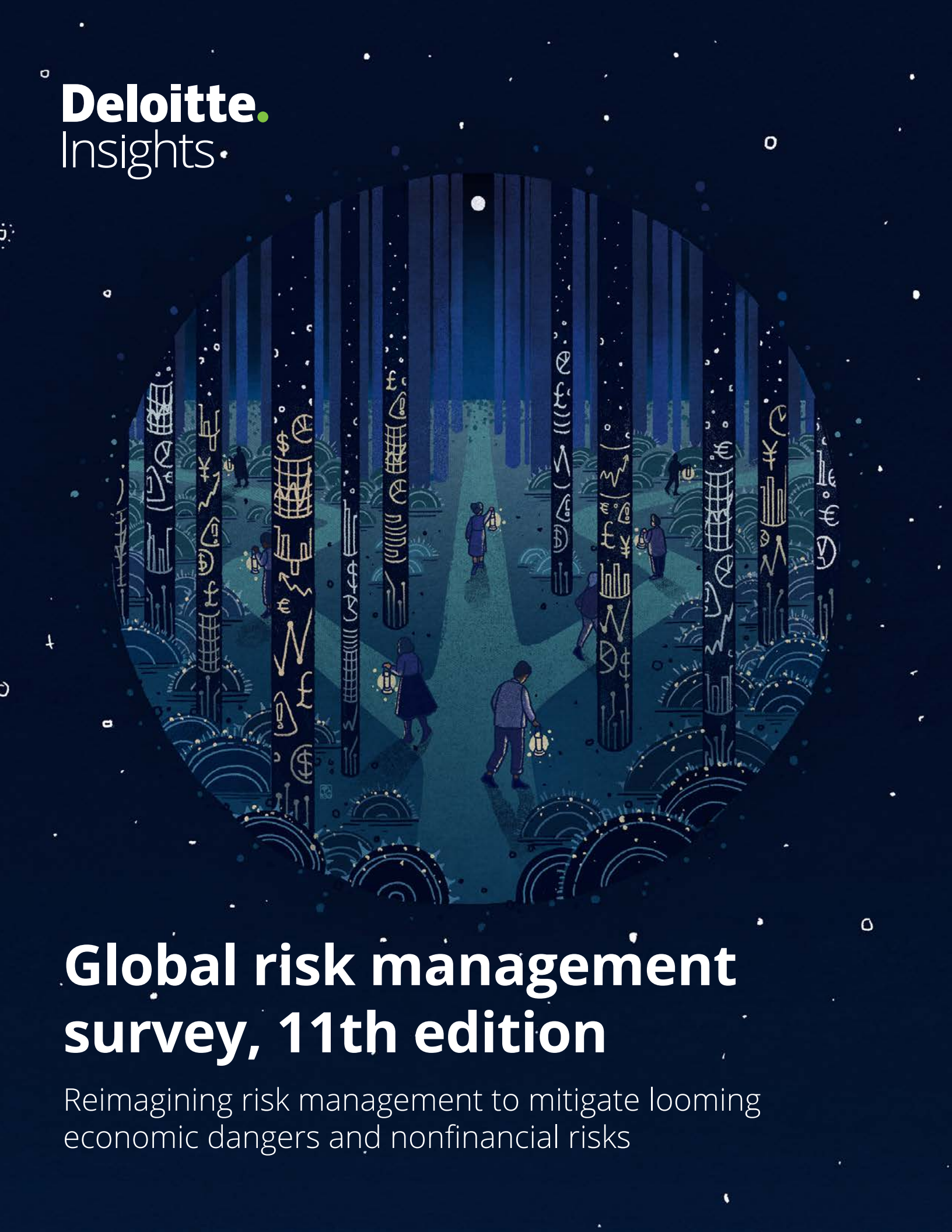
Deloitte.
Insights



Global risk management survey, 11th edition

Reimagining risk management to mitigate looming economic dangers and nonfinancial risks

Deloitte Risk and Financial Advisory helps organizations navigate a variety of risks to lead in the marketplace and disrupt through innovation. With our insights, you can learn how to embrace complexity and accelerate performance.

Contents

Foreword

ON BEHALF OF the Deloitte member firms, I am pleased to present the 11th edition of *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 94 financial institutions around the world and across multiple financial services sectors, representing a total of US$29.1 trillion in aggregate assets. We wish to express our appreciation to all the survey participants for their time and insights.

The current edition found that the trend over the course of the survey series toward widespread adoption of stronger risk management practices has continued. Boards of directors at most institutions are actively providing risk management oversight. The chief risk officer (CRO) position has become nearly universal, and more institutions report that their boards of directors conduct executive sessions with the CRO. Enterprise risk management (ERM) programs designed to identify and manage risks across the organization have been adopted by more than three-quarters of institutions surveyed.

Financial institutions have extensive experience, well-developed methodologies, and access to required data to manage financial risks, and roughly 90 percent of respondents report that their institutions are *extremely* or *very effective* at managing market, credit, and liquidity risks.

While there has been undeniable progress, risk management is now facing a new set of demands as it confronts a number of looming risks. Although the torrent of regulatory change has slowed, there remain major unresolved regulatory issues such as the global capital standard being developed by the International Association of Insurance Supervisors (IAIS) and adopting and implementing the final Basel III capital framework. Meanwhile, as individual regulators have become more willing to vary global regulations for their individual jurisdictions, global institutions need to respond to an increasing divergence in regulatory standards. Geopolitical risk has increased due to the uncertainty over the final terms of the United Kingdom's departure from the European Union (EU) under Brexit; continuing trade negotiations among the United States, China, the EU, and other jurisdictions; decelerating economic growth coupled with rising debt levels in China; and growing concerns that conditions may be ripe for another in the series of periodic financial crises that have affected the global financial markets and economy.

While institutions have become more skilled at managing financial risks, nonfinancial risks—such as cybersecurity, model, third-party, and conduct risk—have assumed greater prominence as the exposure and consequences from these risks have become more evident. For example, financial institutions and regulators around the world have been increasing their focus on cybersecurity risk in the wake of numerous cyberattacks on banks and other financial services institutions. There have been numerous conduct incidents with both consumer and institutional customers, in many cases resulting in significant fines and lasting reputational damage to the firms involved.

Responding to the new environment will require institutions to rethink their traditional approaches. Many institutions have or will likely need to reexamine their three lines of defense risk governance models to clarify the responsibilities of each line and eliminate overlaps and redundancies. Hiring and developing required risk management talent will become even more important, especially in the business units comprising Line 1.

Leveraging the power of advanced technologies—such as robotic process automation (RPA), machine learning, cognitive analytics, and natural language processing—could lead to even more fundamental changes in how risk management operates. These technologies may not only reduce operating expenses by automating manual tasks but also have the potential to improve effectiveness by automatically testing 100 percent of a set of transactions, rather than having humans test a sample, and by identifying potential risk events in real time to allow preventive actions to be taken. Yet, as they are employed more broadly—both in the risk management function and in the business units—advanced technologies also create additional risks that need to be managed.

Effectively managing nonfinancial risks and employing emerging technologies will both place a greater premium on implementing an integrated data architecture and gaining access to high-quality, timely data.

This is a formidable set of challenges posed by today's more complex and uncertain risk environment. Meeting them will require institutions to rethink traditional assumptions and employ fundamentally new approaches to risk management.

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,

Edward T. Hida, CFA
Financial risk community of practice leader
Financial services
Deloitte & Touche LLP

Executive summary

DESPITE THE RELATIVE calm in the global economy, risk management today is confronting a series of substantial impending risks that will require financial services institutions to rethink traditional approaches. The global economy has strengthened, but storm clouds remain on the horizon in the form of tensions over tariffs between the United States, China, the European Union, and other jurisdictions that could potentially result in lower trade volumes. Global economic growth has been reduced by weak growth in Europe coupled with a more slowly growing Chinese economy burdened with increasing debt levels. With the lack of a final Brexit agreement between the European Union and United Kingdom, there remains significant uncertainty as to its impact for many firms.

The global economy has strengthened, but storm clouds remain on the horizon.

While the tsunami of regulatory change in the wake of the financial crisis appears to have crested, financial services institutions are preparing for a number of regulatory requirements that are still to be finalized and assessing the full implications of implementing those that have recently been finalized. Meanwhile, global institutions are facing an environment in which regulations are becoming increasingly fragmented across jurisdictions. The revisions of the Basel Committee on Banking Supervision (Basel Committee) to capital adequacy and other requirements under Basel III, while finalized, have yet to be adopted, and could be revised, by local regulatory authorities. IAIS is working to develop a global insurance capital standard (ICS) with many issues still unresolved, including defining a valuation basis and specifying the role of internal models in determining capital requirements. The final agreement for the withdrawal of the United Kingdom from the European Union under Brexit, which is still being negotiated,

will have important impacts on the supervision of markets and financial institutions based in the United Kingdom and Europe, and for investment banking booking practices and models. The EU's General Data Protection Regulation (GDPR), which took effect in May 2018, places new obligations on all financial institutions that have EU citizen data to secure consumer consent for its use, among other requirements. Initiatives to increase data privacy have also been underway in India and China. There has been a greater focus on conduct risk in many jurisdictions, notably Australia's Royal Commission into Misconduct in the Banking, Superannuation, and Financial Services Industry.

Risk management needs to be infused into strategy so that the institution's risk appetite and risk utilization are key considerations in the process of developing its strategic plan and strategic objectives.

In recent years, financial institutions have improved the capabilities of their risk management programs to manage traditional risk types such as market, credit, and liquidity risk. Managing nonfinancial risk is now assuming greater importance, both for regulators and institutions. Among the many nonfinancial risks, increasingly sophisticated cyberattacks by individuals and nation states have made cybersecurity a top concern. Well-publicized instances of inappropriate behavior at major financial institutions have underscored the importance of managing conduct risk. Risk events at third parties employed by financial institutions can result in significant financial losses and reputational damage.

Financial institutions should consider reengineering their risk management programs to develop the capabilities required to meet these challenges, and some have already undertaken efforts to enhance these programs. The three lines of defense risk governance model should be reexamined to clarify the responsibilities of each line of defense, especially the business units and functions that comprise Line 1. Risk data governance at many institutions will likely need to be enhanced to provide the accessible, high-quality, and timely data required for stress testing, operational risk management, and other applications.

Financial institutions should also consider leveraging the power of digital technologies—such as RPA, machine learning, cognitive analytics, cloud computing, and natural language processing—to increase both the efficiency and effectiveness of risk management. These tools can reduce costs by automating manual tasks such as developing risk reports or reviewing transactions. They can also automatically scan a wide variety of data in the internal and external environments to identify and respond to new risks, emerging threats, and bad actors.

Finally, risk management needs to be infused into strategy so that the institution's risk appetite and risk utilization are key considerations in the process of developing its strategic plan and strategic objectives.

Deloitte's *Global risk management survey, 11th 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 2018 to July 2018 and was completed by 94 financial institutions around the world that operate in a range of financial sectors and with aggregate assets of US$29.1 trillion.

Key findings

CONTINUED GROWING IMPORTANCE OF CYBERSECURITY RISK

There was broad consensus that *cybersecurity* is the risk type increasing the most in importance. Sixty-seven percent of respondents named *cybersecurity* as one of the three risks that would increase the most in importance for their business over the next two years, far more than for any other risk. Yet, only about one-half of the respondents felt their institutions were extremely or very effective in managing this risk. For specific types of cybersecurity risks, respondents most often considered their institutions to be extremely or very effective in managing *disruptive attacks* (58 percent), *financial losses or fraud* (57 percent), *cybersecurity risks from customers* (54 percent), *loss of sensitive data* (54 percent), and *destructive attacks* (53 percent). They were less likely to consider their institutions to be this effective when it came to *threats from nation state actors* (37 percent) or *cybersecurity risks from third-party providers* (31 percent). In managing cybersecurity risk, respondents most often cited as extremely or very challenging *staying ahead of changing business needs* (e.g., social mobile, analytics, and cloud) (58 percent) and *addressing threats from sophisticated actors* (e.g., nation states, skilled hacktivists) (58 percent). The awareness of cybersecurity risk is growing, and fewer respondents than in the last survey considered several related governance issues to be extremely or very challenging: *getting the businesses to understand their role in cybersecurity risk* (31 percent, down from 47 percent), *setting an effective multiyear cybersecurity risk strategy approved by the board* (31 percent, down from 53 percent), and *securing ongoing funding/investment* (18 percent, down from 38 percent).

> "One of the biggest challenges for cyber risk is the war for talent and constantly attracting and retaining good people. Salaries for cyber risk talent are spiraling."
>
> —Chief risk officer, large financial services company

INCREASING FOCUS ON NONFINANCIAL RISKS

Almost all respondents considered their institutions to be extremely or very effective in managing traditional financial risks such as *market* (92 percent), *credit* (89 percent), *asset and liability* (87 percent), and *liquidity* (87 percent). In contrast, roughly one-half of the respondents said the same about a number of nonfinancial risks including *reputation* (57 percent), *operational* (56 percent), *business resilience* (54 percent), *model* (51 percent), *conduct and culture* (50 percent), *strategic* (46 percent), *third-party* (40 percent), *geopolitical* (35 percent), and *data integrity* (34 percent). Financial institutions should consider adopting a holistic approach to managing nonfinancial risks.

ADDRESSING RISK DATA AND IT SYSTEMS IS A TOP PRIORITY

A theme that runs throughout the survey results is the importance of enhancing risk data and IT systems. This has been a continuing issue for financial institutions and the financial services industry for some time and indicates the deep-seated difficulty of providing quality data from source through many systems and processes to its ultimate users. When asked about the risk management priorities for their institutions over the next two years, the issues cited most often as being an extremely or very high priority were *enhancing the quality, availability, and timeliness of risk data* (79 percent) and *enhancing risk information systems and technology infrastructure* (68 percent). This is consistent with results showing roughly one-third of respondents felt their institutions were extremely or very effec-

tive regarding *data governance* (34 percent) and *data controls/checks* (33 percent). Relatively few respondents considered various aspects of their institution's operational risk data to be extremely or very well-developed such as *sufficient duration of internal loss data* (39 percent), *completeness of loss data events* (37 percent), *consistency of loss event capture across different organizational units* (36 percent), *sufficiency and granularity of legal loss data information* (34 percent), and *quality of loss data information* (34 percent). When asked about the challenges in stress testing, *data quality and management for stress testing calculations* was most often considered to be extremely or very challenging both for capital stress testing (42 percent) and liquidity stress testing (30 percent).

