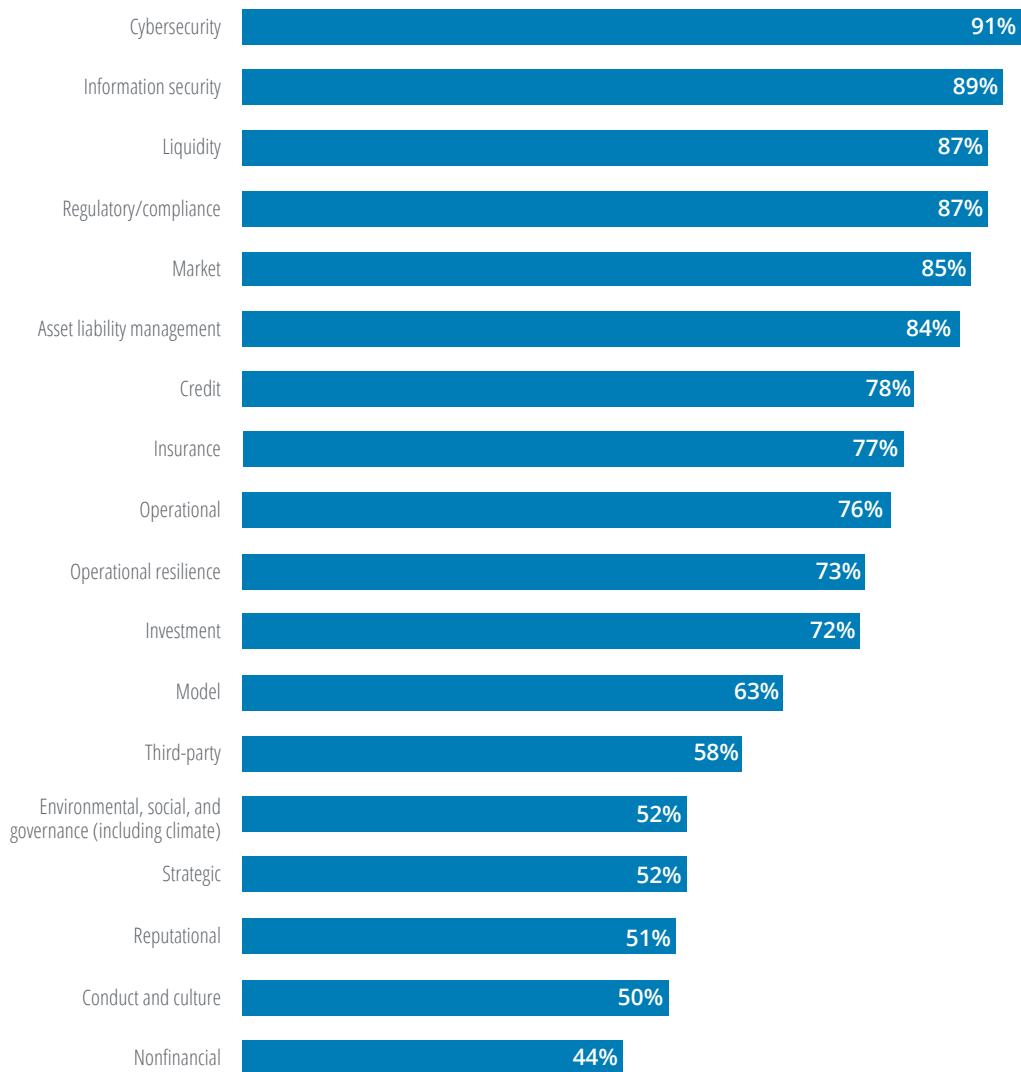
institutions already reporting that a single individual is accountable for risk oversight in this area. Nonfinancial risk is a broad risk category that encompasses specific risk types such as conduct, cybersecurity, third party, and others, and has

become a topic for regulators, especially in Europe. Forty-four percent of institutions reported that a single individual is accountable for oversight of this category across the enterprise. (See the section *Nonfinancial risk* below.)

FIGURE 7

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

Percentage responding “yes”



Source: Deloitte Global Risk Management Survey, 12th ed.

Enterprise risk management

An enterprisewide risk management (ERM) program has as its goal to put in place policies and procedures designed to identify and manage risks facing the institution. An ERM program helps to assess dependencies among the risks identified in different businesses and geographies, create consistency between the organization’s risk utilization and its risk appetite, and assign clear responsibility for managing each risk.

Eighty-four percent of the institutions reported having an ERM program in place, similar to the percentage in the previous edition of the Global Risk Management Survey, with an additional 11% saying that they are currently implementing one (figure 8). When respondents were asked to rate the overall effectiveness of risk management, 75% considered their institution to be extremely or very effective.

Although having an explicit ERM framework and policy has become an accepted practice, it is far from universal. Seventy-four percent of respondents reported that their institutions have an ERM framework or policy approved by their boards of directors or an appropriate board committee. Although it is important to have a written ERM framework, it is preferable that it be approved by the board or a board risk committee.

Among institutions that have an ERM program in place or are currently implementing one, 96% reported that they have an ERM organizational unit. Among these institutions, however, only 67% said their ERM units have substantial risk oversight and risk management responsibilities for the overall organization. Institutions where the ERM unit has either only limited oversight and management responsibility or none at all could benefit from expanding its authority.

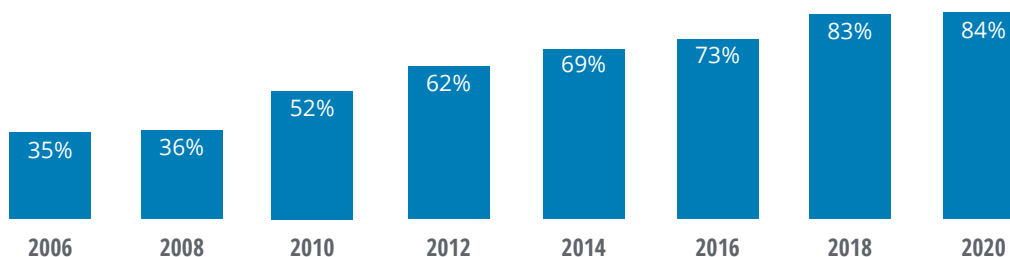
On several issues, many institutions should consider expanding the level of interaction between risk management and other functional areas, one such area being financial crime. Relatively few respondents said that there is an extremely or very high level of interaction with other functional areas on *financial crime* (54%); *strategy* (46%); or the emerging issue of *ESG* (32%).

In the current volatile environment, institutions should recalibrate their risk management programs as they apply the lessons they have learned. Seventy-three percent of respondents said their institutions have either completed a risk management renewal/update, have one in progress, or are planning to undertake one.

FIGURE 8

Does your organization have an enterprise risk management program or equivalent?

Percentage responding “yes”



Source: Deloitte Global Risk Management Survey, 12th ed.

Risk governance and controls framework

THREE LINES OF DEFENSE RISK GOVERNANCE MODEL

The three lines of defense governance model, which details the appropriate roles in risk management of business units, functions, the risk management program, and internal audit, has long been a regulatory expectation and a prevailing practice. The three lines of defense model comprises the following components and summary roles:

- First line: Business units and functions own and manage risks
- Second line: Independent risk management provides oversight and effective challenge
- Third line: Internal audit function validates the effectiveness of the risk and control framework

While all the institutions surveyed reported using the three lines of defense risk model, many said they face significant challenges regarding the first line: *getting buy-in from line 1 (business and functions)* (58%) and *defining the roles and responsibilities between line 1 (business and functions) and line 2 (risk management)* (53%). When asked about their priorities over the next two years, 49% of respondents said an extremely or very high priority will be *transformation of the risk management operating model and providing greater assistance and coverage of the first line of defense*.

Initial client regulatory exams indicate that regulators expect that the first line will take the lead in owning and managing the risks they assume, but this has not been easy to implement. Business units and functions may not have the risk

management expertise required, and their business objectives and incentives may be focused on business outcomes rather than risk management metrics. In clearly defining the role of the first line, it is important to have the business units' and/or functions' responsibilities in managing risk clearly communicated from the top, and to provide the resources and talent required.

Business units and functions may not have the risk management expertise required, and their business objectives and incentives may be focused on business outcomes rather than risk management metrics.

Most respondents said that risk management within the business units and functions at their institutions is handled by business unit and functional management (56%).

ENTERPRISE CONTROL FRAMEWORK AND TESTING FUNCTION

An enterprisewide internal controls framework undergirds effective risk management, and 77% of respondents said their institutions have such a framework, although there was no consensus on where this was located in their organizations. In addition, 63% of respondents said that *internal controls optimization, simplification, and coordination* will be an extremely or very high priority for their institutions over the next two years.

The business units should take the lead on internal controls quality assurance, but only 34% of respondents said this was the case. Instead, respondents more often said that quality assurance is handled by *internal audit* (68%), *risk management* (50%), or *compliance* (48%).⁸ Again, internal audit and risk management may be handling what should be a first line responsibility because business units lack the required resources and expertise.

Again, internal audit and risk management may be handling what should be a first line responsibility because business units lack the required resources and expertise.

Risk appetite

The importance of a written risk appetite statement approved by the board of directors has received increased attention from global regulatory authorities. Regulators now expect risk appetite statements to include nonfinancial risks, such as cybersecurity and third-party risk, as well as difficult-to-quantify risks, such as reputational risk.

Having a board-approved risk appetite statement has become a widely accepted practice. In the current survey, 94% of respondents said their institutions have a written enterprise-level statement of risk appetite that has been approved

by the board of directors, or are in the process of developing one and seeking board approval.

Institutions most often reported that their risk appetite statements and limits address risks at the *corporate/enterprisewide level* (86%). Substantially fewer institutions said this is the case at other levels such as *business level* (51%), *risk stripe level* (39%), *material legal entity level* (43%), or *country/region level* (31%). Institutions, especially those with complex business portfolios, would benefit by having their risk appetite statements drill down to lower levels.

Regulators recommend that risk appetite statements contain both quantitative and qualitative statements, but only 38% of institutions reported that their statements contain a roughly equal mix.

There has been an increased focus on nonfinancial risks, especially among regulators and institutions in Europe, and the COVID-19 pandemic has only served to underscore their importance. Yet, it can be difficult to develop risk appetite statements for nonfinancial risks, which are difficult to quantify. Forty-nine percent of respondents said their institutions find it to be extremely or very challenging to define risk appetite for nonfinancial risk overall, while substantial percentages said the same about specific nonfinancial risks such as strategic (63%), cybersecurity (47%), reputational (45%), and conduct (40%) (figure 9). Many institutions will need to commit more time and effort to developing methodologies and techniques to assess their appetite for nonfinancial risks.

FIGURE 9

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

Base: Institutions with written enterprise-level statement of risk appetite
 Percentage responding “extremely or very challenging”



Source: Deloitte Global Risk Management Survey, 12th ed.

RISK IDENTIFICATION

Identifying new and emerging risks is an essential element of an effective risk management program. Since business units should have responsibility for the risks they assume, an accepted practice is for business units to perform risk identification, with the independent risk management function

structuring and providing challenge to the process. Yet, only 40% of respondents said that this is the approach at their institutions, while 38% said that risk identification is performed by the independent risk management function with input from the business units and functions.

Eighty-five percent of institutions reported conducting risk identification at least annually, with only 48% of institutions conducting risk identification quarterly or more often, which is preferable. Many institutions may benefit by conducting risk identification more frequently.