THE POTENTIAL OF DIGITAL RISK MANAGEMENT

Continued advances in a range of emerging technologies present a significant opportunity to dramatically transform the efficiency and effectiveness of risk management. Much of this opportunity is still to be realized; relatively few institutions reported applying some of these emerging technologies to risk management.

> "We are strengthening the second line of defense with technology tools, like AI and machine learning, to make them more efficient and effective. This will be essential for risk management to be successful in the coming years."
>
> —Chief risk officer, major asset management company

The technologies that institutions most often reported using were *cloud computing* (48 percent), *big data and analytics* (40 percent), and *Business Process Modeling (BPM) tools* (38 percent). Although much attention has been given to RPA to reduce costs and improve accuracy by automating repetitive manual tasks without human involvement, only 29 percent of respondents said their institutions are currently using it. RPA usage is most common in *risk data* (25 percent), *risk reporting* (21 percent), and *regulatory reporting* (20 percent). Other tools are being used by even fewer institutions, including *machine learning* (25 percent), *Business Decision Modeling (BDM) tools* (24 percent), and *cognitive analytics* (including natural language processing/natural language generation) (19 percent).

Although adoption is currently fairly low, respondents believed that emerging technologies will deliver very large or large benefits in many areas such as *increase operational efficiency/reduce error rates* (68 percent), *enhance risk analysis and detection* (67 percent), and *improve timely reporting* (60 percent). Roughly one-half of respondents expected new technologies to provide this level of benefit to *improve the scope and coverage of risk management via exception handling versus sample testing* (54 percent) and *reduce costs* (45 percent).

ADDRESSING THE CHALLENGES IN THE THREE LINES OF DEFENSE RISK GOVERNANCE MODEL

Virtually all institutions (97 percent) reported employing the three lines of defense risk governance model, but said they face significant challenges. The challenges most often cited as significant typically involved the role of Line 1 (business units) including *defining the roles and responsibilities between Line 1 (business) and Line 2 (risk management)* (50 percent), *getting buy-in from Line 1 (the business)* (44 percent), *eliminating overlap in the roles of the three lines of defense* (38 percent), *having sufficient skilled personnel in Line 1* (33 percent), and *executing Line 1 responsibilities* (33 percent). These challenges are consistent with our experience with financial institutions as many have been, or are in the process of, clarifying the roles of the first and second lines of defense and working to improve the efficiency and effectiveness within the three lines of defense model.

INCREASING RELIANCE ON STRESS TESTING

Almost all institutions reported using capital (90 percent) and liquidity (87 percent) stress tests, and are placing greater reliance on them. The most common uses for stress tests were *understanding the organization's risk profile* (100 percent for capital stress tests and 99 percent for liquidity stress tests), *reporting to the board* (97 percent for capital stress tests and 95 for liquidity stress tests), and *reporting to senior management* (97 percent for capital stress tests and 100 percent for liquidity stress tests). Responding to regulatory requirements is a key driver in the use of stress tests, and almost all respondents said their institution uses this tool for *meeting regulatory requirements and expectations* (95 percent for both capital and liquidity stress tests), *assessing adequacy of regulatory capital* (95 percent), and *assessing the adequacy of regulatory liquidity ratios and buffers* (96 percent).

Capital stress tests are being used more often as a key tool for boards and management, with more respondents saying that they are being used *extensively* in many areas than was the case in the prior survey. These tests include *reporting to the board* (64 percent, up from 46 percent), *reporting to senior management* (61 percent, up from 49 percent), *defining/updating capital capacity requirements for risk* (47 percent, up from 24 percent), and *strategy and business planning* (38 percent, up from 26 percent).

Liquidity stress tests are also being used more extensively in several areas: *assessing adequacy of excess liquidity* (57 percent, up from 39 percent), *meeting regulatory requirements and expectations* (65 percent, up from 52 percent), and *setting liquidity limits* (56 percent, up from 44 percent).

STRONGER BOARD OVERSIGHT

Reflecting the slower pace of regulatory change, only 28 percent of respondents said their boards of directors were spending considerably more time on risk management compared to two years ago, which is down from 44 percent in the previous survey. Many institutions are following leading practices[1] in board oversight, with 63 percent of respondents saying that the primary responsibility for risk oversight is placed on a risk committee of the board of directors, and 70 percent saying the risk committee is composed either entirely (35 percent) or of a majority (35 percent) of independent directors, while 84 percent said the committee is chaired by an independent director.

WIDESPREAD ADOPTION OF THE CRO POSITION

The prevalence of the CRO position continues to expand over the course of the survey series, with 95 percent of institutions now having a CRO. However, there remains room for improvement in CRO reporting relationships by having the CRO report both to the CEO and the board of directors. One-quarter of respondents said their CRO did *not* report to the institution's CEO, and roughly one-half said the CRO did not report to the board of directors or a board committee.

CONTINUED INCREASE IN THE ADOPTION OF ERM

Eighty-three percent of respondents said their institutions have an ERM program in place, up from 73 percent in the previous survey, with an additional 9 percent saying they were in the process of implementing one. In addition to addressing data and IT systems issues as noted above, the issues that were most often cited by respondents as being an extremely or very high priority for their institutions' ERM programs were *collaboration between the business units and the risk management function* (66 percent), *managing increasing regulatory requirements and expectations* (61 percent), and *establishing and embedding the risk culture across the enterprise* (55 percent).

Introduction

Economic and business environment

Developments in the global economy, business outlook, and regulatory requirements are creating a challenging new environment for risk management.

Global economic environment

GLOBAL GROWTH IS expected to be 3.7 percent for 2018 and 2019, remaining at its 2017 level, although the economic performance across countries and regions has become more uneven.[2] In the United States, GDP is expected to expand by 2.9 percent in 2018, stimulated by tax cuts enacted in 2017, but slow to 2.5 percent in 2019 due to headwinds from increased tariffs. Growth in the euro area economy is also anticipated to slow from 2.4 percent in 2017 to 2.0 percent in 2018 and 1.9 percent in 2019. The United Kingdom, which is still negotiating an exit from the European Union mandated by the Brexit vote, is expected to expand by 1.4 percent in 2018 and 1.5 percent in 2019. The Japanese economy continues to tread water, with expected growth of just 1.0 percent in 2018 and 0.9 percent in 2019.

China is facing a slowing economy together with rising debt. After expanding 6.9 percent in 2017, economic growth in China is expected to slow to 6.6 percent in 2018 and 6.2 percent in 2019. Over the last several years, the Chinese government has encouraged banks to provide credit to stimulate the economy, which has led to rapidly rising levels of debt. Between the fourth quarter of 2008 and the first quarter of 2018, China's gross debt jumped from 171 percent to 299 percent of GDP.[3] Speculation has driven real estate values higher, raising concerns about a pullback. A decline in real estate values would impact individual investors, who are also major players in the Chinese stock market. At the same time, China is broadening its global reach with its Belt and Road Initiative, an array of infrastructure projects around the world.[4]

The rising tensions over trade policy provide a source of uncertainty in the global economic outlook. In mid-2018, the United States imposed tariffs of US$34 billion on Chinese technology goods and US$3 billion on Chinese steel and aluminum, while China announced tariffs on US$16 billion of US products.[5] On the other hand, in September 2018, agreement was reached on the United States-Mexico-Canada Agreement (USMCA) to replace the North American Free Trade Agreement (NAFTA).[6] The prospect of increased tariffs between the United States and the European Union lessened in July 2018 when President Trump and EC President Jean-Claude Juncker agreed to suspend announced tariff increases and work toward the goal of eliminating all tariffs.[7]

The rising tensions over trade policy provide a source of uncertainty in the global economic outlook.

New sanctions announced by the United States are expected to have a substantial impact on the economies of specific countries including Russia, Turkey, North Korea, and Iran.

There have been growing concerns that the world economy may be ready for another in the series of periodic crises that have hit markets and reduced growth. Although the 2008 financial crisis was especially severe, the prior decades saw the 2000 dot-com crash, the 1997 Asian currency crisis, and the 1987 "Black Monday" stock market crash. While no one can say with certainty what will cause the next crisis, history suggests that one will come in due course. An environment with historically low interest rates has encouraged emerging market countries to substantially increase their debt levels, with much of the exposures being denominated in dollars. In 2018, the sudden drop in the value of the Turkish lira prompted fears that this would cause financial contagion affecting other emerging markets. In October 2016, the International Monetary Fund concluded that emerging market economies remained vulnerable to changes in monetary policy in advanced economies, which have maintained historically low interest rates. Their analysis places a 5 percent probability that emerging market economies (excluding China) could face outflows in their debt portfolio in the medium term of US$100 billion or more over a period of four quarters, similar in magnitude to the global financial crisis.[8]

In addition, there has been a rapid buildup of corporate debt, especially among borrowers with the lowest investment-grade credit ratings (BBB), which now constitute the largest slice of the investment-grade corporate bond market.[9] Lending by nonbanks such as private equity, hedge funds, and mortgage companies has grown rapidly, such as for home mortgages. These institutions typically are willing to offer loans with less restrictive credit terms and conditions, and they are not subject to the same close regulatory oversight of traditional banks.

All these trends suggest that, despite generally positive economic conditions, financial institutions need to remain vigilant in closely monitoring their risk exposures and in considering the ability to survive a potential systemic risk event.

Financial institutions outlook

In contrast to the last several years of weak returns, in 2017 and 2018 financial institutions benefited from stronger economic conditions, especially in the United States. Although the capital markets business has remained slow, consumer business has been strong, with low rates of default and rising interest rates. In the first quarter of 2018, US banks reported record profits that were up 27.5 percent compared to a year earlier, with 70 percent of institutions posting revenue increases.[10]

There have been growing concerns that the world economy may be ready for another in the series of periodic crises that have hit markets and reduced growth.

The performance of European financial institutions has been weaker, with their return on equity decreasing slightly to 6.8 percent in the first quarter of 2018 compared to a year earlier.[11] In particular, revenues have been weak at their investment banking divisions, which have lagged behind the investment banking performance at comparable US institutions.[12]

Financial institutions around the world should begin preparing for the phase out of the London Interbank Offered Rate (LIBOR) in response to the revelations that the rate had been manipulated. Regulatory authorities, such as the Federal Reserve in the United States and the Bank of England, are developing and assessing alternative, more market-

based benchmarks to replace LIBOR. Transitioning away from loans pegged to LIBOR will require substantial work and transition rules. While newly issued loans can be pegged to a new benchmark, the industry will need to determine how to manage the US$300 trillion of existing loans, derivatives, and other contracts pegged to LIBOR if the rate is no longer published.[13] While some loan documents may include language to address the possibility of using an alternative rate, others simply cite the LIBOR rate. Transitioning away from LIBOR creates additional operational risk and the potential for market dislocation.

With the Brexit negotiations still underway, the eventual impact on the financial industry in Europe of the withdrawal of the United Kingdom from the European Union remains unclear. Among the many issues that remain to be resolved are the treatment of derivative contracts and of cross-border insurance contracts with durations beyond the United Kingdom's exit date. Financial services institutions based in the United Kingdom will lose their ability to operate throughout the European Union under the passporting regime. In 2018, an estimated £1.4 trillion in assets were managed in the United Kingdom on behalf of European clients.[14] Some institutions have been opening front offices and dealing rooms on the continent, with cities like Paris, Amsterdam, and Frankfurt benefiting. There is also the possibility that clearing activities and euro-denominated trading may shift from London to these and other cities in the European Union.

Banks, investment management firms, and insurers are also facing new business models with an increased interest in *open banking*, driven by advances in technology and escalating customer expectations. Open banking is the shift from a traditional closed model to one in which data is shared among different members of the banking ecosystem, with authorization from the customer.[15] Complying with evolving regulatory requirements regarding the use of customer data will be an essential component of adopting an open banking model. (For a discussion of these regulatory requirements, see the section, "Regulatory risk.") Open banking can enable institutions to become more customer-centric and can help them create entirely new products and services.

> "The world where insurance is sold and brokered rather than bought by customers is changing. The future generation will be buying insurance over the internet in ways where the product must be transparent, and opacity will be discouraged."
>
> —Chief risk officer, large diversified financial services company

The trends spurring open banking also are stoking interest in new fintech competitors, which are leveraging technology capabilities to introduce new products and directly target customers. Competition from fintech firms is not confined to startups, but now includes major technology and e-commerce companies. Unlike fintech startups, these companies enjoy advantages that make them formidable competitors, including a large base of pre-existing customers, expansive customer data sets, and strong brands. For example, in China, the Yu'e Bao fund created by Ant Financial Services Group, an affiliate of Alibaba, grew in just five years to become one of the world's largest money-market funds with US$210 billion in assets under management as of June 2018.[16]

Regulators around the world are beginning to develop regulatory frameworks for fintech firms. A number of countries, including the United Kingdom, Singapore, and Australia, provide a regulatory "sandbox" that allows fintech firms to experiment with new financial products within a specific space and duration, without making them subject to traditional regulatory requirements.[17] For example, the Australian Securities & Investments Commission allows fintech firms to test certain services for up to 12 months without an Australian financial services or credit license. In March 2018, the European Union issued an action plan designed to help Europe become a global hub for fintech.[18] The US Office of the Comptroller of the Currency announced in July

2018 that it would begin accepting applications for national bank charters from fintech firms.[19]

Traditional financial institutions have started pilot programs themselves to employ new technologies and are entering into joint ventures with fintech firms. These developments offer the promise of designing more customized products and delivering them more quickly to customers at lower operating costs through automated tools. Yet, as technology-powered financial products gain acceptance, institutions will need to be prepared to manage the additional risks these approaches can create due to the heavy reliance on technology such as increased cybersecurity and third-party risk.