Regulatory authorities may expect at least an annual risk identification, with quarterly updates for larger financial institutions. In part, the frequency should reflect the business profile of the institution. Quarterly risk identification is recommended for larger and more complex institutions operating in more dynamic areas, while monthly risk identification may be more appropriate for those competing in especially volatile lines of business or geographies.

Asset liability management

Institutions are experienced in managing risk related to asset liability management, and 80% of respondents said their intuitions are extremely or very effective at managing this risk. The issue most often considered to be extremely or very challenging over the next two years was the *ability to model on a dynamic basis the impact on net interest income of changing interest rates and changing balance sheet* (38%). This may reflect the difficulty in modelling the impact of negative interest rates in certain locations. In addition, 33% of institutions considered *integrating the modeling of interest rate risk in the banking book (IRRBB) and credit risk within the banking book to stress scenarios* to be extremely or very challenging.

Stress testing

Financial institutions and regulators have come to rely more heavily on stress testing to assess financial resilience and allocate capital to different businesses. Most respondents reported that their institutions employ stress tests for capital (83%)

and for financial risks such as liquidity (92%), market (81%), and credit (77%). Although regulators have widened their focus to include nonfinancial risks in stress tests, only 38% of institutions reported conducting stress tests for nonfinancial/operational risk.

European regulators are also expanding the use of stress testing for macroprudential policy by developing models that take into account interfirm contagion and adverse feedback loops between the financial sector and the real economy. In addition, a number of European regulators have either undertaken or are planning to develop climate related risk stress tests.

CAPITAL STRESS TESTS

The impacts on balance sheets of the economic downturn in 2020 have underscored the importance of capital stress tests. While the use of capital stress tests was almost universal in the survey, institutions should consider whether these stress tests are sufficiently rigorous, employing well-calibrated models and high-quality data.

Among the institutions that reported using capital stress tests, respondents said they most often used stress tests extensively for *assessing the adequacy of regulatory capital* (64%), *reporting to the board* (64%), and *meeting regulatory requirements and expectations* (62%) (figure 10).

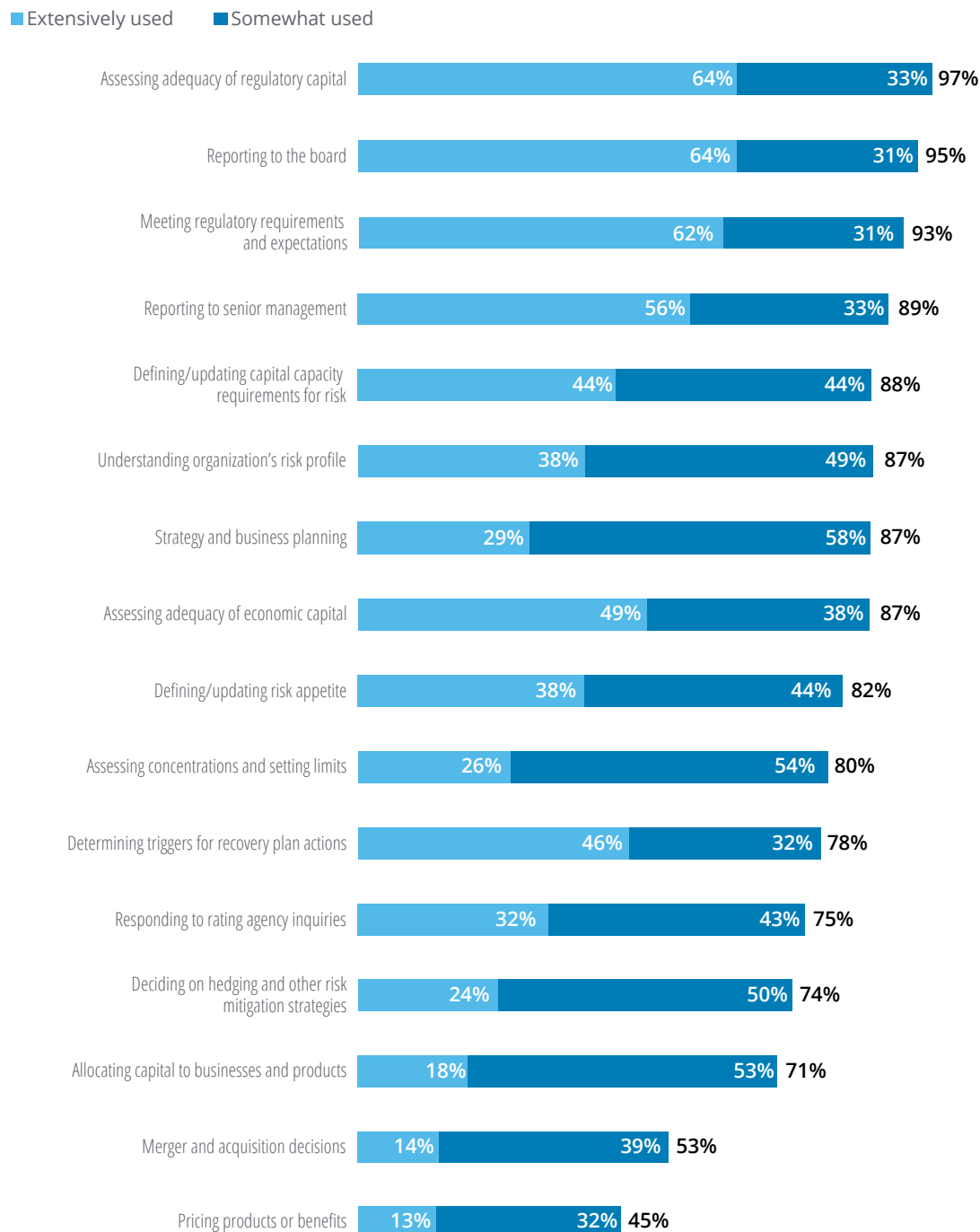
LIQUIDITY STRESS TESTS

Liquidity stress tests are also employed widely. Liquidity stress tests present special challenges such as *incorporating intraday liquidity risk into liquidity stress test assumptions*, which was considered to be extremely or very challenging by 39% of respondents (figure 11). Risk management IT systems typically calculate end-of-day balances that do not necessarily reflect the liquidity position at various times during the day. However, given the speed of financial markets, regulatory authorities are indicating that institutions need to move to continuous liquidity monitoring.

FIGURE 10

To what extent are the results of capital stress tests used by your organization for each of the following purposes?

Base: Institutions that perform capital stress tests

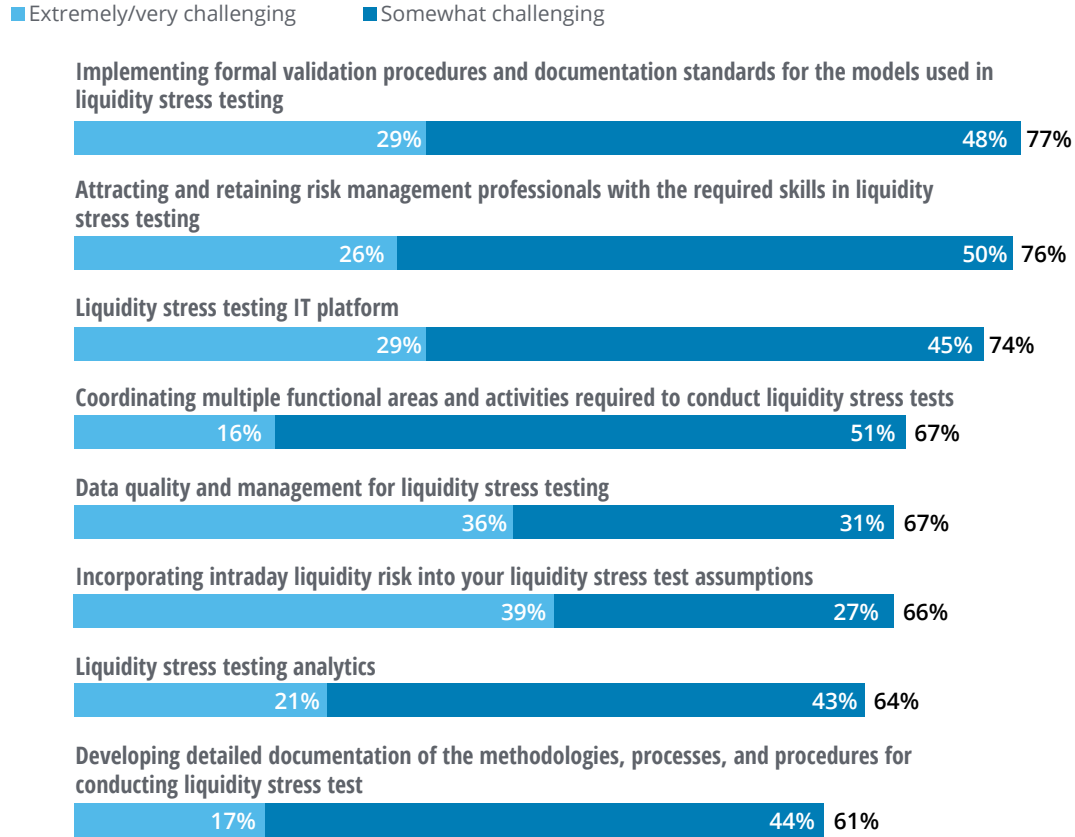


Note: Some percentages may not total due to rounding.
Source: Deloitte Global Risk Management Survey, 12th ed.

FIGURE 11

How challenging is each of the following for your organization’s use of liquidity stress testing?

Base: Institutions that perform liquidity stress tests



Source: Deloitte Global Risk Management Survey, 12th ed.

Management of individual risk types

INSTITUTIONS HAVE LONG experience in managing financial risks, such as market, credit, and liquidity, but in recent years they have increased their attention to a variety of nonfinancial risks, which can have serious impacts but are more difficult to measure and manage. Large majorities of respondents said their institutions are extremely or very effective at managing traditional financial risks such as *liquidity* (89%), *credit* (85%), and *market* (82%) (figure 12). But they gave their institutions much lower ratings when it came to nonfinancial risks overall (65%) or specific nonfinancial risks such as *operational resilience* (64%), *strategic* (55%), *geopolitical* (42%), and *ESG (including climate)* (33%). Yet, with the single

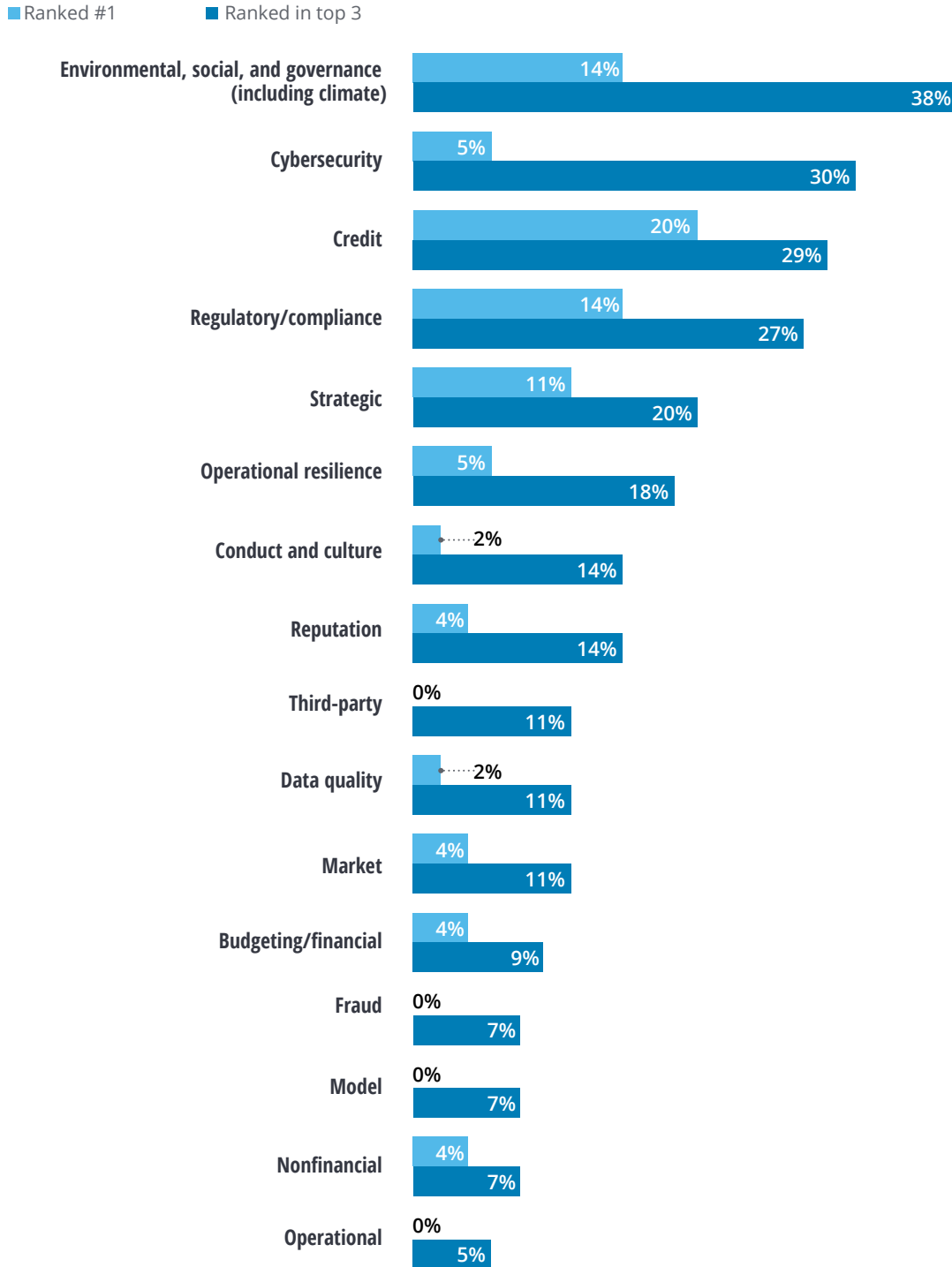
exception of credit risk, respondents most often expected nonfinancial risks to be those that increase the most in importance for their institutions.

Risk management is also confronting a series of fundamental macrotrends. The top three cited macrotrends that will increase in importance for respondents' institutions over the next two years were: *global financial crisis* (48%), *global pandemics* (42%), and *credit quality deterioration* (39%) (figure 13). *Growth of digital customer platforms and intermediaries* (38%) was also ranked by many respondents among the top three trends.

Institutions have long experience in managing financial risks, such as market, credit, and liquidity, but in recent years they have increased their attention to a variety of nonfinancial risks, which can have serious impacts but are more difficult to measure and manage.

FIGURE 12

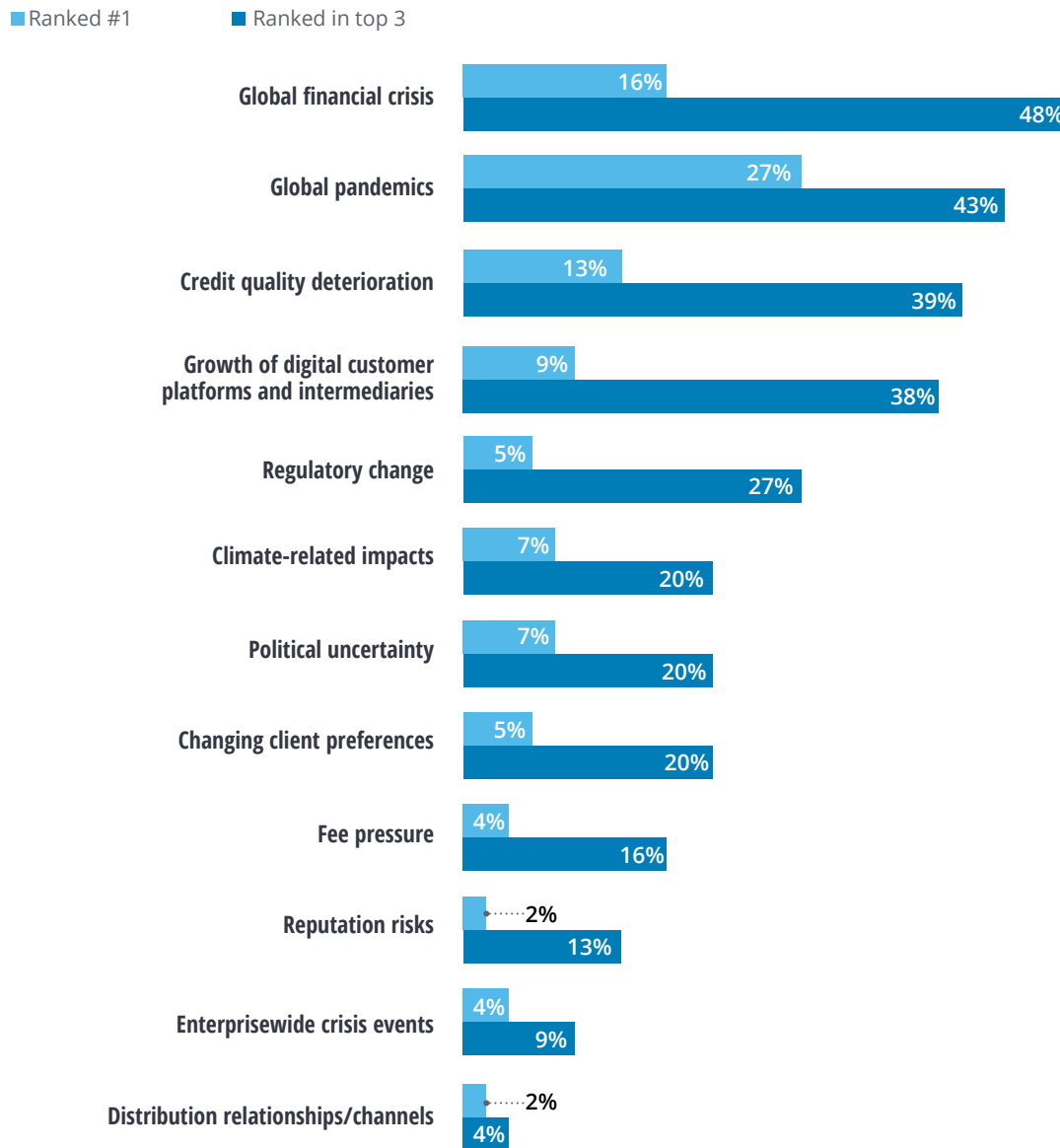
Over the next two years, which three risk types do you think will increase the most in their importance for your business?



Source: Deloitte Global Risk Management Survey, 12th ed.

FIGURE 13

Over the next two years, which three of the following emerging macrorends do you think will increase the most in their importance for your organization?



Source: Deloitte Global Risk Management Survey, 12th ed.

Financial risk

CREDIT RISK

The rapid economic contraction due to COVID-19 has led to increased attention on managing credit risk from lending to both consumers and businesses. Many institutions had already

tightened credit standards in 2019 as many economies were in the late stages of the credit cycle, and the sharp economic downturn due to COVID-19 has only heightened those concerns.

An August 2020 analysis by Fitch Ratings found that rising credit risk costs at seven major

European financial institutions due to the economic contraction caused by COVID-19 drove a 42% decline in their aggregate operating profit in the second quarter of 2020 compared with the year before, with credit costs skyrocketing by 430%.⁹

When asked to name the risks that they believed would increase the most in importance for their institutions over the next two years, respondents most often named *credit* (20%) as number one, a sharp increase from 3% in the previous edition of the Global Risk Management Survey. The increased importance of credit risk likely the result of the contraction in economic activity around the world. Among banking respondents, this figure rose to 34%. In addition, 66% of banking respondents believed that *credit quality deterioration* would be one of the three macrotrends that will increase the most in importance for their institutions over the next two years, a higher percentage than for any other trend. Seventy-seven percent of banking respondents said

that *credit risk measurement* will be an extremely or very high priority for their institutions over the next two years.

Yet, 86% of banking respondents said they believed their institutions are extremely or very effective at managing credit risk. When asked about the challenges their institutions will face over the next two years in specific areas related to credit risk, more banking respondents said several areas would be extremely or very challenging than in 2018: *collateral valuation* (48%, up from 25% in 2018), *commercial credit* (48%, up from 16%), *commercial real estate* (43%, up from 31%), *unsecured credit* (43%, up from 20%), and *leveraged lending* (41%) (figure 14).¹⁰ With commercial real estate, it is unclear to what extent employees will return to the office or whether the move to remote work will become permanent for many, reducing the demand for office space over the long term.

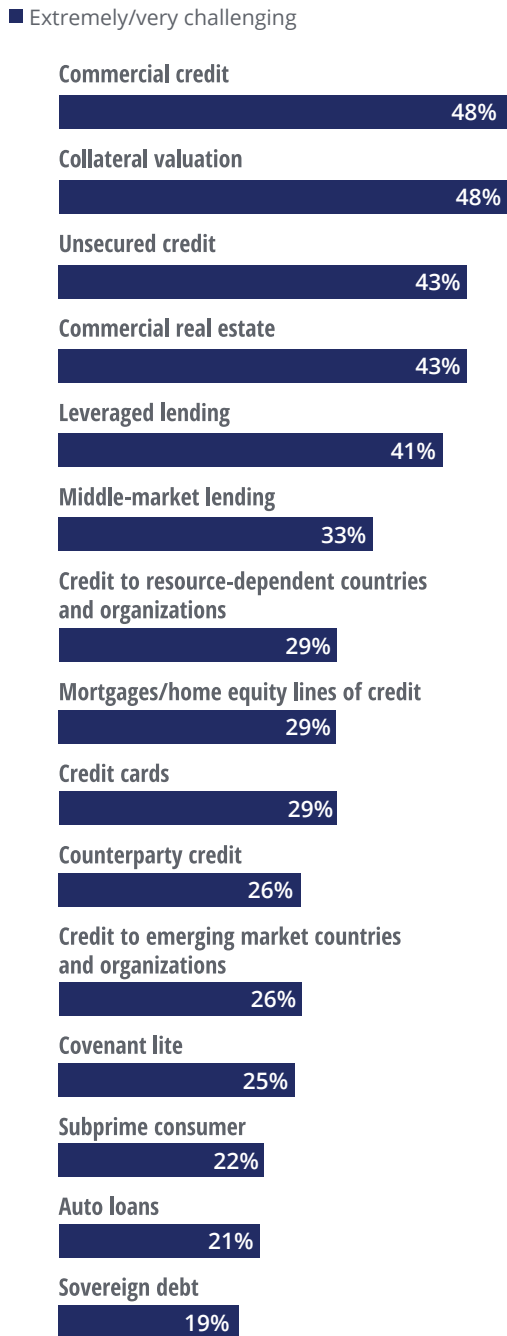
“We decided not to lend money to new customers and only maintain our existing relationships. Since then, I think we’ve added only three new customers, very high-grade credit customers and very selectively analyzed. Since March, we’ve been conducting daily monitoring of our drawdowns, daily monitoring of our customers, as well as weekly updates with regard to our positions: asset quality, potential downgrades, etc. So, credit has been monitored intensely since March.”