Global regulatory environment

The Basel Committee reached a final agreement on the Basel III reforms, and no major new regulatory reforms are anticipated from the group in the near term. The Basel Committee's finalization of the Basel III framework is an indication that the post-crisis regulatory reform era has ended.

In the United States, in May 2018 the Economic Growth, Regulatory Relief, and Consumer Protection Act marked the most significant changes to the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) since its enactment in 2010. It adjusted regulatory thresholds, thereby modifying or eliminating certain requirements such as capital stress tests, resolution planning, and liquidity requirements for thousands of banks with less than US$250 billion in assets, while leaving stricter supervision in place for the largest, most systemically important institutions.[20]

However, the pace of regulatory examinations and findings about improving risk management and governance practices continues, at times reaching the level of enforcement actions and fines. This indicates that while the pace of new regulations has slowed down, the overall level and intensity of regulatory supervision show no signs of abating.

China announced the merger of its banking and insurance regulators, the China Banking Regulatory Commission (CBRC) and China Insurance Regulatory Commission (CIRC), providing new authority to its central bank to provide macro supervision.[21] Although there had been discussion of also merging the securities regulator, the China Securities Regulatory Commission (CSRC) will remain separate.

Despite an overall slowdown in the pace of regulatory change, regulators around the world are increasing their focus on a number of issues such as risk management data and IT systems, and especially the management of nonfinancial risks such as cybersecurity, consumer data protection and privacy, conduct and culture, and anti–money laundering. In the area of consumer privacy, the EU's GDPR placed new requirements on financial services institutions operating in the European Union to allow consumers to understand, and take control of, how their personal data is being used.

Anti–money laundering regulations have also been the subject of increased attention. In 2018, the European Banking Authority (EBA) found "general and systematic shortcomings" in Malta's application of anti-money laundering rules, launched an inquiry into the Danish supervision of a major financial institution with regard to alleged money laundering, and announced a review into how all EU member states are applying rules in this area.[22]

Regulatory initiatives to strengthen the management of conduct and culture risk by enhancing accountability have been taken in the United States, United Kingdom, Australia, and Hong Kong, among others.[23] (For discussions about cybersecurity, conduct and culture, and data and IT systems, see the sections, "Cybersecurity," "Conduct and culture," and "Risk management information systems and technology.")

Risk management

The increased volatility and unpredictability in the business and regulatory environment provide strong incentives for financial institutions to transform their risk management programs. Institutions are pivoting from responding to a continual

series of new regulatory requirements to focus instead on infusing risk management into business strategy and their lines of business, and on improving operations.

Nonfinancial risks are now assuming greater importance than before. Increasingly sophisticated cyberattacks, including by nation states, have put cybersecurity at the top of the agenda for risk management. The increasing reliance on models for product pricing, Generally Accepted Accounting Principles (GAAP) and statutory valuation, risk and capital management, strategic planning, and other purposes have intensified institutions' and regulators' attention to model validation and model risk management.[24] A series of instances of inappropriate conduct have inflicted significant reputational damage on major institutions and increased the attention devoted to managing conduct and culture risk.[25]

Institutions are engaging in risk management re-engineering and renewal programs to help ensure their risk management programs can address these and other challenges. An important element of many renewal programs is to re-examine the "three lines of defense" risk governance model to eliminate overlapping responsibilities, ensure business units take clear ownership of the risks they assume, and have risk management provide oversight and challenge.

Institutions are re-engineering risk management by employing the latest technologies and digital tools, such as big data, cloud computing, robotics and process automation, cognitive analytics, and natural language processing. These digital tools can not only increase efficiency by automating manual tasks, they can identify emerging threats, while providing insight into interactions among risks and their causal factors. Among the many applications, AI capabilities are providing greater visibility into managing risk sensitivities in capital markets, improving insurance underwriting, optimizing margin valuation adjustments, and detecting anomalous projections generated by stress-testing models. Further, by automating risk management assessments, these tools make it possible to review 100 percent of a set of transactions, rather than relying on human review of only a sample.

> "We are using a variety of new technologies. For example, we are using automation for processing data and reporting, and are building tools for automatically monitoring compliance and Bank Secrecy Act/Anti Money Laundering Law, as well as our reputation in the marketplace."
>
> —Chief risk officer, major multinational bank

To employ these tools effectively, however, most institutions will need to enhance their risk frameworks to address risks created through use of these technologies. In addition, data management and IT infrastructure will also require attention. While some financial institutions have made progress in improving their data environments, many still lack access to granular, high-quality data, including unstructured data such as emails, chat, voice, social media, and others that is required to unlock the potential of digital technologies. Beyond gaining access to this data, institutions will need to ensure their data environments comply with consumer privacy regulations such as GDPR.

Institutions are engaging in risk management re-engineering and renewal programs to help ensure their risk management programs can address these and other challenges.

About the survey

This report presents findings from the 11th edition of Deloitte's ongoing survey of risk management practices in the global financial services industry. The survey gathered the views of CROs or their equivalents at 94 financial services institutions around the world and was conducted from March to July 2018.

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).[26]

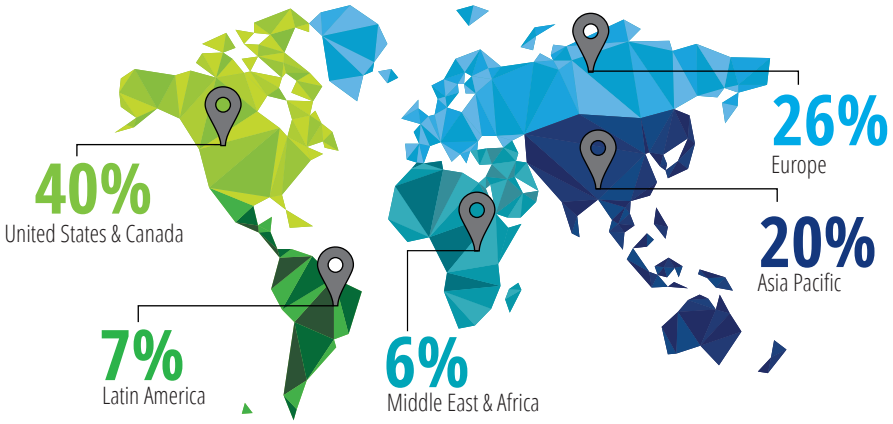
Most of the survey participants are multinational institutions, with 72 percent having operations outside their home country.

The participating institutions provide a range of financial services, including banking (61 percent), investment management (49 percent), and insurance (46 percent) (figure 2).[27]

The institutions have total combined assets of US$29.1 trillion and represent a range of asset sizes (figure 3). Institutions that provide asset management services represent a total of US$23 trillion in assets under management.

FIGURE 1

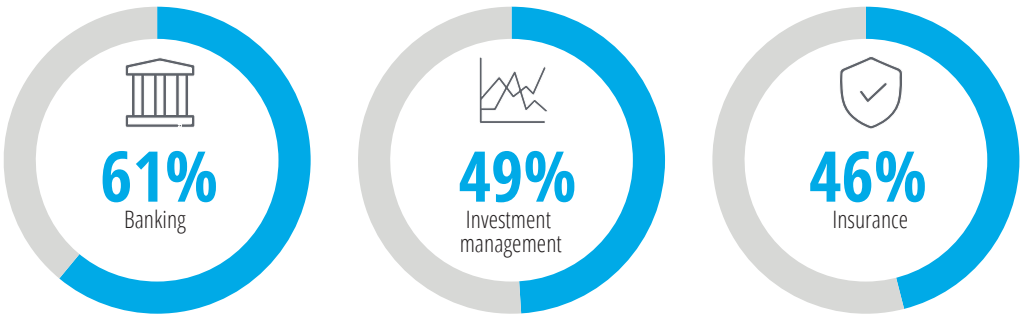
Participants by headquarters location



Note: Percentages may not total 100% due to rounding.
Source: Deloitte analysis.

FIGURE 2

Participants by financial services provided



Source: Deloitte analysis.

Where relevant, the report compares the results from the current survey with those from earlier surveys in this ongoing series.

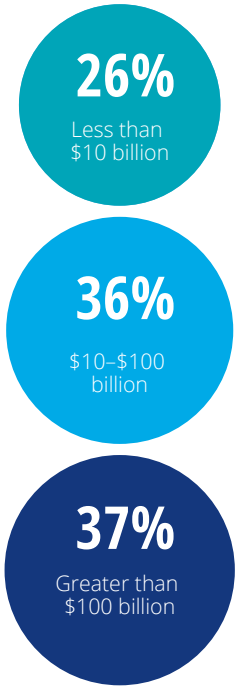
ANALYSIS BY ASSET SIZE

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

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

FIGURE 3

Participants by asset size



Note: Percentages may not total 100% due to rounding.
Source: Deloitte analysis.

Risk governance

Role of the board of directors

THE IMPORTANCE OF the board of directors in providing oversight for a financial institution's risk management program is included in regulatory guidance or mandates by numerous regulatory authorities around the world. The Basel Committee principles stipulate that a bank's board of directors should have overall responsibility for the institution's risk management.[28] The 2018 revisions to the Dodd-Frank Act modified the thresholds of the Enhanced Prudential Standards (EPS) rule issued by the Federal Reserve so that all US banks with consolidated assets of US$50 billion or more are required to have a risk committee of the board of directors chaired by an independent director, up from US$10 billion or more previously.[29] The standards of the US Office of the Comptroller of the Currency (OCC) require large banks to have a risk-governance framework approved by the board of directors.

In the insurance industry, the passing of the Risk Management Own Risk and Solvency Assessment Model Act #505, by the National Association of Insurance Commissioners, requires that companies submit an annual filing that specifies its risk management framework. This includes the policies and role of its board of directors.[30] Solvency II has specific requirements for a "fit and proper" board that conducts proper oversight of risk management throughout an insurance company's activities.

In response to the financial crisis, risk governance and the role of the board of directors in risk management increased substantially in importance. Boards of directors became much more active in providing oversight of the risk management program, rather than merely receiving periodic reports from management. Yet, often the lines have blurred between the appropriate role of the board and that of senior management, as boards have assumed operational responsibilities that are more appropriately executed by management. For example, under the US Federal Reserve's annual Comprehensive Capital Analysis and Review (CCAR), boards of directors are expected to provide oversight of the assumptions used in risk scenarios. In June 2018, in its draft paper on the composition and role of the board, the IAIS found that some insurance companies lack a clear distinction between oversight responsibilities appropriate to the board and day-to-day management of the business.[31]

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

There is now a recalibration underway to have boards instead concentrate on providing oversight and challenge. The US Federal Reserve has proposed revisiting the supervisory expectations of bank boards "to establish principles regarding effective boards of directors focused on the performance of a board's core responsibilities."[32] The proposal reviews the role of the board with the goal of creating a stricter delineation between board oversight responsibilities and management's obligation, and provides new Board Effectiveness (BE) guidance.[33]

With the pace of regulatory change slowing and the recognition that boards should concentrate on

effective oversight, respondents were less likely to say their board of directors was spending more time on risk management compared to two years ago. Although 79 percent of respondents said their boards of directors are spending more time on risk management compared to two years ago, only 28 percent said they are spending *considerably* more time, which is down from 44 percent in the 2016 survey. The slowing of the rate of change is even more dramatic in specific regions. In the United States/Canada, only 18 percent of respondents said their boards are spending considerably more time on risk management compared to 44 percent in the prior survey, while the percentages for European institutions were 29 percent, down from 50 percent.

Boards of directors at most institutions have a wide range of risk management responsibilities (figure 4). More than 90 percent of institutions

FIGURE 4

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

Source: Deloitte analysis.

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

Locating oversight responsibility for risk management in a risk committee of the board of directors is a regulatory expectation and has become a widely accepted practice.

> "We report information on current and trending risk appetite utilization in every board meeting so that board members are well-informed about where we are relative to risk appetite."
>
> —Chief risk officer, large financial services company

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

Stress tests have assumed greater importance for regulators and financial institutions to assess capital adequacy and financial resilience. Seventy-nine percent of respondents said that *review stress testing scenarios and results* is a board responsibility, while 67 percent cited *review individual risk management policies* as a responsibility of their boards.

The percentage of respondents who said that *conduct executive sessions with the CRO* is a board responsibility rose from 53 percent to 66 percent, which is a sign of progress in the independence and seniority of the risk management function.

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

Board risk committees

Locating oversight responsibility for risk management in a risk committee of the board of directors is a regulatory expectation and has become a widely accepted practice. The guidance issued in 2010 by the Basel Committee emphasized the importance of a board-level risk committee, especially for large and internationally active banks, and the revised guidance issued in 2015 specified the appropriate role of the risk committee.[34] The US Federal Reserve's EPS requires that US banks have a separate risk committee, with some related requirements phased in based on the size of the institution.[35]

Sixty-three percent of respondents reported that the primary responsibility for risk oversight is placed in a risk committee of the board of directors. An additional 21 percent of respondents said that oversight responsibility is placed with other committees, such as jointly with the combined risk and audit committees (7 percent). Placing oversight responsibility in the board risk committee is more common with banks (72 percent) than with investment management (61 percent) or insurance (56 percent). Only 14 percent of institutions said that the full board of directors has oversight responsibility.

There has also been a trend among regulators to expect risk committees to contain independent directors that possess risk management expertise and skills. The US Federal Reserve's EPS not only requires that banks have a separate risk committee but also that this committee has an independent chairman and a risk expert.