— Chief Risk Officer, Major global bank

FIGURE 14

Challenges in managing credit risk over the next two years

Base: Organizations that provide banking services
Percentage responding “extremely or very challenging”



Source: Deloitte Global Risk Management Survey, 12th ed.

LIQUIDITY RISK

Financial institutions should consider reviewing their procedures for managing liquidity risk in light of the recent economic contraction and volatility.¹¹ Among the issues that should be examined is whether liquidity risk management has sufficient visibility across the organization and robust reporting capabilities. If required, institutions should take steps to develop an accurate view of the projected cashflow and liquidity shortfall across entities and businesses, and determine whether changes are needed to their liquidity models and cash flow forecasts to more accurately reflect current and projected conditions given the COVID-19 crisis. Institutions should consider reviewing their collateral management procedures to assess whether they are adequate to meet the challenges of determining the value, availability, and eligibility of collateral during the ongoing pandemic.

Almost all respondents believed their institutions are extremely or very effective at managing liquidity risk (89%). Surprisingly, few respondents considered specific issues related to liquidity risk management to be challenging. For example, it is more difficult to assess an institution’s liquidity position moment by moment throughout each day, rather than at the end of the day. Yet, only 21% of respondents said that *monitoring and managing intraday liquidity risks* will be extremely or very challenging for their institution over the next two years.

Nonfinancial risk

Risk management has widened its focus in recent years to encompass a series of nonfinancial risks including cybersecurity, third-party, ESG, and conduct and culture. Regulators are requiring institutions to demonstrate the adequacy of their risk management programs to manage these and other nonfinancial risks.

Nonfinancial risk is different from other risk types, since it is an overall umbrella category comprising a variety of individual risk types. While many institutions rely on managing these risks individually, there has been a trend, especially in Europe, for institutions to focus on nonfinancial risk as an overall category and appoint a leader to oversee it across the organization. Forty-four percent of respondents said their institutions have taken this approach and have a single individual who is specifically accountable for oversight of nonfinancial risk.

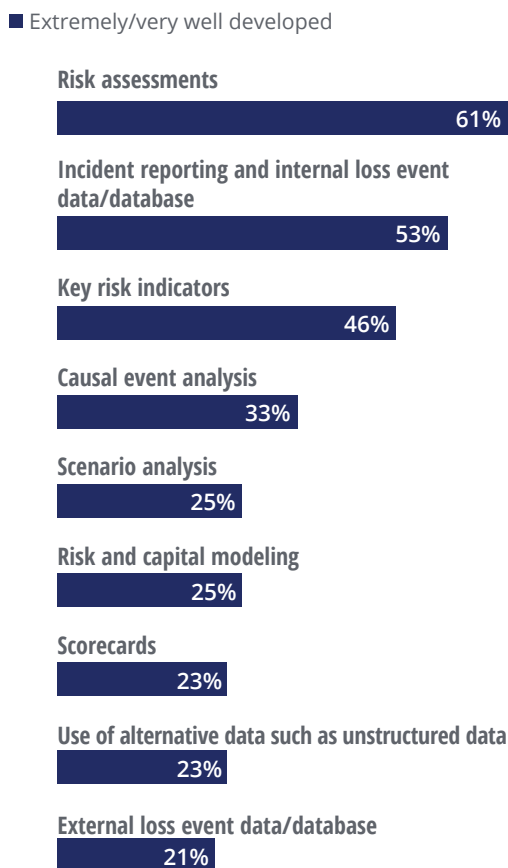
Respondents were asked for which areas their institutions have adopted a nonfinancial risk management approach. Most respondents said their institutions have either adopted, or are in the process of adopting, a nonfinancial risk management approach for a variety of areas including *risk identification* (87%), *risk taxonomy categories* (80%), *overall risk management framework* (83%), *risk reporting* (78%), *regulatory reporting* (69%), and *risk management organization structure* (74%).

Relatively few respondents considered various nonfinancial/operational risk methodologies at their institutions to be extremely or very well developed. The two methodologies that were most often rated this highly were *risk assessments* (61%) and *incident reporting and internal loss event data/database* (53%) (figure 15). Fewer respondents considered other methodologies to be extremely or very well developed at their institutions such as *scenario analysis* (25%), *risk and capital modeling* (25%), *scorecards* (23%), and *external loss event data/database* (21%). Notably, none of the respondents considered their risk methodologies to be extremely or very well developed when it came to *use of alternative data such as unstructured data*.

Most respondents said their institutions have either adopted, or are in the process of adopting, a nonfinancial risk management approach for a variety of areas.

FIGURE 15

How well developed is each of the following nonfinancial/operational risk management methodologies at your organization?



Source: Deloitte Global Risk Management Survey, 12th ed.

CYBERSECURITY

Managing cyber threats is a major priority for financial institutions, and regulatory authorities around the world continue to make cybersecurity an important focus. A 2018 International Monetary Fund (IMF) analysis of potential losses due to cyberattacks in 50 countries found that the annual losses to financial institutions could reach US\$270 billion to US\$350 billion in a severe scenario, almost half of banks' net income, and could have systemic impacts on the financial system.¹²

The threat has only grown with many employees working remotely due to COVID-19. One study found that cyberattacks against major US financial institutions increased substantially between February and April 2020.¹³ In April 2020, the New York Department of Financial Services issued new guidance in light of a significant increase in cybercrime related to the COVID-19 outbreak.¹⁴

Companies remain intensely focused on cybersecurity. Eighty-seven percent of respondents said it will be an extremely or very high priority for their institutions over the next two years to improve their ability to manage cybersecurity risks, a higher percentage than for any of the other 16 potential priorities. Only 61% of respondents believed their institutions are extremely or very effective at managing cybersecurity risk overall.

Institutions face multiple challenges in safeguarding themselves against continuously evolving cyber threats. Given the volatility in the business environment and changing consumer behavior, respondents most often considered as extremely or very challenging *staying ahead of changing*

business needs (e.g., social, mobile, analytics) (67%) (figure 16). With companies across all industries working to protect their operations against hackers and other cyber threats, there has been fierce competition for cybersecurity talent, not only with other financial services institutions but also with companies in technology and other industries. As a result, 57% of respondents said that *hiring or acquiring skilled cybersecurity talent* is extremely or very challenging.

Eighty-seven percent of respondents said it will be an extremely or very high priority for their institutions over the next two years to improve their ability to manage cybersecurity risks, a higher percentage than for any of the other 16 potential priorities.

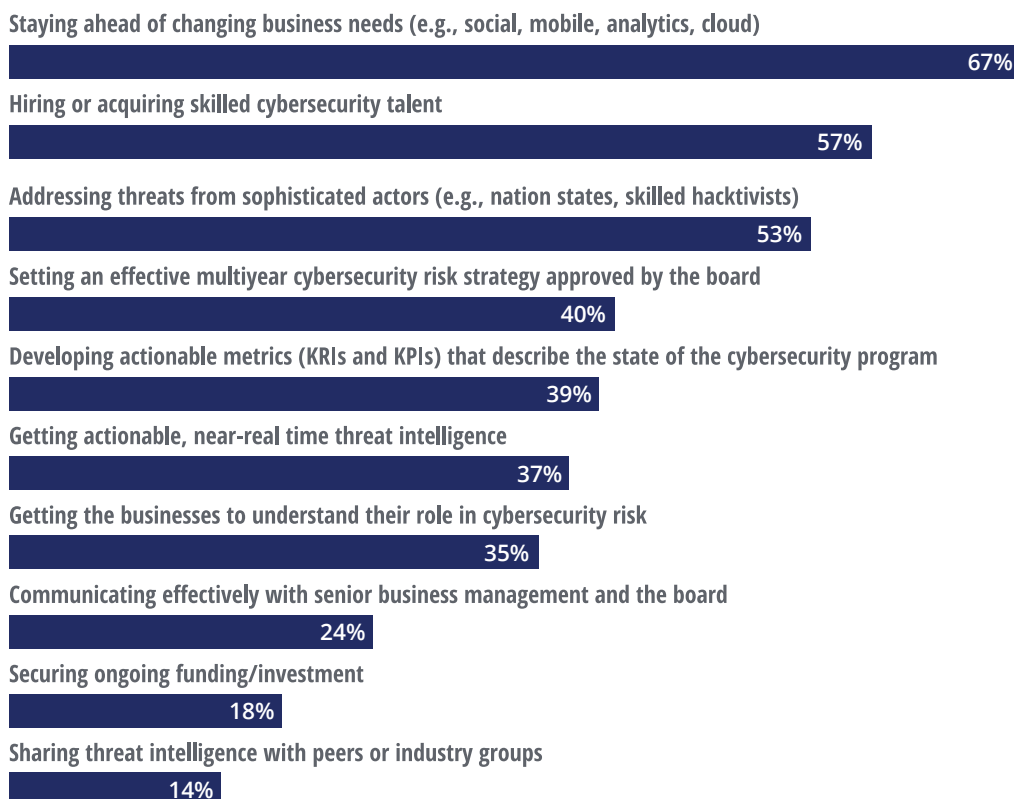
“There are a lot of online frauds, phishing, and spoofing kinds of cyber tricks to get our clients to transfer money on their cell phones. But if money goes out of their account, they will of course look at the bank. Cyber risk is also targeting the bank as all our employees are working from home. So we see a big spike in efforts to directly target the bank.”

— Integrated Risk Manager, Major diversified financial services company

FIGURE 16

In your opinion, how challenging is each of the following for your organization in managing cybersecurity risk?

■ Extremely/very challenging



Source: Deloitte Global Risk Management Survey, 12th ed.

THIRD-PARTY RISK

Effective management of third-party risk is a basic regulatory expectation, and regulators have made it clear that financial institutions remain responsible for the actions of their vendors. Third-party relationships present distinctive challenges since institutions must strive to have their vendors achieve a similar level of rigor in their risk management processes, such as in cybersecurity or operational resilience, as aimed for by the institution itself. Effectively managing third-party risk requires standardized processes that are integrated with tools and data, aligned with proactive decision-making capabilities, and supported by analytics. Formal assessments of

resiliency should include the impact of third-party relationships. An additional challenge is to gain insight into and manage the additional risk created by fourth-party relationships, when an institution's third-party service providers in turn pass some of the work to additional subcontractors.

Only 44% of respondents considered their institution to be extremely or very effective in managing risks from third-party service providers, which was 30th out of 33 risk types. Respondents most often considered their institutions to be extremely or very effective at managing *financial risk* (59%) related to third parties. Fewer respondents rated their institutions this highly when it came to other third-party risks such as *resilience*

and continuity (48%), performance and operations (46%), and reputation (43%).