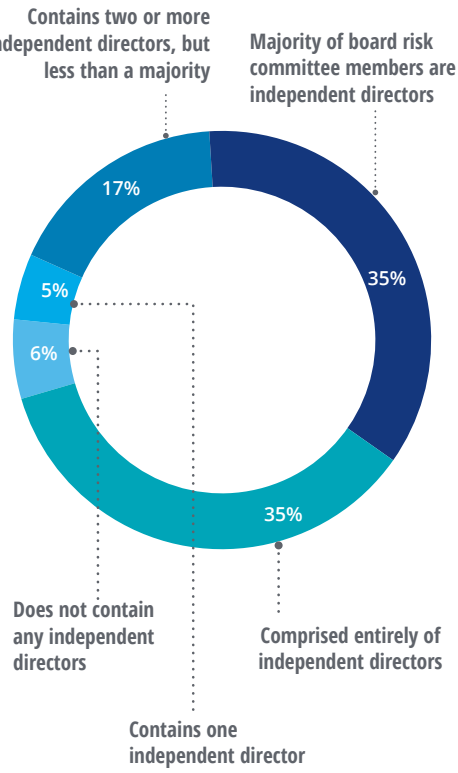
These regulatory expectations have had an impact, and in the survey, 70 percent of respondents said their board's risk committee is comprised either entirely (35 percent) or of a majority (35 percent) of independent directors (figure 5). Only 6 percent of respondents said their board risk committee does not contain any independent directors.

The move toward independent directors is most pronounced in the United States/Canada, where 87 percent of respondents reported their board risk committee was composed of either entirely or a majority of independent directors, compared to 67 percent in Europe and 58 percent in Asia-Pacific.

Further, an independent director chairs the board risk committee or equivalent committee for risk management oversight at 84 percent of participating institutions, which is up from 72 percent two years ago. Having the risk committee be chaired by an independent director is more common in the United States/Canada (92 percent, up from 78 percent in the prior survey) than it is in Asia-Pacific (82 percent) or Europe (79 percent). The prevalence of this practice in the United States/Canada is likely in response to the requirements of the US Federal Reserve's EPS.

FIGURE 5

Which one of the following accurately describes the membership of independent directors on your board risk committee or the equivalent committee(s) responsible for overseeing risk management?



Note: Percentages may not total 100% due to rounding.
Source: Deloitte analysis.

The presence of one or more risk management expert on the board risk committee is becoming a regulatory expectation for larger institutions. In the past, this has presented challenges due to a limited number of suitable director candidates with risk management experience. Yet, 84 percent of respondents in the current survey said their institution has one or more risk management expert on its board risk committee, up from 67 percent two years ago. This indicates that institutions are increasingly able to identify and retain board director risk experts.

Having risk management experts on the board risk committee is more common among banks (91 percent) and investment management firms (91

percent) than among insurance companies (77 percent), which is likely the result of the greater focus on this issue among banking regulators.[36]

Role of the CRO and the independent risk management function

There has been progress in meeting the regulatory expectation that financial institutions have an independent risk management function. The existence of a CRO position is almost universal, with 95 percent of respondents saying they have a CRO or equivalent, a figure that has risen steadily over the course of this survey series (figure 6).

There are important benefits in having the CRO report to both the CEO and the board of directors, but this is not always the practice. Seventy-five percent of respondents said their CRO reports to the CEO, which means that in one-quarter of institutions, the CRO does not report to the most senior management executive. Similarly, only 52 percent of respondents said that their CRO reports to the board of directors or a board committee. These results suggest that many institutions have more work to do to put in place appropriate reporting relationships for the CRO.

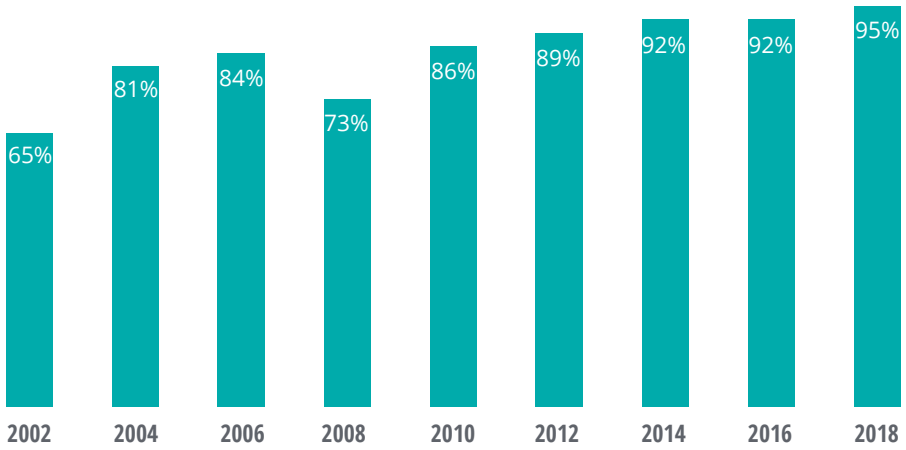
However, 97 percent of respondents said their independent risk management group led by the CRO meets regularly with the board of directors or board committees responsible for risk management. Providing the board of directors the opportunity to meet with the CRO, ideally sometimes without the CEO or other members of senior management present, can allow the board to receive an unvarnished assessment of the institution's risk management program.

> "The strategic planning process is a joint exercise between the business and risk management. Dedicated senior risk leaders are also responsible for providing advice and oversight pertaining to a business risk."
>
> —Senior risk executive, large diversified financial services company

Respondents reported that their risk management functions are tasked with a wide range of responsibilities. Some responsibilities are virtually universal, including *identify new and emerging risks* (99 percent), *develop and implement the risk management framework* (99 percent), and *meet regularly with board of directors or board commit-*

FIGURE 6

Percentage of institutions with a CRO or equivalent



Source: Deloitte analysis.

tees responsible for overseeing risk management (97 percent).

Responsibilities for managing risk management models have become more widespread. *Oversee model governance* is a responsibility of the risk management function at 85 percent of institutions, an increase from 75 percent two years ago. Similarly, *conduct back-testing of risk and related models* is a responsibility at 78 percent of institutions, up from 66 percent in the prior survey.

Model risk management has received additional attention from financial institutions and from regulators in the years since the US Federal Reserve issued SR 11-7 guidance on model risk management.[37] Expectations for model risk management are addressed in CCAR in the United States, and recently the European Central Bank (ECB) issued the Targeted Review of Internal Models (TRIM) guidance designed to enhance the credibility and confirm the adequacy of approved Pillar I internal models.[38]

The survey also indicates that progress is being made in infusing risk management considerations into strategy and day-to-day business decisions. Eighty-one percent of respondents said that a responsibility of risk management is to *provide input into business strategy development and the periodic assessment of the plan*, which increased from 65 percent in the previous survey, *while participate in day-to-day business decisions (e.g., transactions) that impact the risk profile* is a responsibility at 74 percent of institutions, up from 63 percent two years ago.

Risk appetite

A written risk appetite statement is a foundation for effective risk management, providing guidance for senior management when establishing strategic objectives and for lines of business when considering the appropriate level of risk for business decisions. Since the global financial crisis, the importance of a risk appetite statement has received greater attention from regulators including the Financial Stability Board (FSB) and the Basel Committee.[39] Regulators are expecting institutions to integrate nonfinancial risks, such as cybersecurity and conduct risk, into their risk appetite statements, including inherently unquantifiable risks, such as reputational risk.

Institutions are making progress in this area, but more work remains to be done. Ninety percent of respondents said their institutions either have a risk appetite statement that has been approved by the board of directors (84 percent) or are developing a statement for approval (6 percent).

Progress is being made in infusing risk management considerations into strategy and day-to-day business decisions.

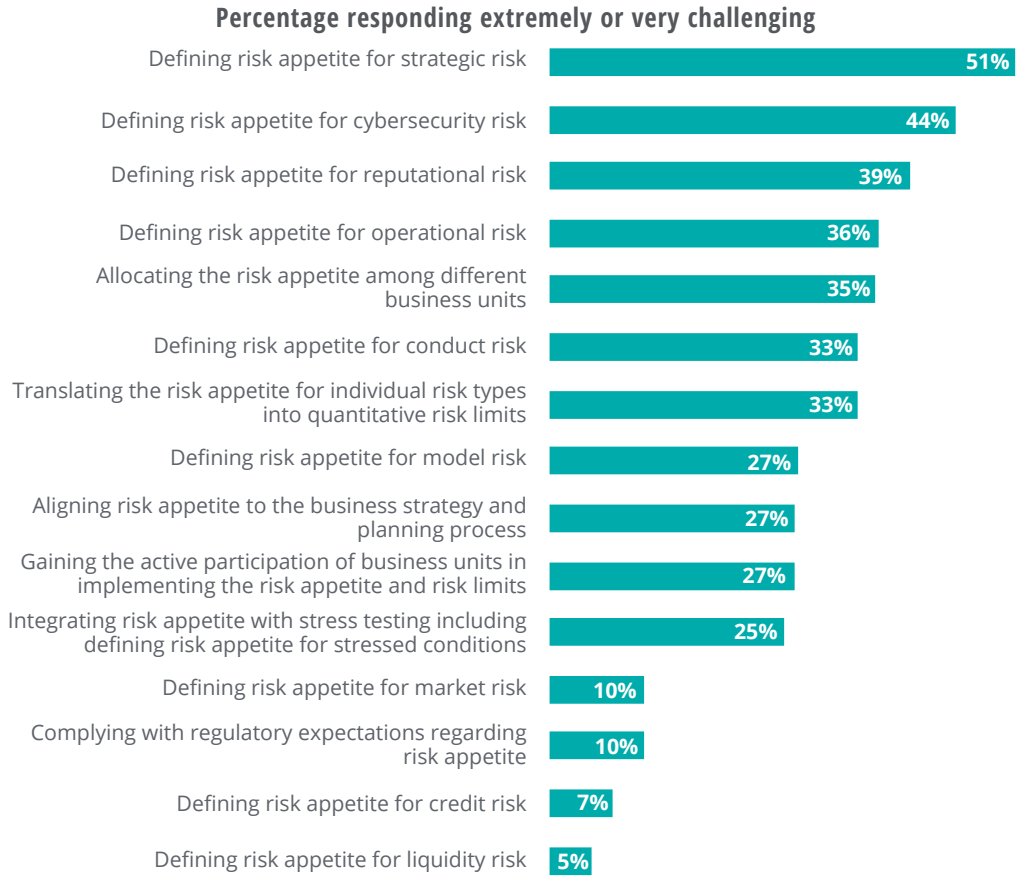
> "We've been spending more time on refining the risk appetite framework and creating a stronger linkage between strategy and risk appetite, and ensuring that it's more explicit at the board and senior management levels. We are also focused on cascading the risk appetite down into appropriate key risk indicators (KRIs) so that we can preemptively monitor and make sure that we don't hit the risk appetite."
>
> —Senior risk management officer, large financial services company

Institutions face a variety of challenges in defining and implementing an enterprise-level risk appetite statement. The issues that were cited most often as being extremely or very challenging in defining risk appetite concerned nonfinancial risks such as *strategic risk* (51 percent), *cybersecurity risk* (44 percent), and *reputational risk* (39 percent) (figure 7). *Conduct risk*, which has been a focus of regulators and is difficult to quantify, was

FIGURE 7

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

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



Source: Deloitte analysis.

also considered to be extremely or very challenging by one-third of respondents.

Defining risk appetite in a quantitative manner for operational risk has also received extensive regulatory attention. Thirty-six percent of respondents said that defining risk appetite for operational risk was extremely or very challenging, up from 27 percent in the prior survey.

In contrast, the financial categories of market, credit, and liquidity risk are more easily quantified, and only 10 percent or fewer of respondents believed they posed this level of challenge in defining risk appetite.

Three lines of defense risk governance model

The "three lines of defense" risk governance model, which details the appropriate roles in risk management of business units, 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:

- Line 1: Business units own and manage their risks
- Line 2: Independent risk function provides oversight and challenge
- Line 3: Internal audit function validates the risk and control framework

Virtually all institutions (97 percent) reported employing the three lines of defense risk governance model. However, while the concept behind the model is sound, institutions confront significant challenges in employing it effectively, especially in establishing the risk management responsibilities of Line 1 (business units). When asked to name the significant challenges for their institution in employing the three lines of defense model, Line 1 was involved in the issues cited most often including *defining the roles and responsibilities between Line 1 (business) and Line 2 (risk management)* (50 percent), *getting buy-in from Line 1 (the business)* (44 percent), *having sufficient skilled personnel in Line 1* (33 percent), and *executing Line 1 responsibilities* (33 percent).

Institutions also face the related challenge of *eliminating overlap in the roles of the three lines of defense* (38 percent). While the role of Line 3 (internal audit) is well understood, it is more difficult to separate the risk management responsibilities of Line 1 (business units) and Line 2 (risk management program).

Although in recent years institutions have devoted greater attention to the importance of business units managing the risks they assume, this has not been easy to achieve. Risk management is still considered by some to be outside the core mission of business units, which are rewarded on their success in generating revenues and profits, rather than their management of risk. Risk management is new territory for many first line business units, and some may resist this additional responsibility. Even when business units buy in to their role in managing risk, many will likely find that they need to hire or develop additional skills. Hiring can be difficult since businesses need to find skilled professionals who combine risk management expertise with experience in the specific business.

In fact, many institutions are making changes to their three lines of defense models. Forty-three percent of respondents said their institutions either have revised their three lines of defense model or are reassessing or planning to reassess their models. Respondents at banks (51 percent) and investment management firms (52 percent) were more likely to report that their institutions have revised or are planning to reassess their models than were those at insurance companies (30 percent). Banks typically have the most developed three lines of defense models, which, over time, can become inefficient and require re-engineering. For institutions offering multiple financial services, such as banking and investment management or insurance, in many cases the banking regulators have spurred them to build their risk governance models across their enterprise, including in their nonbanking operations. Pure investment management firms have not had the same regulatory pressure as banks to build their risk governance frameworks, but they may also be rethinking the appropriate role of each line of defense. Insurance companies also have faced less regulatory pressure than banks to build out their risk governance models and may not face the challenges to the same degree that can arise with a large ERM function.

Many institutions are making changes to their three lines of defense models.