Consistent with this low self-assessment, 64% of respondents said that it is an extremely or very high priority for their institution over the next two years to improve third-party risk management. Many institutions reported they had not yet established many basic aspects of a program to manage third-party risk, although more institutions said they are in progress of implementing them. For example, 67% of institutions said they had established *standard contract language and service-level agreements (SLAs)*, while an additional 22% said this is in progress (figure 17). Having standard contract language in place with SLAs and having

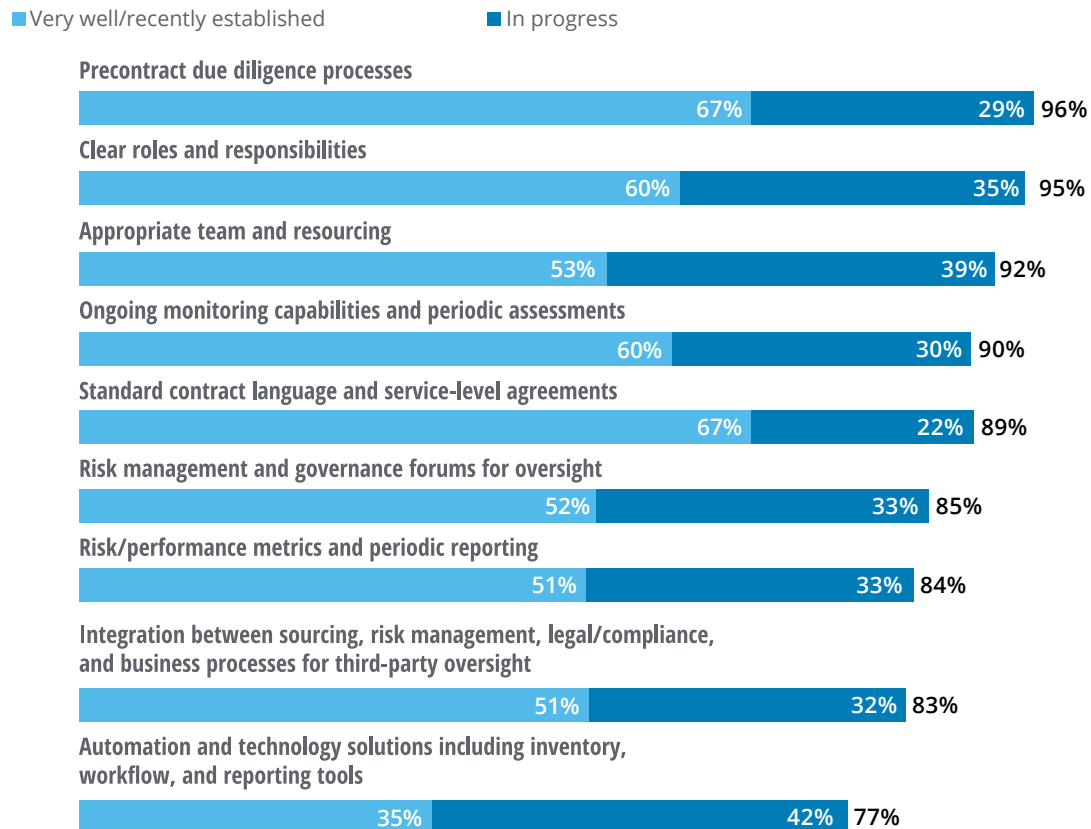
clear roles and responsibilities are foundational steps that every institution should take.

“We just had a spate of ransomware attacks against our vendor supply chain. Now we’re talking about how we can be more proactive with our vendors. Can we actively share indicators of compromise? Can we do special assessments to make sure we know what certain threat actors are doing and that our vendors are well prepared, above and beyond the annual due diligence that we do on them?”

— Chief Risk Officer, Investment management firm

FIGURE 17

When managing risk from third parties, which of the following has your organization established as part of your program?



Source: Deloitte Global Risk Management Survey, 12th ed.

REGULATORY RISK

Even more than 10 years after the global financial crisis, which triggered a blizzard of regulatory developments, financial institutions continue to face an array of evolving regulatory requirements addressing such issues as capital adequacy, data governance, cybersecurity, and third-party risk, among others. Although there have been indications that the pace of regulatory change has slowed, 94% of respondents expected that the regulatory requirements on their institutions would increase over the next two years, with 31% expecting a *significant* increase. These figures are similar to those in 2018, which may reflect the many regulatory changes that remain to be implemented fully, and indicates that the respondents did not expect the pace of regulatory change to slacken.

Given the ongoing regulatory focus on the security of IT systems and the continued threat of cyberattacks, respondents most often said they are extremely or very concerned about the impact on their institutions of supervisory or regulatory processes in the area of *cybersecurity* (54%) (figure 18). The area cited next most often was the general concern regarding *standards or regulations that will raise the cost of doing business* (49%). This concern, which may become

especially more pronounced in a period of weak economic conditions, could lead more institutions to leverage technology solutions, such as RPA and AI applications, in order to increase efficiency and reduce risk management costs.

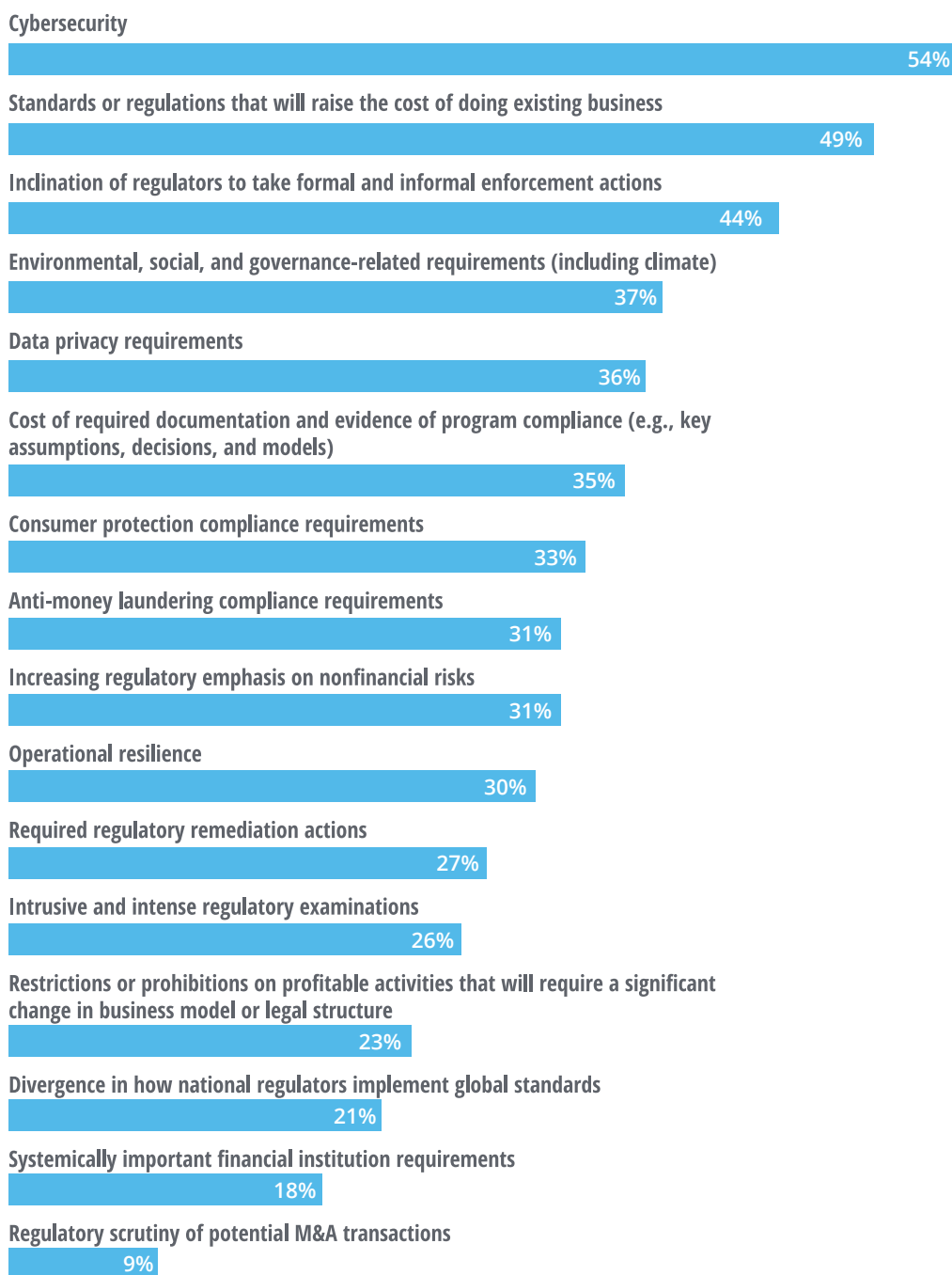
IBOR transition

Institutions are under pressure as the target date for cessation of interbank offer rates (IBORs) in new contracts (end of 2021 for most cases) approaches. While relatively few respondents expected that IBOR transition would be especially challenging, they may have underestimated the work required and would be well advised to prepare for the transition. For example, only 24% considered *technology/applications updates and development* to be extremely or very challenging, while 22% said the same about *processes and controls updates and development*. Yet, it can be challenging to identify all the systems that can make the detailed calculations that reference the London Interbank Offered Rate along with the required changes.

FIGURE 18

Over the next two years, how concerned are you about the potential impact on your organization of each of the following regarding supervisory and regulatory processes?

■ Extremely/very likely



Source: Deloitte Global Risk Management Survey, 12th ed.

ENVIRONMENT, SOCIAL, AND GOVERNANCE RISK

ESG is a nonfinancial risk type that is receiving increasing attention from institutions and their regulators. Institutions will need to become ready to meet the evolving regulatory requirements in this area. For example, the Bank of England plans to run its first stress test exercise for climate risk in 2021 as its biennial exploratory scenario.¹⁵ In October 2020, the European Insurance and Occupational Pensions Authority (EIOPA) published a consultation on the use of climate risks scenarios in the Own Risk and Solvency Assessment.¹⁶

This risk was named by 38% of respondents as being among the three risk types that would increase the most in importance for their institutions over the next two years, more than for any other risk type (figure 12). In addition, 37% of respondents were extremely or very concerned about the potential impact on their institutions of new regulatory requirements in this area. As a result, 47% of respondents said that it is an extremely or very high priority over the next two years for their institutions to improve their capabilities in managing ESG.

“Climate risk has a lot of focus in our scenario analysis to get better insights in where the sensitivities of physical and transition risks are. This gives us better insight on what it means for our climate risk strategy and climate risk management capabilities. ESG is clearly a top 5 risk priority for us.”

— Integrated Risk Manager, Major diversified financial services company

CONDUCT AND CULTURE

Managing conduct risk and establishing a risk-aware culture have become more important in recent years due to well-publicized instances of inappropriate business conduct and practices that have resulted in regulatory fines and reputational damage for prominent institutions.

Conduct risk has also received attention from the regulators. A key development was the final report of Australia’s Royal Commission into misconduct in the banking, superannuation, and financial services industry, which was released in February 2019.¹⁷ The report issued principles of good conduct for institutions and has sparked greater attention on conduct and culture among regulatory authorities in Asia Pacific and beyond. Monitoring conduct and engendering an appropriate culture have become even more difficult than before since most employees are now working remotely.

Only 55% of respondents considered their institutions to be extremely or very effective at managing *conduct and culture risk*, and 40% said it is extremely or very challenging to define and implement their risk appetite statement in this area. As a result, many respondents said that *establishing and embedding the risk culture across the enterprise* (61%) will be extremely or very high priorities for their institutions over the next two years. Among institutions that have completed or undertaken a risk management renewal program, 76% said that *focus on conduct risk and risk culture* is an extremely or very high priority of their renewal programs.