> "Some of our biggest challenges with the first line of defense in managing risk are making sure that they take responsibility for ownership of their risks and training them so that they are knowledgeable about the risk issues."
>
> —Chief risk officer, major multinational bank

Among institutions that have revised or are planning to reassess their three lines of defense models, 56 percent of respondents said their institutions have increased, or plan to increase, the risk management responsibilities of Line 1 (business units) to manage the risks they assume. Fifty-eight percent also said their institutions are increasing the responsibilities of Line 2 (risk management). This indicates that the expectations for the risk management function continue to grow for most organizations. Consistent with the role of internal audit being widely understood, few of the institutions that are making changes are altering the responsibilities of Line 3, with only 23 percent increasing them.

Another important governance decision is how to assign responsibility for each risk type (or "stripe"). For each risk stripe, institutions need to determine whether there should be a single executive responsible for oversight of the risk across the organization, rather than have responsibility decentralized. Having a single individual accountable for oversight is common for some of the important risk stripes such as *market* (86 percent), *liquidity* (85 percent), *regulatory/compliance* (80 percent), and *credit* (79 percent). However, a large majority of respondents also said that a single individual has accountability at their institutions for other risk stripes such as *information security* (85 percent) and *cybersecurity* (82 percent). For some of these risk stripes, accountability is less often placed in a single individual such as *strategic* (43 percent), *reputational* (38 percent), and *conduct and culture* (33 percent).

There has been a broad trend toward assigning accountability for major risk stripes to a single individual. For example, the percentage of respondents saying their institution has a single individual responsible grew for *market risk* (86 percent, up from 75 percent), *cybersecurity* (82 percent, up from 67 percent), *operational risk* (76 percent, up from 67 percent), *insurance risk* (68 percent, up from 56 percent), and *third-party risk* (54 percent, up from 44 percent).

Enterprise control and testing function

Effective risk management requires that an institution's risk and control framework has an effective enterprise control testing function. The survey found that institutions take a wide variety of approaches to where this function is located in the organization. Among the most common locations for this function were *conducted by internal audit* (25 percent), *embedded within the second line of defense centralized control testing function* (22 percent), and *embedded within the second line of defense risk team* (12 percent). In addition, this activity is fragmented at many institutions, with one-quarter of respondents saying it was *performed in various functions*.

Many institutions are finding that a better approach for enterprise control testing is to locate it in a Center of Excellence (COE), which allows them to gain the benefits of economies of scale and more effectively deploy advanced technologies. Institutions can also consider whether to achieve additional savings by locating a COE in a lower-cost location. (See the section, "Increasing ERM efficiency.")

Enterprise risk management

AN ERM PROGRAM is designed to implement a disciplined process to identify and manage risks facing an institution. An organization-wide ERM program helps ensure that all important risks are identified, interdependencies among risks in different business or geographic markets are assessed, clear accountability is assigned, and risk utilization is aligned with the organization's risk appetite. Having an ERM program has become a regulatory expectation, and institutions are expected to employ the insights generated by their ERM program when developing business strategies and making business decisions. The prevalence of an ERM program has steadily increased during the course of this survey series, with 83 percent of institutions in the current survey having an ERM program in place, up from 73 percent in the prior survey (figure 8). Having an ERM program is more common among institutions in the United States/Canada (92 percent) compared to those in Europe (75 percent) or Asia Pacific (79 percent). This indicates that, while ERM programs have become nearly universal in the United States/Canada, there remains some room for increased adoption in Europe and Asia Pacific.

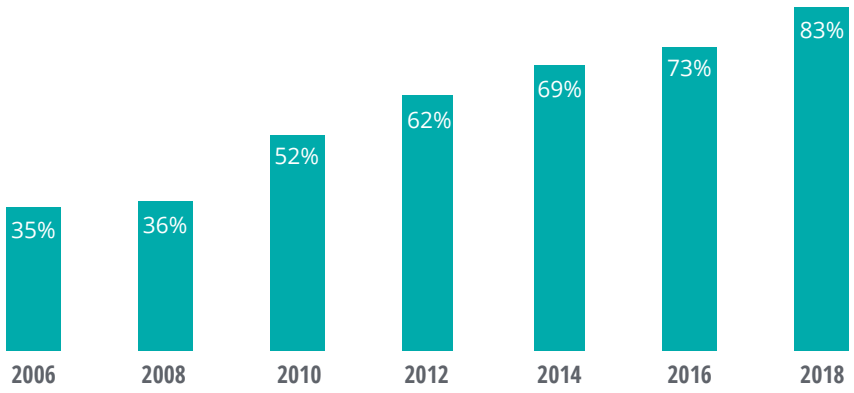
An additional 9 percent of respondents said their institution was in the process of implementing an ERM program, while an additional 4 percent said they were planning to create one. Only 4 percent of respondents said their institution had no plans to create an ERM program.

ERM priorities

An ERM program should have an explicit framework and policy that has been reviewed and approved by the board of directors and the board risk committee, and this has become a widespread practice. Eighty-four percent of respondents reported that their institution has an ERM framework and/or ERM policy that has been approved

FIGURE 8

Percentage of organizations with an ERM program in place



Source: Deloitte analysis.

by their board of directors or appropriate board committee. Over time, as ERM programs mature, one would expect that more institutions would follow this approach.

Respondents cited a wide range of priorities for their institution's risk management programs over the next two years (figure 9). Leading the list was *enhancing the quality, availability, and timeliness*

FIGURE 9

Over the next two years, how much will each of the following be a priority for your organization in risk management?

Percentage responding extremely or very high priority

Source: Deloitte analysis.

of risk data (79 percent) and *enhancing risk information systems and technology infrastructure* (68 percent). Institutions are focusing on unleashing the power of the latest technologies such as RPA and cognitive analytics, and this will require modernized risk technology infrastructure and access to high-quality and timely data on which these tools can operate.

Regarding the challenges facing the three lines of defense models, respondents said a priority for their institutions is to ensure that Line 1 (business units) plays its appropriate role and coordinates with risk management. Sixty-six percent of respondents said that *collaboration between the business units and the risk management function* was an extremely high or very high priority; the issue ranked third highest. Clear lines of responsibility and close coordination between the business units and the risk management program is essential to effectively implement the three lines of defense governance model and presents challenges for many institutions. (See the section, "Three lines of defense risk governance model.") Although only 13 percent of respondents rated *rethinking the three lines of defense model and risk alignment* as a top priority, it is clear that setting clear responsibilities for the role of Line 1 in the three lines of defense model is a key objective for many institutions.

Having an ERM program has become a regulatory expectation, and institutions are expected to employ the insights generated by their ERM program when developing business strategies and making business decisions.

Managing increasing regulatory requirements and expectations was rated in fourth place, with 61 percent considering it to be an extremely high or very high priority. This figure is somewhat lower than 67 percent in the prior survey, which reflects the slower pace of regulatory change.

Roughly one-half or more of respondents considered a variety of other issues to be extremely or very high priorities in such areas as managing emerging risks, managing strategic risk, managing capital and liquidity, increasing efficiency, and attracting and retaining skilled risk management professionals.

Increasing ERM efficiency

With risk management budgets having increased significantly since the financial crisis, 53 percent of respondents cited *increasing the efficiency of the risk management program* as an extremely high or very high priority for their institutions. Fifty-six percent of respondents expected their institution's annual spending on risk management would increase over the next two years, but the pace of budget increases appears to be abating. Twenty-eight percent of respondents anticipated that their institution's annual spending on risk management would increase by more than 10 percent over the next two years, which is down significantly from 44 percent in the prior survey.

Institutions are also working to employ alternative delivery methods to increase efficiency. Respondents were asked which alternative delivery methods their organization uses in 14 individual risk management areas. By far the most common method was a COE, which was cited on average by 70 percent of respondents across the 14 areas. This method was cited most often in the areas of *risk policy* (86 percent), *ERM* (82 percent), and *risk reporting* (77 percent).

While COEs provide important benefits, they are only a first step. Yet, it appears that relatively

few institutions are moving beyond COEs to employ other delivery methods such as *nearshoring* (25 percent) and *offshoring* (6 percent). Respondents named nearshoring most often with respect to *control testing* (35 percent), *risk data* (30 percent), *risk technology* (30 percent), and *credit underwriting* (30 percent). Respondents most often said offshoring is used in *risk technology* (11 percent).

On average across different areas of risk management, only 6 percent of respondents said *outsourcing* was employed, with the most common areas being *model validation* (19 percent), *risk technology* (15 percent), and *model development* (13 percent), which are areas in which institutions often seek additional expertise and capabilities.

The interest in leveraging new technologies to automate formerly manual risk management processes is still in the early stages; much more opportunity remains. There has been discussion of the potential to automate risk management but to date, the fanfare has outpaced the reality. Only 29 percent of respondents said their institutions are currently using RPA, with institutions most often automating *risk data* (25 percent), *risk reporting* (21 percent), and *regulatory reporting* (20 percent). There remains substantial opportunity for institutions to introduce automation into many more aspects of their risk management programs. (See the section, "Risk management information systems and technology.")

Re-engineering risk management

With the volatile environment for risk management, many institutions are undertaking efforts to re-engineer and renew their programs to enhance both their efficiency and effectiveness.[40] Seventy percent of respondents said their institutions have either recently completed a risk management program renewal/update or have one in progress, while an additional 12 percent said they are planning to undertake one. (See the sidebar, "The future of risk management" for a summary of Deloitte's perspective on the issues driving these risk management renewal efforts.)

When asked to what extent specific issues were a priority in their risk renewal programs, respondents most often said that *infuse risk management into strategy* was an extremely or very high priority for their institution (61 percent). In some institutions, senior management establishes strategic objectives without explicit consideration of their implications for risk utilization, with risk management involved after the strategic decisions have been made, simply managing the risks that have been assumed. Instead, risk appetite and utilization should be a key consideration in developing business strategy.

Another issue that was considered by roughly one-half of respondents to be an extremely or very high priority in their risk renewal programs was *focus on conduct risk and risk culture* (53 percent), which has been a regulatory focus and is challenging to quantify and manage.

Leverage emergent technologies was named as an extremely or very high priority by 48 percent of respondents in their risk renewal programs. Institutions are looking to modernize their risk infrastructure by employing new technologies such as RPA, cognitive analytics, and cloud computing, although only a minority of institutions are employing them currently. These tools can allow risk management programs to increase efficiency by automating tasks that are currently done manually. But they can simultaneously improve the effectiveness of risk management by reducing errors and identifying potential risk events. (See the section, "Risk management information systems and technology.") Twenty-four percent of respondents considered *rethink the three lines of defense risk governance model* to be an extremely or very high priority for their risk renewal programs. As we saw above, 42 percent of respondents also said their institutions have revised, or are planning to revise, their three lines of defense governance model. Although use of the three lines of defense model is nearly universal, a significant portion of institutions believe they need to review and enhance their current approach.

THE FUTURE OF RISK MANAGEMENT

The increased volatility and unpredictability in the global economy and in regulatory requirements have created new and more complex challenges for risk management. Regulatory requirements remain uncertain in many areas as individual jurisdictions will implement, and potentially significantly revise, global rules such as Basel III. Geopolitical risk has risen with decelerating economic growth coupled with rising debt levels in China; the United Kingdom's departure from the European Union under Brexit; and continuing trade negotiations among the United States, China, the European Union, and other jurisdictions.

At the same time, the risk landscape is changing. While financial risks remain, nonfinancial risks (such as cybersecurity risk, conduct and culture risk, model risk, and third-party risk), which can be complex and difficult to quantify and manage, are increasing in importance.

This new environment demands that financial institutions rethink their traditional approaches in order to raise their risk management functions to a new level of effectiveness and efficiency. A key theme of the new approach is to move risk management from a reactive to a proactive role. As they reassess their approach to risk management and take steps to modernize risk management to meet the new environment, financial institutions should employ the following four levers to drive change.

- **Infuse risk management into strategy.** Rather than simply managing the risks that have been assumed after the fact, risk management should be an active participant in developing the institution's strategic plans and objectives, and in assessing the impact of new products and markets on its risk profile including its capital and liquidity position.
- **Focus on people.** Institutions need to ensure they have sufficient professionals with the skills to manage high-risk and complex activities, including addressing nonfinancial risks that are growing in importance such as cybersecurity risk and conduct risk. To engage employees throughout the organization, institutions need an active program to create a risk-aware culture that encourages ethical employee behavior, constructive challenges, appropriate incentives, and transparency.
- **Enhance the three lines of defense.** Institutions should reexamine their three lines of defense models to ensure they have clearly defined the risk management responsibilities of each line of defense, have eliminated any overlapping responsibilities, and have enabled business units to take full ownership of the risks in their areas.
- **Leverage emerging technologies.** The latest technologies—such as cognitive analytics, machine learning, natural language processing, and big data—have the potential to fundamentally transform risk management. In addition to reducing costs through automation, these technologies can also enhance the overall effectiveness of risk management by providing new capabilities such as building controls directly into processes, prioritizing areas for testing and monitoring, and identifying potential risk events in real time to allow preventive action to be taken.

For a discussion of the new environment for risk management and how financial institutions should respond, see Deloitte's report, *The future of risk in financial services*.

Economic capital

ALL THE FINANCIAL institutions participating in the survey calculate economic capital, which is a tool used to assess risk-adjusted performance and allocate capital. Respondents most often said their institution calculates economic capital for financial risk types such as *market* (87 percent) and *credit* (87 percent), and for *operational risk* (74 percent) (figure 10). Economic capital is calculated much less often for nonfinancial risk types such as *reputational* (22 percent), *model* (17 percent), *cybersecurity* (16 percent), and *conduct and culture risk* (6 percent). Risk management approaches to managing these risk types are still developing and face the challenge that relevant data is hard to access, making them difficult to quantify.

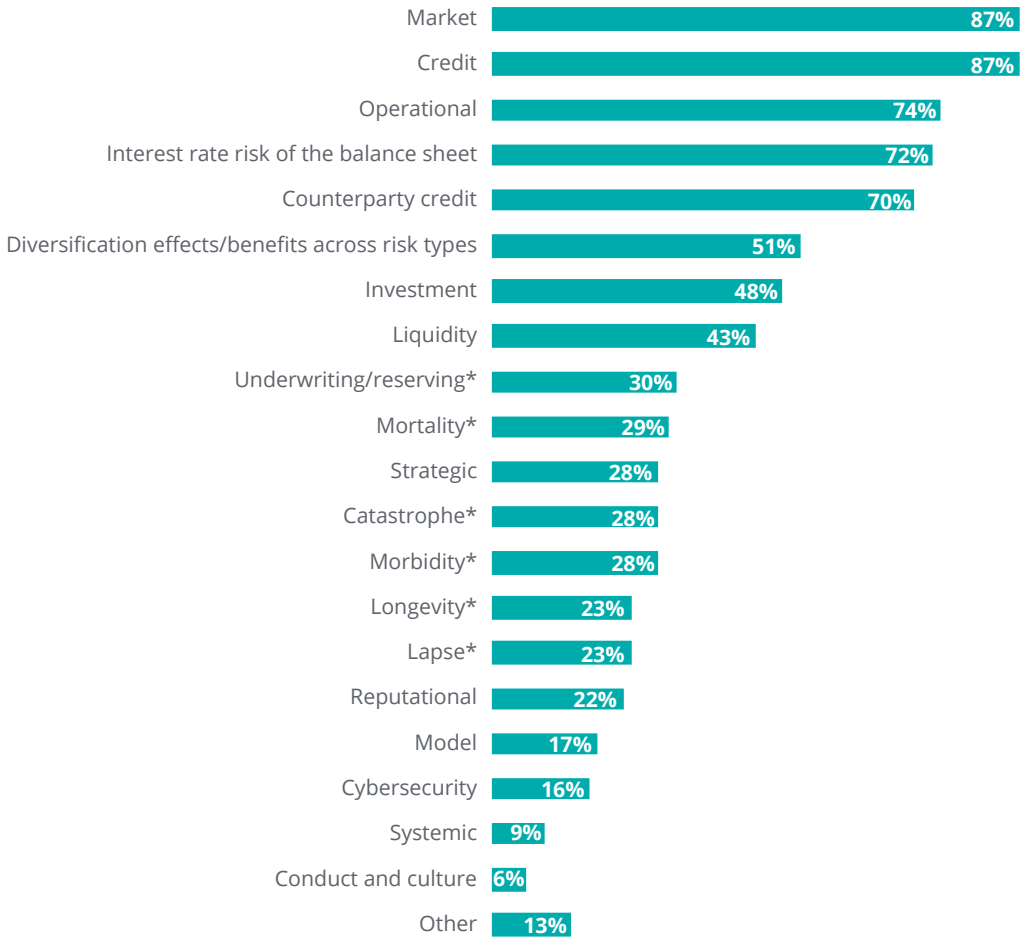
When asked how their institutions use economic capital, respondents most often said *to evaluate/allocate economic capital* (67 percent), which is down from 76 percent in the last survey, which shows that economic capital remains fairly widely used in allocating capital. The decline is likely attributable to greater use of stress testing by many organizations. The other areas in which respondents often said their institutions are using economic capital were *to support risk-based profitability analysis* (61 percent), *for strategic decision-making* (61 percent), and *for risk-based pricing* (60 percent).

In the wake of the financial crisis, economic capital was criticized for not performing as well as expected.

In the wake of the financial crisis, economic capital was criticized for not performing as well as expected. Economic capital was originally introduced as a more advanced method than the regulatory capital requirements that were in place. Since then, regulatory capital requirements have become substantially more sophisticated such as the CCAR stressed capital requirements, and institutions have come to rely more heavily on stress testing to assess financial resilience and increasingly to allocate capital to different businesses.

FIGURE 10

For which of the following risk types does your organization calculate economic capital?



*Only asked of organizations that provide insurance services.

Source: Deloitte analysis.

Stress testing

Capital stress testing

REGULATORS HAVE COME to rely increasingly on stress tests to determine if a financial institution has sufficient capital. The requirement that financial institutions conduct capital stress tests has been adopted by regulators around the world, including the US Federal Reserve, the Bank of England, the EBA, the European Insurance and Occupational Pensions Authority (EIOPA), the Japan Financial Services Agency, and the Australian Prudential Regulation Authority (APRA) in Australia.

Financial services institutions are increasingly relying on stress tests to assess capital adequacy.

European stress-testing requirements have been ratcheted up after criticism that earlier rounds were not sufficiently rigorous. In January 2018, the EBA released the scenarios against which the 48 largest banks in the European Union will be tested, which included a potential major recession with the economy shrinking by 8 percent by 2020 and residential property prices dropping by 27.7 percent.[41]

In 2018, the Dodd-Frank Act in the United States was revised to remove the requirement that banks with less than US$250 billion in assets be required to conduct stress tests, concluding that stress testing requirements were excessive for small and medium-sized institutions.[42]

Ninety percent of respondents reported using capital stress tests, up from 83 percent two years ago. The use of capital stress tests is nearly universal among large (97 percent) and mid-size institutions (93 percent), while somewhat less common among smaller institutions (71 percent).

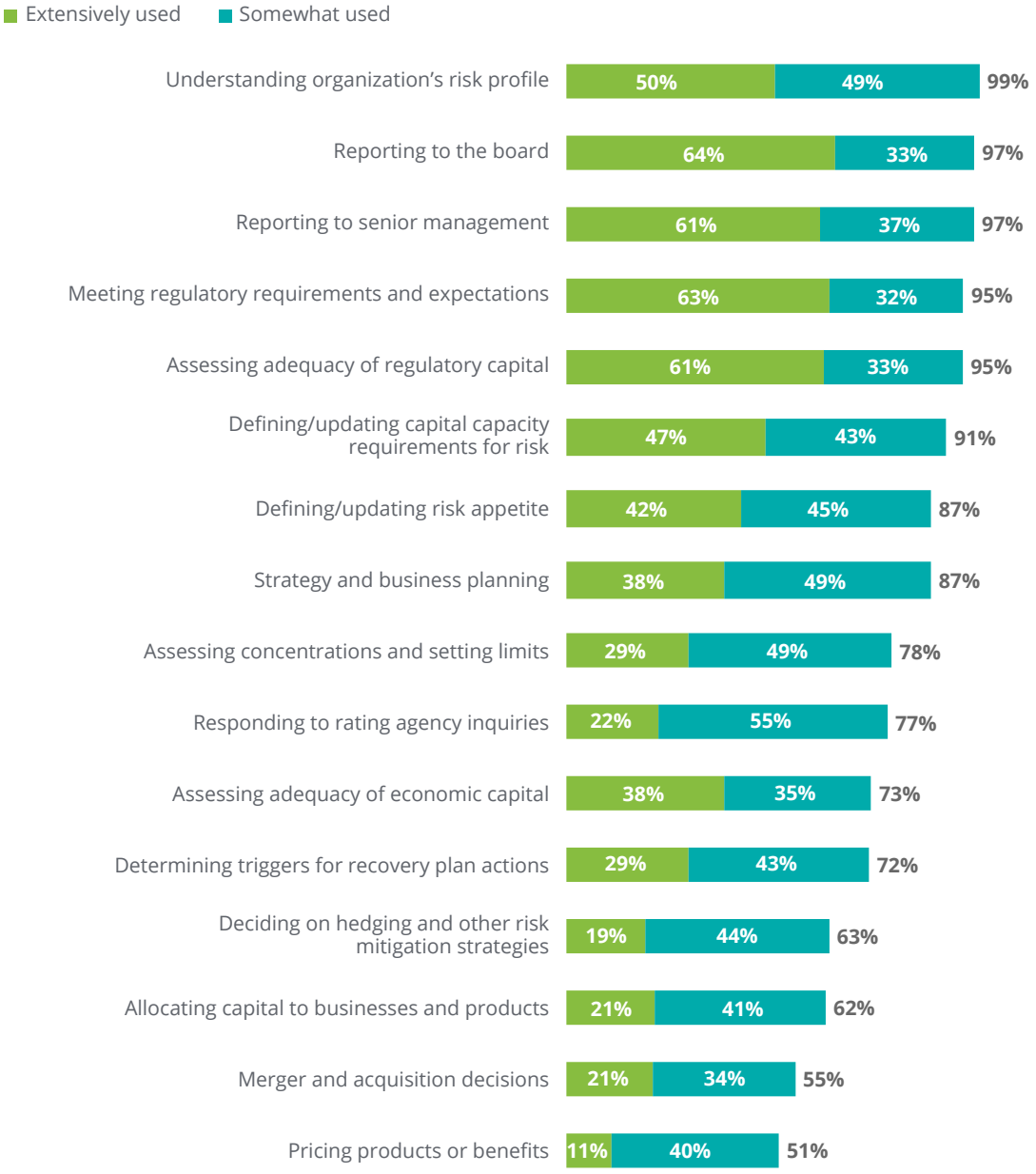
More than 90 percent of respondents who reported that their institutions use capital stress tests said they use them for *understanding the organization's risk profile* (99 percent), *reporting to the board* (97 percent), and *reporting to senior management* (97 percent).[43] Responding to regulatory requirements is a key driver in the use of capital stress tests, and almost all respondents said their institution uses this tool for *meeting regulatory requirements and expectations* (95 percent, including 63 percent that use it extensively), and *assessing adequacy of regulatory capital* (95 percent, including 61 percent that use it extensively) (figure 11).

Financial services institutions are increasingly relying on stress tests to assess capital adequacy. In many areas, significantly more institutions reported *extensively* using capital stress tests than was the case in the prior survey, including *reporting to the board* (64 percent, up from 46 percent), *reporting to senior management* (61 percent, up from 49 percent), *defining/updating capital capacity requirements for risk* (47 percent, up from 24 percent), and *strategy and business planning* (38 percent, up from 26 percent).

One indication of the increasing importance of capital stress tests compared to economic capital calculations is that while 87 percent of respondents said that capital stress tests were used for strategy and business planning, the comparable figure for economic capital was only 61 percent. On the other hand, economic capital is used more often

FIGURE 11

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



Note: Some percentages do not total due to rounding.

Source: Deloitte analysis.

for pricing products than is capital stress testing (61 percent versus 51 percent), which suggests that it remains more tractable than stress testing for certain applications.

Most stress testing requirements include both quantitative and qualitative requirements. In addition to employing quantitative methodologies to demonstrate that the institution has sufficient capital to pass capital ratio thresholds under

stressed conditions, institutions are also required to meet qualitative requirements indicating they have a strong risk management program with strong internal controls, documentation of policies and procedures, access to quality data, and a robust IT infrastructure.

Data management and IT capabilities can be especially challenging. Conducting capital stress tests requires an institution to aggregate data from different business units and functional areas. A capital stress-testing platform is also required, which typically is developed in-house since marketplace solutions primarily address specific components of the overall end-to-end functionality needed.

However, institutions appear to be increasing their capabilities in these areas since access to data and the IT platform were less likely to be considered extremely or very challenging in capital stress tests than they were two years ago. These included *data quality and management for capital stress testing calculations* (42 percent, down from 52 percent) and *capital stress testing IT platform* (for example, the ability to conduct various scenarios tailored to the group's profile more frequently and in a more granular manner) (41 percent, down from 66 percent).

Respondents were also less likely to report that they consider other issues to be extremely or very challenging in capital stress testing than they did two years ago, including *coordinating multiple functional areas and activities required to conduct capital stress tests* (for example, risk, treasury, business units, IT, developing and implementing models, and validating models) (29 percent, down from 48 percent), *implementing formal validation procedures and documentation standards for the models used in capital stress testing* (28 percent, down from 47 percent), and *developing capital stress testing methodologies/models accepted by regulatory authorities as part of supervisory stress testing exercises* (26 percent, down from 44 percent).

Further, the survey findings suggest that senior management has become more involved in the capital stress testing process with only 14 percent of respondents saying *active engagement by senior management and the board of directors in setting capital stress testing objectives, defining scenarios, and challenging methodologies and assumptions* was extremely or very challenging, down from 40 percent in the prior survey.