Risk management technology and data

Digital risk management

Institutions have recognized the potential of the latest technologies—such as cognitive analytics, RPA, machine learning, natural language processing, and digital tools—to drive down risk management costs. The economic downturn in 2020 triggered by COVID-19 has placed pressure on revenues and only served to strengthen the desire to increase efficiency. Fifty percent of respondents said that *efficiency tools (such as RPA, cognitive intelligence, AI/machine learning)* will be an extremely or very high priority for their institutions over the next two years.

Yet, relatively few institutions reported employing these tools currently. Respondents most often said their institutions use *cloud computing* (46%), with fewer saying they use RPA (29%), *machine learning* (27%), or *cognitive analytics* (13%) (figure 19).

While these technologies can reduce operating costs by automating manual processes, their benefits go far beyond cost reduction to offer substantial improvements in effectiveness and quality. Among many potential applications, they can be leveraged to build controls directly into processes, prioritize areas for testing and monitoring, allow all transactions to be reviewed rather than relying on sample testing, and identify potential risk events in real time to allow preventive action to be taken. By automating routine tasks, they can also free employees to work on higher-value activities.

Even as they work to capture these benefits, institutions need to manage the additional risks these

technologies can create. Failures of automated processes could have even deeper and more extensive impacts than would result from a problem in a manual process. Machine learning systems, where the application learns and makes individual decisions on its own rather than being explicitly programmed, have the potential to create inadvertent bias, rogue programs, or inaccurate results.

COVID-19 has created further challenges. With economic and business conditions having changed abruptly, machine learning models, such as fraud detection models, which had been trained on pre-COVID-19 data may have “learned” to identify data patterns and correlations that no longer accurately predict future outcomes. In many cases, institutions may have to retrain and revalidate their models.

The regulatory implications must also be addressed as new requirements and guidance are put in place. AI applications powered by machine learning can be “black boxes,” where decisions based on personal data cannot be explained. This can create issues with respect to legislative (e.g., General Data Protection Regulation [GDPR] in the European Union) and regulatory requirements. The Bank of Japan investigated the legal issues stemming from the use of black-box algorithms in investment management and concluded that existing legislation will need to be adjusted to reflect the unique nature of AI.¹⁸

Institutions will need to demonstrate to regulators and the public that their model risk management frameworks have been enhanced to be able to identify and manage these risks in their IT systems

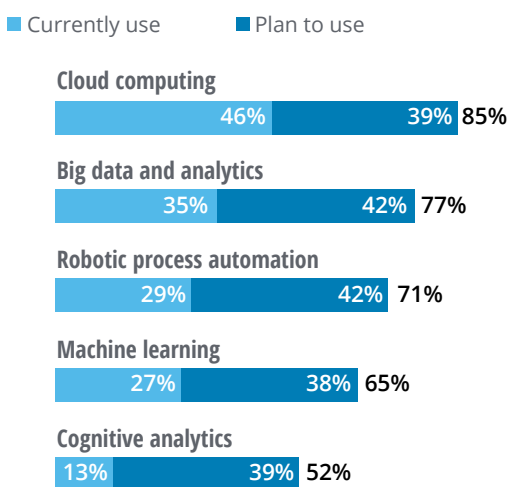
as well as broader data ethics implications. Regulators will expect institutions to establish clear risk appetite frameworks and parameters that encompass risks related to AI systems and put in place effective controls. This will be especially important for material models such as those used for risk and regulatory capital calculations or that drive consumer outcomes. Institutions will need to build teams of risk professionals across the three lines of defense with the required AI skills and experience.

“More has happened on the digital front in the first four months of COVID-19 than in the previous decade. We feel our competition is going to really accelerate here, and this is a key focus for us.”

— Chief Risk Officer, Large bank

FIGURE 19

Does your organization use or plan to use any of the following emerging technologies in the risk management function?



Source: Deloitte Global Risk Management Survey, 12th ed.

Risk IT systems and data management

To take advantage of the latest technologies requires risk data that is accurate, comprehensive, and timely. This is lacking in many institutions due to multiple legacy IT systems for different lines of business or geographic markets, often the result of a series of past acquisitions that were never fully integrated.

BCBS 239, which was released in 2013 for implementation by global systemically important banks, has provided a benchmark against which regulators around the world are measuring the adequacy of risk data programs within the financial sector more generally. While the industry has made strides, institutions will need to have in place a process of continuous improvement so they can quickly respond to increasing data requirements and maintain the comprehensive, high-quality data needed to manage risk. Some institutions are establishing central data offices led by a chief data officer (CDO), which set data quality standards, monitor data quality across the institution, and develop models for firmwide data infrastructure. Other approaches that can yield benefits including identifying the lineage (i.e., the original sources of information) of data used for reporting and decision-making, and conducting independent assessments of the risk to the institution of poor data quality to determine where enhanced controls should be applied and to prioritize data remediation efforts.

Most institutions recognize that they have more work to do to improve data management. Sixty-nine percent of respondents said that *enhancing the quality, availability, and timeliness of risk data* will be an extremely or very high priority for their institution over the next two years. Only about one-quarter of respondents believed their institutions are extremely or very effective at managing *data*

quality (26%), data management key performance and risk indicators (24%), and data standards (27%) (figure 20). And just 8% of respondents considered their institution to be this effective at use and management of unstructured data.

“Data-driven risk management has become a big evolution in our risk management practices. Across the board, the trend

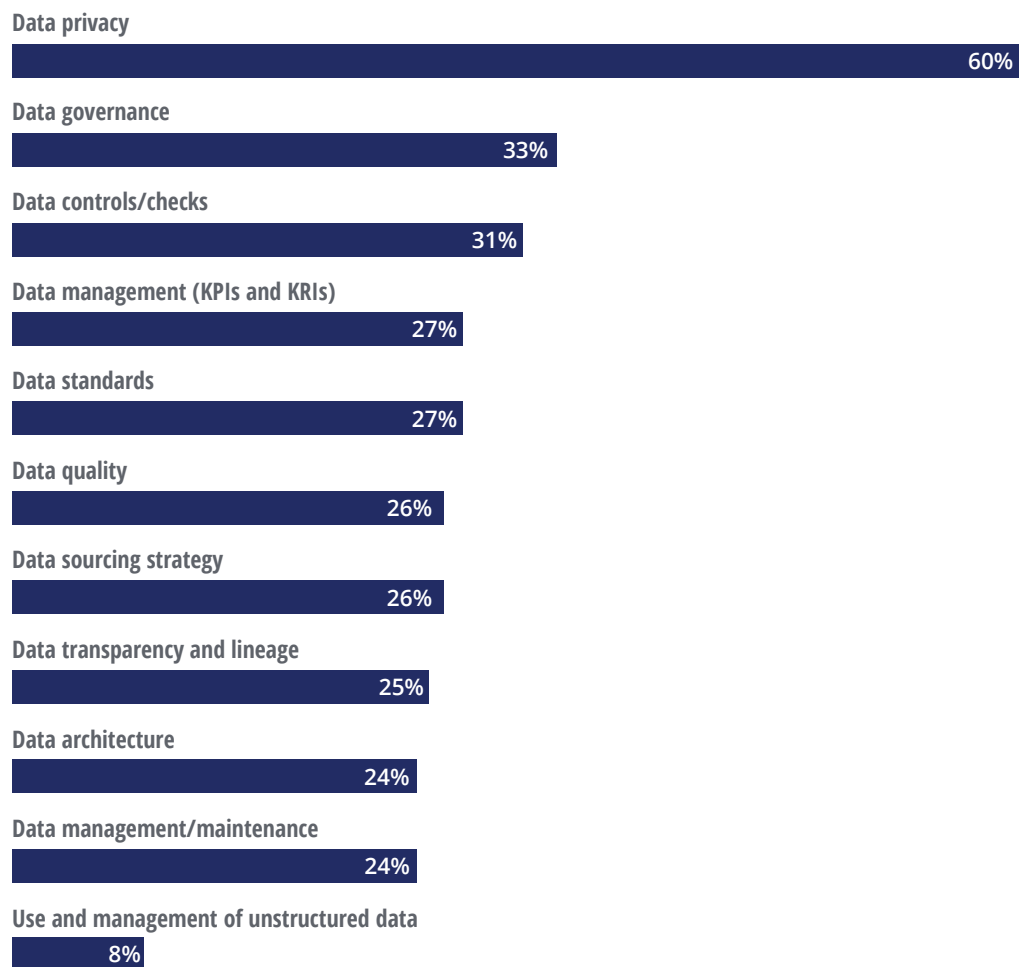
across risks is to move away from qualitative assessments to be more data and scenario driven. The shift was underway but has been accelerated with increased focus and governance during the pandemic. Financial risks are further ahead but operational risk is moving rapidly in that direction.”

— VP Enterprise Risk, Large financial institution

FIGURE 20

How effective do you think your organization is in each of the following aspects of risk data strategy and infrastructure?

■ Extremely/very effective



Source: Deloitte Global Risk Management Survey, 12th ed.

Data privacy

When asked about risk data strategy at their institutions, the only area where a majority of respondents rated their institutions as extremely or very effective was *data privacy* (60%). The high rating for *data privacy* may be overly optimistic since only 31% considered their institutions to be extremely or very effective at *data controls/checks*, which are required to safeguard data privacy. In addition, 63% of respondents said *that data privacy, protection, and risk management* will be an extremely or very high priority for their institutions over the next two years.

This is probably due to the intense focus on this issue by regulators. The European Union's GDPR, which took effect in May 2018, placed data protection requirements on all institutions that hold the data of EU citizens, even if they are headquartered elsewhere, including the need to obtain consumer consent before collecting personal data, among other provisions. In the United States, California's Consumer Privacy Act has led to other states also enacting data privacy and security legislation. Many other countries have done so as well.

When asked whether their institutions have implemented and tested their capabilities to comply with data governance and management

guidance and regulations (such as BCBS 239, GDPR, and the California Consumer Privacy Act), 39% of respondents said their institutions have fully implemented and tested capabilities required to comply, while an additional 32% said they had implemented but not yet tested their capabilities. Although GDPR is fairly recent, BCBS 239 has been in existence since 2013. These results indicate that many institutions need to increase their pace of implementation. In addition, the fact that most institutions have not yet fully implemented and tested their capabilities to comply with these requirements is another indication that many respondents may be giving their institutions overly positive ratings regarding their effectiveness in safeguarding data privacy.

"Data loss is something that we're very focused on. One of the outcomes of people working from home is you're more exposed to data loss. We've had a rising incidence there, but we've been able to put in place appropriate prevention and detection controls. We're certainly alert to some of the confidentiality risks that occur. How do you manage control of data?"

— Chief Risk Officer, Diversified financial services firm

Sector risk topics

Banking

For banking institutions in the United States, there has been a trend toward aligning regulatory requirements more closely to the complexity of the bank. The Federal Reserve's revised enhanced prudential standards for domestic and foreign holding companies fine-tuned many requirements based on financial metrics that serve as a proxy for an institution's size, complexity, interconnectedness, and systemic importance. These efforts were driven by a concern that the requirements as initially written did not appropriately balance the tradeoff between *safety and soundness* and *burden*, especially for smaller, less complex banks.¹⁹

In Europe, even before the slowdown in economic activity due to the COVID-19 pandemic, some banks faced an expected capital shortfall from the implementation of the finalized Basel III standards.²⁰ In March 2020, the Basel Committee announced that it would delay the implementation of the final phase of the Basel III rules by one year, to January 1, 2023, to help ease the imposition of higher capital constraints that some banks could have faced during the ongoing economic recession.²¹

Although the implementation has been delayed, banks should continue their efforts to prepare to implement the Basel Committee's revisions to its capital requirements for market risk, known as the Fundamental Review of the Trading Book (FRTB). When asked about the status of their institution's implementation of FRTB, only 5% of respondent institutions subject to FRTB said they were *already fully FRTB compliant*, while 53% said *implementation was in progress*.