Liquidity stress testing

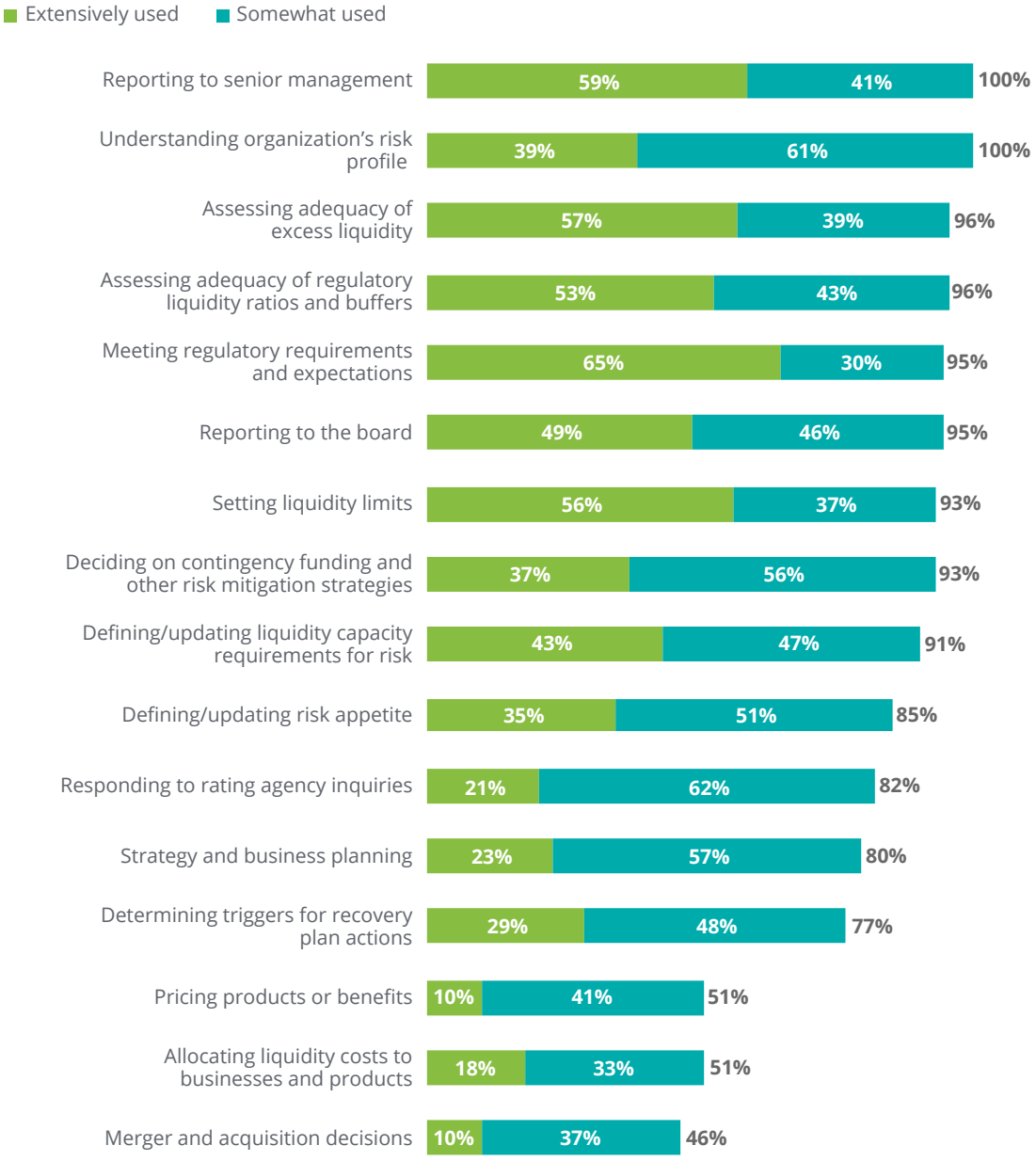
The focus by regulators on the importance of liquidity stress testing has paralleled that placed on capital stress testing. Liquidity risk was an important issue during the financial crisis, and the regulatory focus began with the Basel III requirements for the liquidity coverage ratio (LCR) and the net stable funding ratio (NSFR). Other regulators have established additional requirements for liquidity stress testing, such as the US Federal Reserve SR 10-6 and FINRA Notice 10-57 implemented eight years ago. Since this is an evolving area, institutions are still gaining experience with liquidity stress testing, and regulatory expectations are also still developing.

Liquidity stress testing is already widespread, with 87 percent of institutions reported using it, up from 82 percent in the prior survey. Most likely in response to regulatory requirements, banks (96 percent) most often reported conducting liquidity stress testing compared to investment management firms (86 percent) and insurance companies (76 percent). As expected, liquidity stress testing is also more common at large institutions (94 percent) than at mid-size (86 percent) or small institutions (76 percent).

All the respondents who reported that their institutions use liquidity stress testing said they use them for *reporting to senior management and understanding organization's risk profile* (figure 12).[44] Compared to the prior survey, liquidity stress tests are being used more extensively in several areas: *assessing adequacy of excess liquidity* (57 percent, up from 39 percent), *meeting regulatory requirements and expectations* (65 percent, up from 52 percent), and *setting liquidity limits* (56 percent, up from 44 percent).

FIGURE 12

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



Note: Some percentages do not total due to rounding.

Source: Deloitte analysis.

Fifty-one percent of respondents said liquidity stress tests are used by their institution for *determining triggers for recovery plan actions*, with only 29 percent saying they are used extensively. Liquidity stress tests can play an important role in recovery planning, and their use in this area is likely to grow over time.

Although liquidity stress testing is widely used in the same areas as capital stress testing, institutions tend to rely on it less. For example, 64 percent

of respondents said their institution uses capital stress testing extensively for *reporting to the board* compared to 49 percent for liquidity stress testing. Similarly, while 50 percent of respondents said that capital stress testing is used extensively for *understanding the organization's risk profile*, the comparable figure for liquidity stress testing was 39 percent. Regulatory expectations are likely to lead institutions to have liquidity stress testing play a more prominent role going forward including in monitoring liquidity risk.

Respondents cited a similar list of challenges for their institutions in using liquidity stress testing as they did for capital stress testing. As with capital stress testing, the two issues that respondents most often said were extremely or very challenging for their institutions when using liquidity stress testing concerned data and the IT infrastructure: *data quality and management for liquidity stress testing calculations* (30 percent) and *liquidity stress testing IT platform* (for example, the ability to conduct various scenarios tailored to the group's profile more frequently and in a more granular manner) (30 percent).

Access to data can be more difficult in capital stress testing since it typically has to be aggregated across more areas in the organization, while the data required for liquidity stress testing is often more centralized. This is reflected in 42 percent of respondents considering *data quality and management for capital stress testing calculations* to be extremely or very challenging, while 30 percent said the same about data for liquidity stress testing.

Having professionals with the required skills poses a challenge for both types of stress tests. Attracting and retaining risk management professionals with the required skills was considered at least somewhat challenging by 78 percent for capital stress testing (including 28 percent who considered it extremely or very challenging) and by 71 percent for liquidity stress testing (including 22 percent who considered it extremely or very challenging).

The survey results suggest that institutions are becoming more comfortable with liquidity stress tests, and for a number of issues, fewer respondents considered them to be extremely or very challenging than was the case in the prior survey: *liquidity stress testing IT platform* (30 percent, down from 45 percent), *coordinating multiple functional areas and activities required to conduct liquidity stress tests* (19 percent, down from 31 percent), *implementing formal validation procedures and documentation standards for the models used in liquidity stress testing* (14 percent, down from 30 percent), *liquidity stress testing analytics* (for example, scenario projections, loss calculations, and aggregation of results) (16 percent, down from 27 percent), and *developing detailed documentation of the methodologies, processes, and procedures for conducting liquidity stress tests* (15 percent, down from 25 percent).

Sector spotlight

Banking

AT THE END of 2017, the Basel Committee announced an agreement had been reached on revisions to the final Basel III capital framework, reforms that have been dubbed by some as "Basel IV." These updates have focused on the RWA treatment of credit risk, operational risk, and capital floors and will be rolled out along with revisions to capital requirements for market risk (Fundamental Review of the Trading Book (FRTB)).[45] The Basel Committee's revisions to FRTB include a specification of instruments to be assigned to the trading book and to the banking book, introduction of a capital add-on for risk factors that cannot properly be modeled due to insufficient data, changes to the standardized approach to incorporate risk sensitivities across asset classes and to align with front-office pricing and models, and a move from a Value at Risk (VaR)-based measure to an expected shortfall measure of risk under stress and incorporation of varying liquidity horizons.

A key aim of the proposed revisions is to address what the Basel Committee has described as "unwarranted and unwanted variation" in risk-weighted assets (RWAs) by improving the consistency and comparability of capital calculations, both across firms using internal models and between those using internal models and those employing standardized approaches.[46] The revisions restrict the use of internal models for certain regulatory capital calculations and set a standardized minimum output floor of the level of capital calculated by a bank's internal models at a minimum of 72.5 percent of the capital calculated by standardized approaches.

Internal models are often used to calculate the capital requirements of financial services institutions. For example, in the banking sector in the European Union, roughly one-half of the regulatory capital is calculated by internal models.[47] However, there are concerns about the accuracy of these calculations since internal models have been seen to produce different results for similar risks in different institutions. In addition, there have been concerns that employing internal models for capital adequacy may create inappropriate incentives for institutions to only develop models that lower their capital requirements.

Although the Basel Committee reached final agreement on the Basel III package in December 2017, its implementation in specific jurisdictions remains unclear. Fragmentation of regulation is a growing challenge for globally active banks as individual regulators are increasingly willing to vary prudential regulations for their jurisdiction. This divergence in regulatory standards creates additional costs and complexities for global banks as they attempt to design regulatory capital models without knowing whether these will comply with the rules that are ultimately adopted in individual jurisdictions around the world.

In 2017, the ECB started conducting its TRIM project to assess whether the internal models used by banks are reliable and comparable, with the goal of reducing inconsistencies and unwarranted variability between models when calculating their risk-weighted assets.[48]

The European Union is negotiating its "Risk Reduction Package" (which includes Capital Requirements Directive V/Capital Requirements Regulation II (CRD V/CRR II)), which may require some extended consultations. This process will delay the implementation of the Basel III framework, including FRTB. Beyond delays, EU legislators have demonstrated their willingness to alter the content of the Basel standards in important areas, in some

cases proposing substantial discounts to capital requirements.

Implementation has also been delayed in Asia-Pacific. Japan has not published proposals on the Basel Committee standardized approach to counterparty credit risk (SA-CCR) and decided not to implement the NSFR on January 1, 2018 as planned. The Hong Kong Monetary Authority (HKMA) decided to shift the implementation timeline for new standards on Interest Rate Risk in the Banking Book (IRRBB) from 2018 to January 1, 2019. During 2017, Australia, Singapore, and Hong Kong each announced that they will postpone implementation of FRTB.

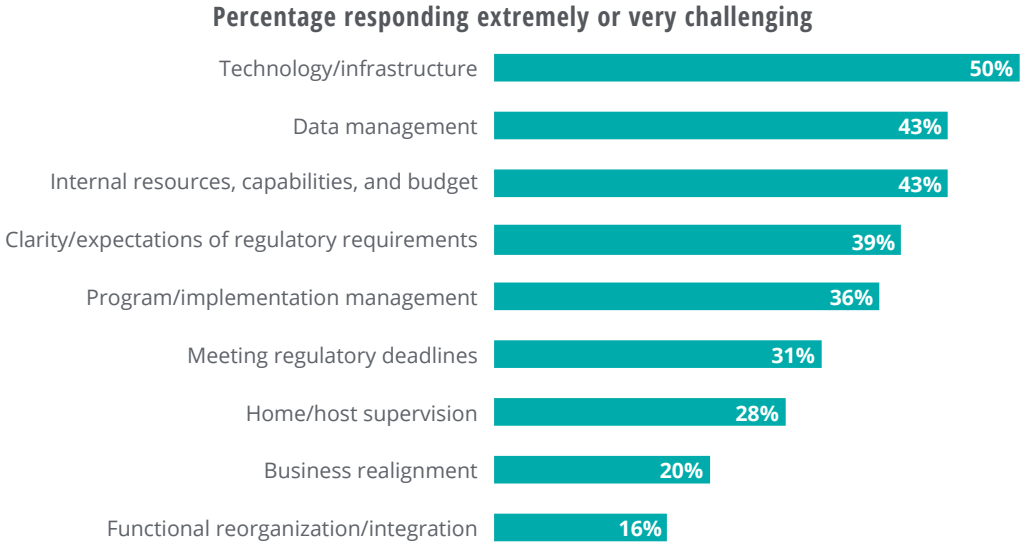
Given the implementation difficulties in most jurisdictions, the Basel Committee has delayed implementation of FRTB from January 2019 until January 2022. The additional time should provide banks with the opportunity to invest in the additional capabilities and technologies required.

Most respondents said their institutions still have substantial work to do to implement the FRTB rule. Only 9 percent of respondents said their institutions were already completely or substantially compliant with FRTB, while 39 percent said implementation was in progress. More than one-half of the institutions remain at earlier stages of implementation, either having *developed a project plan and approach* (24 percent) or currently studying the impact of the rule (27 percent). There appears to be more activity in this area among institutions in the United States/Canada, with 50 percent saying that implementation is in progress compared to 30 percent among both European and Asian institutions. The survey results indicate that many institutions will need to increase their efforts and the pace of implementation of FRTB.

As with many other aspects of risk management, two of the issues most often considered by respondents to be extremely or very challenging in implementing the FRTB market risk rules were *technology/infrastructure* (50 percent) and *data management* (43 percent) (figure 13). Securing adequate budget for the effort is also a concern, with

FIGURE 13

In your opinion, how challenging for your organization is each of the following aspects of implementation of the new Basel Committee market risk rules (resulting from the Fundamental Review of the Trading Book (FRTB) including the new standardized approach for counterparty credit risk and securitization)?



Source: Deloitte analysis.

43 percent of respondents citing *internal resources, capabilities*, and *budget* as being extremely or very challenging.

> "One of our continuing big challenges is in ensuring that we have high-quality data for use in our risk analyses and decisions, and dealing with the costs necessary to maintain this data."
>
> —Senior risk executive, large global diversified financial services company

Many respondents indicated that they believe more clarity is required in the FRTB requirements, and institutions are working with regulators to achieve this. Thirty-nine percent of respondents said their institutions find a lack of clarity and expectations of the FRTB regulatory requirements to be extremely or very challenging, although this is down from 54 percent in the prior survey.

Now that institutions have had an additional two years of experience with the FRTB rule, they appear to be improving their capabilities in other areas as well. A number of other issues were less likely to be rated as extremely or very challenging than they were two years ago, including *program/implementation management* (36 percent, down from 45 percent), *meeting regulatory deadlines* (31 percent, down from 45 percent), *business realignment* (20 percent, down from 40 percent), and *functional reorganization/integration* (16 percent, down from 31 percent).

Sector spotlight

Insurance

Regulatory and economic capital

INSURANCE COMPANIES ARE facing increased capital standards, with the most influential regime being Solvency II, which was developed by EU regulators. Around the world, insurance companies and regulators continue to develop capital metrics that are increasingly risk-focused. Many countries have drawn lessons from Solvency II, as seen in Europe, Asia-Pacific, and the Americas. Additionally, the focus on capital adequacy requirements has been raised through efforts such as the IMF's Financial Sector Assessment Program.[49] Examples of new developments include the United States where, for the first time, a Group Capital Calculation is in development.

Around the world, insurance companies and regulators continue to develop capital metrics that are increasingly risk-focused.