Investment management

Although the economic downturn triggered by COVID-19 created additional market volatility, investment management respondents rated their firms highly in managing this risk. Eighty-six percent of respondents at firms that provide investment management services believed their organizations are extremely or very effective at managing *market risk*.

These respondents were asked how challenging a range of issues were for their investment management business, and relatively few respondents considered any issue to be especially challenging. The two issues most often rated as extremely or very challenging related to data: *data management and availability* (30%), and *use of alternative and unstructured data in investment and operational processes (e.g., crowdsourcing, geospatial, cognitive analytics)* (30%).

Respondents reported that a variety of roles and responsibilities are assigned to the individual or individuals responsible for managing risk in their investment management function, most often citing *monitor compliance with investment guidelines related to investment risk (e.g., tracking error, sector/industry exposures)* (80%).

Other responsibilities that were cited by a majority of respondents included *developing and implementing the investment risk management framework, methodologies, standards, policies, and limits* (75%); *meeting regularly with governance committees responsible for overseeing investment risk management* (75%); *periodic reassessment of investment risk to identify risk concentrations and potential style drifts* (65%);

and *managing the stress-testing process, including governance, methodology, and reporting* (60%).

THIRD-PARTY OVERSIGHT

Managing third-party risk is an issue for all institutions but it is especially important for those providing investment management services, which often rely heavily on third-party vendors. These institutions often outsource day-to-day management of client investments to investment subadvisers, and employ service providers for technology applications, data management, and operational aspects. Only 15% of respondents at institutions providing investment management services *rated oversight over third-party managers, service providers, and suppliers* as being extremely or very challenging for their organization's investment management business.

Conducting ongoing monitoring to review the risks from third-party relationships is an important element of effective risk management. Respondents at firms providing investment management services most often said their institutions review the risks from these relationships annually, with this being most common for administrators (60%), transfer agents (60%), pricing vendors (58%), prime brokers (50%), and reference data providers (50%). Reviewing the risks from these relationships more often—either monthly or quarterly—was most often reported for custodians (33%), transfer agents (30%), and infrastructure technology vendors (29%).

Continuous monitoring was only reported by roughly 20% of institutions or less for the different types of vendors, with the single exception of intermediaries (27%). Over time, we may see more institutions move to continuous monitoring for certain categories of vendors, such as administrators.

DATA AND ANALYTICS

Relatively few respondents providing investment management services rated issues regarding IT systems and data as extremely or very challenging for their investment management business, with this being most common *for data management and availability* (30%), *use of alternative and unstructured data in investment and operational processes* (e.g., *crowdsourcing, geospatial, cognitive analytics*) (30%), and *IT applications and systems* (technology) (25%).

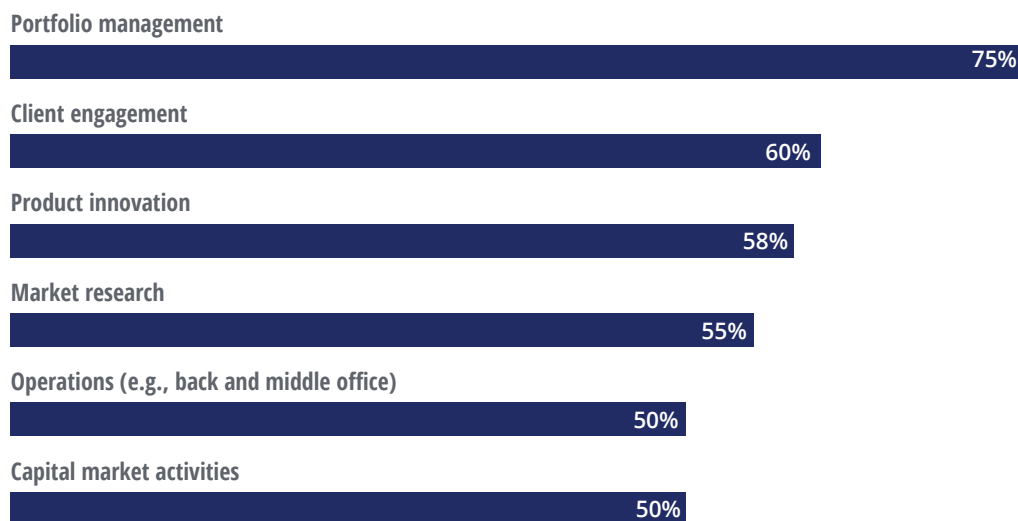
Firms providing investment management services are increasingly recognizing the potential of emerging technologies such as RPA, cognitive analytics, machine learning, and natural language processing to increase efficiency while improving the ability to identify potential risk events, such as instances of insider trading. A substantial number of respondents said they thought it was extremely or very likely that their institutions would seek to enhance their data and analytics capabilities to improve various aspects of their investment management business, including *portfolio management* (75%), *client engagement* (60%), *product innovation* (58%), and *market research* (55%) (figure 21).

FIGURE 21

Over the next two years, how likely is your organization to seek to enhance its data and analytics capabilities to improve each of the following aspects of its investment management business?

Base: Organizations that provide investment management services

■ Extremely/very likely



Source: Deloitte Global Risk Management Survey, 12th ed.

Insurance

ASSESSING INSURANCE RISK

Respondents at companies providing insurance services considered their companies to be extremely or very effective at managing various types of insurance-related risks such as *morbidity* (92%), *underwriting/reserving* (88%), *mortality* (86%), and *catastrophe* (83%). However, insurance companies will need to be vigilant in monitoring these risks, especially *morbidity* and *mortality*.

In contrast, only 48% of respondents at institutions providing insurance services rated their institutions as extremely or very effective in managing *geopolitical* risk, an area that will require more focus given the increasing uncertainties in the global political environment.

Respondents at these institutions reported using a variety of approaches to assess insurance risk. The approaches used most often as a *primary methodology* are *actuarial reserving* (68%), *internal capital framework/model* (55%), *value at risk* (53%), *regulatory capital* (50%), *stress testing* (50%), and *claims ratio analysis* (50%) (figure 22).

Among institutions providing insurance services that perform stress testing, almost all respondents said it is performed on *market risk* (85%) and *interest rate risk* (80%), areas where risk scenarios are relatively easy to define and quantify. Somewhat surprisingly, 85% of respondents also said that stress testing is performed on *operational events* (e.g., *cyber*, *business resiliency*, or *third-party vendor*), where it is more challenging to employ. Stress testing was less often reported to be conducted on other risk factors such as *property and casualty claim cost* (65%), *expense* (45%), and

ESG (including climate) (30%). Many insurers will need to consider deploying stress testing more broadly, especially with regard to climate risk, which is increasingly being required by regulators.

REGULATORY AND ECONOMIC CAPITAL

Regulatory authorities around the world are imposing stricter capital standards on insurance companies, with the most influential regime being Solvency II, which was developed by EU regulators. Many insurance companies have applied for and received approval of internal capital models permitted by Solvency II.

In June 2020, EIOPA announced that it would extend the date by which it would deliver its advice on the Solvency II review to the European Commission to the end of December 2020 to allow for an assessment of the impact of COVID-19 on the insurance industry.²²

Among the institutions providing insurance services that participated in the survey, 38% said they are subject to Solvency II requirements. With other regulators looking to Solvency II as a model, an additional 33% of these respondents said their institutions are subject to regulatory capital requirements similar to Solvency II.

Half of the respondents providing insurance services said their companies are required by their lead insurance regulator to undertake a solvency test for their insurance group, while 33% said their insurance group is not subject to a solvency test, but believed it would likely be in the future.

Insurers should expect that a group solvency requirement will gain ground in the coming years, and they should take steps to be ready to comply. Eighty-one percent of respondents providing insurance services said they are subject to a legal entity solvency test, and the remaining 19% said they are not currently subject to one, but believed they are likely to be in the future.

GLOBAL CAPITAL STANDARD

The IAIS is working to develop a global insurance capital standard (ICS) with the aim of allowing insurers to operate across borders more efficiently, reduce costs, and bring benefits to consumers. On March 27, 2020, the IAIS announced that as part of its efforts to address the impact of COVID-19 on the insurance sector, it had extended the deadline for submitting data for its review of the ICS reporting and the aggregation method to October 31, 2020.²³

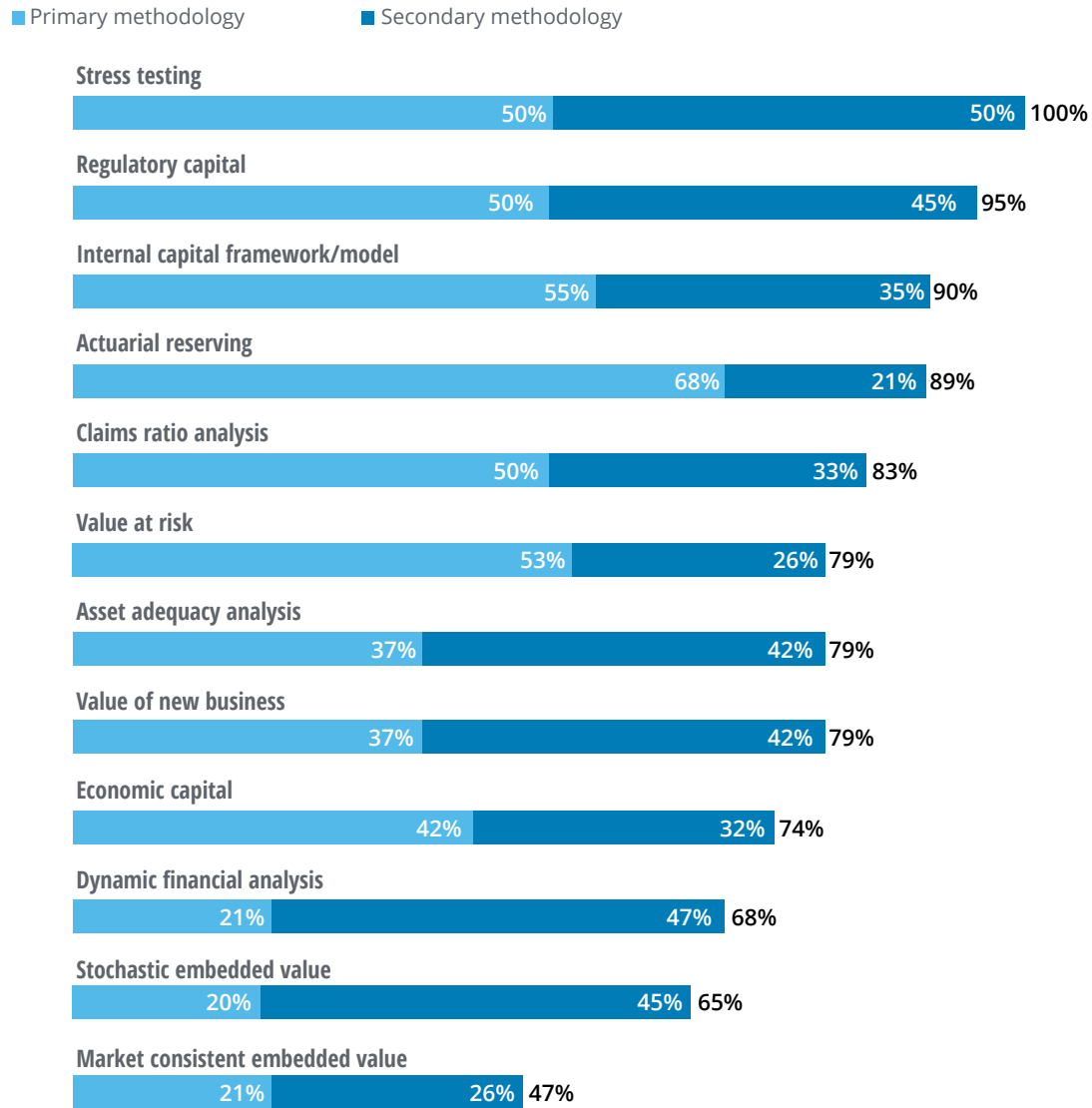
Respondents that provide insurance services were asked what level of impact they expected the ICS to have on their company. These respondents most often considered the ICS to have at least a somewhat significant impact (74%), although only 37% expected the impact would be extremely or very significant.

The two other issues where insurance respondents most often expected at least a somewhat significant impact were *broader ComFrame requirements of risk management and governance* (63%, with 26% extremely or very significant) and *recovery and resolution planning* (60%, with 20% extremely or very significant).

FIGURE 22

To what extent does your organization use each of the following methods to assess insurance risk?

Base: Organizations that provide insurance/reinsurance services



Source: Deloitte Global Risk Management Survey, 12th ed.

Conclusion

IN 2020, RISK management faced an exceptionally volatile and uncertain business environment created by the COVID-19 pandemic. Looking ahead, governments are facing the conundrum of how best to balance public health concerns and economic health for their citizens.

The global health crisis and the resulting economic contraction served to heighten some longstanding risks while also creating distinctive new issues. The economic downturn significantly increased credit risk among both retail and business customers. Institutions will need to monitor carefully which countries and sectors are returning to growth fairly quickly and which have a longer road to recovery.

The pressure on revenues increased the existing motivation to reduce risk management expenses, which have been growing continually since the global financial crisis. The drive to reduce risk management budgets is likely to grow if the recession is prolonged.

The goal of reducing risk management expenses could spur increased investment in emerging technologies that can drive down costs by automating both routine manual tasks and also decisions that require human judgment, with exceptions flagged for review by human professionals. At the same time, these technologies can improve the overall effectiveness of risk management by reducing human error, improving testing, and identifying potential risk events before they occur so that steps can be taken to avoid or mitigate them.

Yet, institutions will need to recognize that machine learning or other predictive technologies that have been trained on pre-COVID-19 data may need to be retrained since business conditions and

consumer behavior have changed dramatically. Institutions will also need to monitor and comply with an evolving set of regulatory expectations regarding AI and other technologies.

The global health crisis and the resulting economic contraction served to heighten some longstanding risks while also creating distinctive new issues.

These technologies depend on timely, high-quality risk data that has been aggregated across the organization, but this is often difficult to achieve. Many institutions could benefit from making data management a higher priority and may want to consider creating a data management office led by a CDO to oversee data management across the enterprise.

The health crisis has increased the importance of effectively managing nonfinancial risks. COVID-19 tested the operational resilience of institutions and their ability to rely on digital tools to allow their employees to work virtually. One senior risk management executive interviewed for this study commented that they had compressed a decade of transformation work into a matter of months.

Employees working remotely due to COVID-19 have created additional cybersecurity challenges. Institutions may be more vulnerable to cyberattacks, fraud, and breaches of customer data, which could expose them to greater risk of

noncompliance with data privacy requirements. The potential for conduct risk can grow, since conversations with customers may not be subject to the same monitoring and controls.

As the pandemic continues, the responses of governments, businesses, and consumers to COVID-19 are transitioning from short-term measures into a longer-term set of working practices with no end date in sight. Institutions should consider how they can maintain productivity if the COVID-19 practices become the new normal. How can they successfully maintain morale and communicate their culture and values when employees, especially new hires, are working virtually? How can they continue to innovate, when team members can't brainstorm while sitting around a table in a meeting or over a meal or drink after hours? How to maintain morale in a virtual working environment will continue to be a particular concern at institutions that are reducing overall headcount to shrink operating budgets.

In short, COVID-19 has raised the stakes, and shifted the playing field, for risk management. Risk management will need the flexibility to respond quickly to volatile economic conditions and changing work practices, while continually monitoring which changes are temporary responses to the pandemic and which are destined to become permanent. At the same time, institutions will need a strong foundation in place—including a risk appetite statement that informs strategy and decision-making, a CRO with sufficient independence and authority, an effective three lines of defense governance model, and robust IT systems with comprehensive, high-quality supporting data.

The challenges have not been this great in recent memory. To meet them successfully, risk management will need strong governance, coupled with the agility to respond to the morphing profile of risks in these volatile times.

Risk management will need the flexibility to respond quickly to volatile economic conditions and changing work practices, while continually monitoring which changes are temporary responses to the pandemic and which are destined to become permanent.

Endnotes

1. International Monetary Fund, "World economic outlook: A long and difficult ascent," October 2020.
2. Y Charts, "10-year Treasury rate," accessed December 24, 2020.
3. Tadhg Enright, "How will Brexit impact London as Europe's leading financial hub?," Euronews, November 10, 2020.
4. European Central Bank, "ECB Banking Supervision provides temporary relief for capital requirements for market risk," press release, April 16, 2020.
5. For a discussion of regulatory responses to COVID-19, see Deloitte, *Interim regulatory outlook 2020: Hard times*, 2020.
6. In this report, institutions that provide banking services will sometimes be termed "banks" (even if they also provide other types of financial services); institutions that provide insurance services will be termed "insurance companies" (even if they also provide other types of financial services); and institutions that provide investment management services will sometimes be termed "investment management firms" (even if they also provide other types of financial services).
7. Percentages total more than 100% since respondents could make multiple selections.
8. Percentages total more than 100% since respondents could make multiple selections.
9. FitchRatings, "European GTUBs' rising credit costs drive 2Q20 profit slump," August 6, 2020.
10. *Leveraged lending* was not included in the 2018 survey.
11. For a discussion of the impact on COVID-19 on liquidity management, see Deloitte's report, *COVID-19 impact on bank liquidity risk management and response*, 2020.
12. Christine Lagarde, "Estimating cyber risk for the financial sector," IMF Blog, International Monetary Fund, June 22, 2018.
13. Charlie Osborne, "COVID-19 blamed for 238% surge in cyberattacks against banks," ZDNet, May 14, 2020.
14. Peter Baldwin, "New York Department of Financial Services issues new guidance regarding COVID-19 cybersecurity risks," *National Law Review*, April 14, 2020.
15. Bank of England, "The 2021 biennial exploratory scenario on the financial risks from climate change," December 18, 2019.
16. European Insurance and Occupational Pensions Authority, "EIOPA consults on the supervision of the use of climate change scenarios in ORSA," October 5, 2020.
17. For a discussion of the Royal Commission, see the report by Deloitte Australia, *Post Royal Commission—A new era*, 2019.
18. Bank of Japan, "Legal responsibility in investment decisions using algorithms and AI," 26 April 2019.
19. For a discussion of the tailoring of regulatory requirements in the United States, see Deloitte's report *Banking regulatory outlook 2020*, 2020.
20. Deloitte, *Consensus no more? Financial Markets Regulatory Outlook 2020*, 2020.
21. FitchRatings, "EU banks key beneficiaries of Basel III coronavirus delay," April 1, 2020.

22. European Insurance and Occupational Pensions Authority, "EIOPA revises its timetable for advice on Solvency II Review until end December 2020," April 30, 2020.
23. Thomson Reuters Practical Law Financial Services, "COVID-19: IAIS addresses impact on insurance sector," March 27, 2020.

About the author

J. H. Caldwell | jacaldwell@deloitte.com

J. H. Caldwell, a partner at Deloitte Risk & Financial Advisory, Deloitte & Touche LLP, as well as Global Risk Advisory leader for the Financial Services Industry, has more than 25 years of risk management experience within the sector. He has deep experience with the complete credit lifecycle, enterprise risk management, operational risk, and integrated compliance risk management. His extensive experience in the area of credit includes quantitative methodology, portfolio analytics, process, and controls, integrating risk management practices, and addressing and resolving the Office of the Comptroller of the Currency (OCC) and other regulatory issues.

Acknowledgments

SUBJECT MATTER ADVISERS

- **Laurent Berliner**, Luxembourg, lberliner@deloitte.lu
- **Kristina Davis**, Boston, kbdavis@deloitte.com
- **Karl Ehram**, Parsippany, kehram@deloitte.com
- **Richard Godfrey**, Parsippany, rgodfrey@deloitte.com
- **Edward Hida**, New York, ehida@deloitte.com
- **Julian Leake**, London, jleake@deloitte.co.uk
- **Ricardo Martinez**, New York, rimartinez@deloitte.com
- **Nino Montemarano**, Toronto, nmontemarano@deloitte.ca
- **Monica O'Reilly**, San Francisco, monoreilly@deloitte.com
- **Markus Salchegger**, Munich, msalchegger@deloitte.de
- **David Sherwood**, Stamford, dsherwood@deloitte.com
- **David Strachan**, London, dastrachan@deloitte.co.uk
- **Kristen Sullivan**, Stamford, ksullivan@deloitte.com
- **Tony Wood**, Hong Kong, tonywood@deloitte.com.hk

EDITORS

J. H. Caldwell

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

Jesselyn Garrisi

Senior manager | Deloitte & Touche LLP
+1 646 872 4704 | jgarrisi@deloitte.com

This report is the result of a team effort that included contributions by financial service 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.

In addition, the following individuals from Deloitte in the United States conducted analysis and provided project management, editorial, and/or design support:

Lisa Hallman, Senior Manager, Deloitte Services LP

Ulyana Stoyan, Manager, Deloitte & Touche LLP

Contact us

Our insights can help you take advantage of change. If you're looking for fresh ideas to address your challenges, we should talk.

Industry leadership

Bob Contri

Global leader | Financial services industry | Deloitte Global
+1 212 436 2043 | bcontri@deloitte.com

Anna Celner

Global leader | Banking and capital markets | Deloitte Global
+41 58 279 6850 | acelner@deloitte.ch

Neal Baumann

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

Cary Stier

Global leader | Investment management | Deloitte Global
+1 203 708 4642 | cstier@deloitte.com

Deloitte.

Insights

Sign up for Deloitte Insights updates at www.deloitte.com/insights.



Follow @DeloitteInsight

Deloitte Insights contributors

Editorial: Hannah Bachman, Aditi Rao, and Nairita Gangopadhyay

Creative: Victoria Lee and Jaime Austin

Promotion: Hannah Rapp

Cover artwork: Daniel Hertzberg

About Deloitte Insights

Deloitte Insights publishes original articles, reports and periodicals that provide insights for businesses, the public sector and NGOs. Our goal is to draw upon research and experience from throughout our professional services organization, and that of coauthors in academia and business, to advance the conversation on a broad spectrum of topics of interest to executives and government leaders.

Deloitte Insights is an imprint of Deloitte Development LLC.

About this publication

This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or its and their affiliates are, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your finances or your business. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

None of Deloitte Touche Tohmatsu Limited, its member firms, or its and their respective affiliates shall be responsible for any loss whatsoever sustained by any person who relies on this publication.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.