Solvency II is more complex in its approach to regulatory capital calculations than some non-European countries, with the allowance and in some cases capital benefit of an internal capital model. Many insurers have applied for supervisory approval of internal capital models since the introduction of Solvency II in 2016. Sixty-eight percent of the aggregate insurance industry Solvency Capital Requirement in the United Kingdom is by insurers using internal models in whole or in part, while the figure for Germany is 82 percent and in France, 25 percent.[50]

As in the banking sector, there are concerns whether internal models are adequately assessing risks. Studies by the ECB's EIOPA have found high variability in the output of internal models. EIOPA is expected to issue further guidance in 2018 on internal model convergence, which can help provide methodological and quantitative expectations for approved internal models. EIOPA will deliver its final advice on Solvency II to the European Union in 2018. The use of a hard floor is likely to be considered for the insurance sector, similar in concept to the output floor adopted by the Basel Committee for banking.

There are also concerns whether the use of internal models encourages institutions to only design changes to their models that reduce capital requirements. Regulators will expect companies to provide a detailed, risk-based justification to secure approval for model changes.

Among the insurance companies participating in the survey, 40 percent were subject to Solvency II requirements. Other regulators are looking to Solvency II as a model, and 24 percent of respondents said their institutions were subject to regulatory capital requirements similar to Solvency II. Solvency II or similar requirements are most prevalent in Europe, where 91 percent of respondents said their institutions were subject to Solvency II and the remaining respondents said they were subject to similar requirements. In contrast, in the United States/Canada and in Asia-Pacific, 56 percent of

respondents said their institutions were not subject to Solvency II or similar requirements.

Respondents cited a wide range of issues as areas in which their institutions are planning to focus over the next two years related to Solvency II or similar regulatory capital requirements, with *scenario analysis* (70 percent) and *enhancements to risk tolerance and risk appetite* (63 percent) cited most often.

Reflecting two additional years of experience with Solvency II, there were several areas where fewer respondents said their institutions were planning to focus than was the case in the prior survey. These include *Own Risk and Solvency Assessment* (ORSA) (48 percent, down from 56 percent), *management information* (39 percent, down from 53 percent), *risk quantification* (35 percent, down from 47 percent), and *training* (30 percent, down from 41 percent).

Insurance companies appear to have made progress in addressing the data challenges of Solvency II. In 2016, 63 percent of respondents said their institutions were planning to focus on *data infrastructure and data handling processes*, making it the issue cited second most often. In the current survey, this issue was cited as a priority by 48 percent, making it the item cited fifth most often.

The IAIS is working to develop an ICS with the aim of allowing insurers to operate across borders more efficiently, reduce costs, and bring benefits to consumers. Among the important issues that will need to be addressed are:

- Either defining a single valuation basis, or if this is not possible, achieving comparability between a market-adjusted valuation (MAV), which is consistent with Solvency II, or a GAAP with adjustment (GAAP Plus), which generally reflects the approach used by shareholder-owned insurance companies in the US market.
- The role that internal models will play in determining capital requirements.
- Resolving the purpose of Margin Over Current Estimate, which is analogous to the risk margin under Solvency II, and its interaction with capital requirements.

At its annual conference in 2017, the IAIS agreed that the future ICS version 2.0 will be implemented in two phases. For the first five years, the ICS will be used for confidential reporting to the group supervisor and for discussions in supervisory colleges and will be calculated using MAV, although GAAP Plus can also be reported if the group supervisor chooses to do so. At the end of the five-year monitoring period, the ICS will be implemented as a Prescribed Capital Requirement, which is theoretically a suitable basis for triggering supervisory action, although it remains to be seen how it will interact with, or sit alongside, existing capital standards, such as Solvency II.

Respondents were asked what impact they expected for their company from the global regulatory capital standards being developed by the IAIS. Respondents most often considered the *insurance capital standard* to have at least a somewhat significant impact (62 percent), although only 29 percent expected the impact would be extremely or very significant.

The two other issues in which respondents most often expected at least a somewhat significant impact were *basic capital requirement and high loss absorbency standards* (59 percent, with 24 percent extremely or very significant) and *recovery and resolution planning* (52 percent, with 18 percent extremely or very significant).

Another important development was the publication in May 2018 by the International Accounting Standards Board of International Financial Reporting Standards (IFRS) 17, which will be effective for periods beginning on or after January 1, 2022. The new standard requires insurance liabilities to be measured at a current fulfillment value and is designed to provide a more uniform measurement and presentation approach.[51] IFRS 17 will require vast changes across operating models, processes, and technology to allow insurance companies to comply with the new requirements in how insurance con-

tracts are accounted for, recognized into income, and presented in financial statements. There have been industry proposals that the requirements be simplified and that the implementation date for IFRS 17 be delayed.

Assessing insurance risk

Respondents said their institutions use a variety of methods as either a primary or secondary methodology to assess insurance risk. Roughly 90 percent or more of respondents cited *regulatory capital*, *stress testing*, *actuarial reserving*, *claims ratio analysis*, *internal capital framework/model*, and *economic capital* (figure 14). With the focus on Solvency II and similar regulatory initiatives to assess capital adequacy, the method most often cited as a primary methodology was r*egulatory capital* (72 percent).

Insurance companies appear to be using a wider range of methods to assess insurance risk than respondents said was the case two years ago, including *value at risk* (76 percent, up from 53 percent), *value of new business* (76 percent, up from 46 percent), *asset adequacy analysis* (71 percent, up from 50 percent), *dynamic financial analysis* (68 percent, up from 40 percent), and *stochastic embedded value* (66 percent, up from 26 percent).

The methods employed to assess risk vary by company size. For example, *stress testing* is used more often by larger insurers. *Stress testing* is used as a primary methodology by 65 percent of the largest insurers, compared to 50 percent of mid-size and 20 percent of smaller insurance companies. *Economic capital* is also used much more often as a primary methodology by the largest insurers (71 percent) than by mid-size (31 percent) or small insurers (33 percent). Both methods require the resources and sophisticated capabilities to create internal capital models.

In contrast, *value at risk* is more often a primary methodology at small insurance companies (60 percent) than at mid-size (31 percent) or large companies (44 percent). *Claims ratio analysis*, a simpler technique, is also more often a primary methodology at small insurers (75 percent) than at mid-size (46 percent) or large companies (56 percent).

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

Among the insurers that conduct stress testing to assess insurance risk, respondents most often said that testing is performed on two financial risk factors where it is relatively easy to apply: *market risks* and *interest rate risk* (84 percent each). The next most common risk factors were *mortality* (66 percent), *property and casualty claim cost* (58 percent), *morbidity* (58 percent), *expense* (53 percent), and *lapse* (53 percent).

> "We are embracing AI and predictive analytics, for example, in areas like monitoring customer behavior and potential fraud issues as well as applying robotics to automate manual policy processing tasks."
>
> —Senior risk executive, major insurance and asset management company

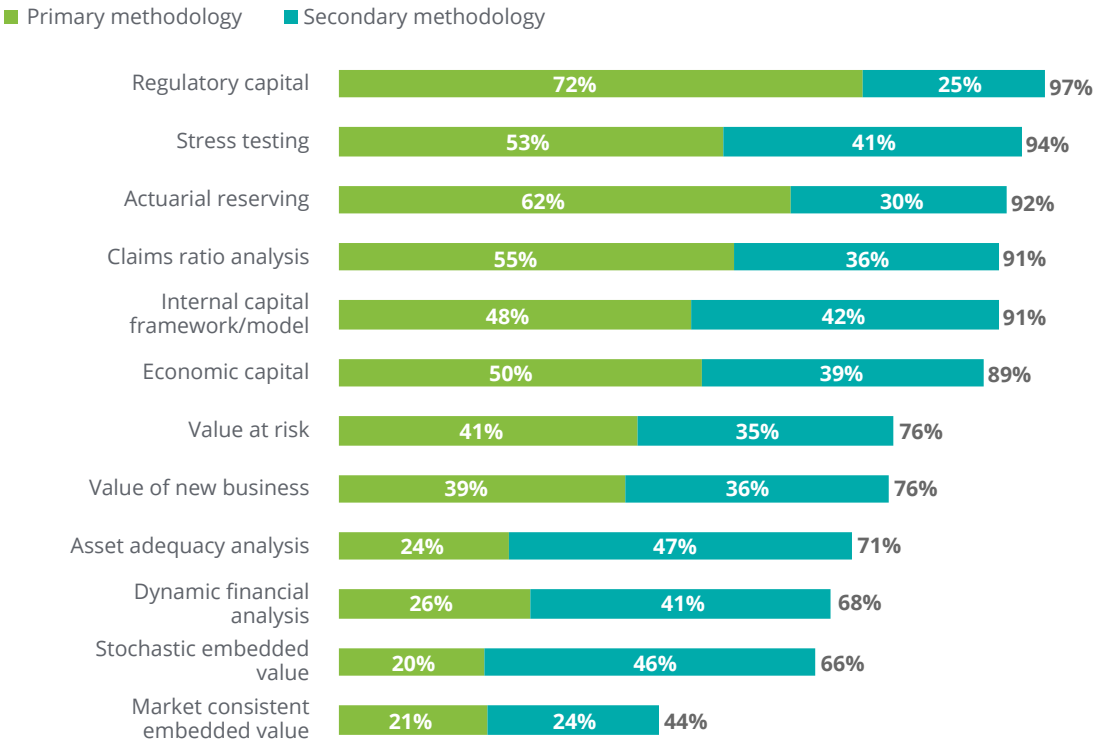
Insurance companies will also need to focus on the risks created by new technologies. AI and risk analytic technologies are expected to enhance pricing and underwriting capabilities, thereby improving risk selection/portfolio structures and risk

diversification, enabling new products and business models, and allowing real-time risk assurance, while streamlining operations. Yet these technologies will create their own risk management issues. For example, the increased use of AI-powered real-time claims processing will demand new types of fraud risk management, including real-time detection. The increased level of personalization allowed by these technologies, such as in price and cover, create the potential for customer pricing issues and socioeconomic impacts, which might lead to additional regulatory requirements regarding the use of data and AI algorithms. (See the section, "Risk management information systems and technology.")

FIGURE 14

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

Base: Organizations that provide insurance/reinsurance services



Note: Some percentages do not total due to rounding.

Source: Deloitte analysis.

Sector spotlight

Investment management

THE INVESTMENT MANAGEMENT sector comprises a range of organizations that provide investment management products and solutions, from large global firms that have a diversified product lineup and access to significant distribution channel network to niche managers that have targeted products in an asset class. In their investment management activities, these firms engage with clients to determine investment goals and risk tolerances and then manage customer financial assets in an effort to achieve or exceed their goals.

Clients of investment management firms include both individual retail investors, who may have limited financial knowledge, and institutional clients, who continue to grow in sophistication, understanding, and monitoring of their investment portfolios. The wide range in the types of clients creates a complex set of risks to manage. Firms need to adopt risk management priorities that align with their client mix and investment approach.

The operating environment for the investment management industry continues to be challenging. In particular, investors are favoring low-cost investment solutions, while at the same time, customer preferences and technology innovation are evolving. Competitive pressures are driving investment management firms to take strategic decisions designed to grow assets, efficiently and effectively run operations, and deliver a superior customer experience. Because of these trends, firms are reevaluating their technology capabilities to align with their growth plans, as the shift to AI and alternative data requires more and different capabilities and skill sets than in the past. They are also broadening their product reach, consistent with their capabilities, to better serve the preferences of clients and distributors. The survey results described below illustrate the risk management challenges investment management firms face in understanding and mitigating a broad range of enterprise risks including operational, strategic, technology/cyber, financial, regulatory, and external market pressures, to name a few.

Current focus of risk managers and executives in the investment management industry

Similar to the risk management challenges found in other sectors, data and technology were the issues most often rated by respondents at investment management firms as extremely or very challenging: *use of alternative data in investment and operational processes* (for example, social media, payments, crowdsourcing, geospatial, and cognitive analytics) (54 percent), *data management and availability* (53 percent), and *IT applications and systems* (47 percent) (figure 15).

The concern over *data management and availability* has grown, with 53 percent of respondents rating it as extremely or very challenging compared to 36 percent in 2016. The challenges presented by *IT applications and systems* remained fairly steady, with 47 percent considering it extremely or very challenging compared to 50 percent in 2016.[52]

With more observers considering the rising risks in the financial system, it is notable that 24 percent of respondents considered *preparing for and responding to enterprise events (that is, crises)* to be extremely or very challenging for their firm.

In some areas, investment managers were less likely to consider certain risks extremely or very challenging. These include *managing market risk*

FIGURE 15

In managing risks in your organization's investment management business, how challenging is each of the following?

Base: Organizations that provide investment management services

Source: Deloitte analysis.

and its impact on portfolio construction risk (19 percent), *risk governance* (19 percent), *managing risks to organizational reputation* (17 percent), and *managing liquidity risk* (14 percent). This may be due to investment managers' long history of managing assets, including their reputation.

Respondents were asked about the challenges their firms face in responding to new and emerging regulations such as the SEC's mutual fund modernization and the liquidity rules. Two of the issues that many respondents considered to be extremely or very challenging concerned their firm's data and IT infrastructure: *ongoing data collection, validation, aggregation, and filing with the regulatory authorities* (54 percent) and *enhancing technological capabilities to meet complex requirements* (54 percent).

Similarly, roughly one-half of respondents also said their institutions faced the broader challenges with regard to their compliance programs, specifically *enhancing systems and processes to meet new or revised regulatory requirements* (51 percent) and *enhancing infrastructure and increasing resources with respect to people, process, and technology* (49 percent).

Risks posing the greatest challenges in the next two years

When respondents were asked which three risk types present the greatest challenges for their organization's investment management business over the next two years, *cybersecurity* was named far

more often as one of the top three risks (60 percent) than any other risk, including 23 percent who ranked it as the number one challenge (figure 16). This is a notable change from two years ago, when 28 percent of investment management respondents considered cybersecurity to be one of their three greatest challenges and only 3 percent ranked it as the number one challenge. This may be due to a number of developments, including global regulators' adoption of increased privacy protections and penalties, coupled with a rise in the number of cyber incidents.

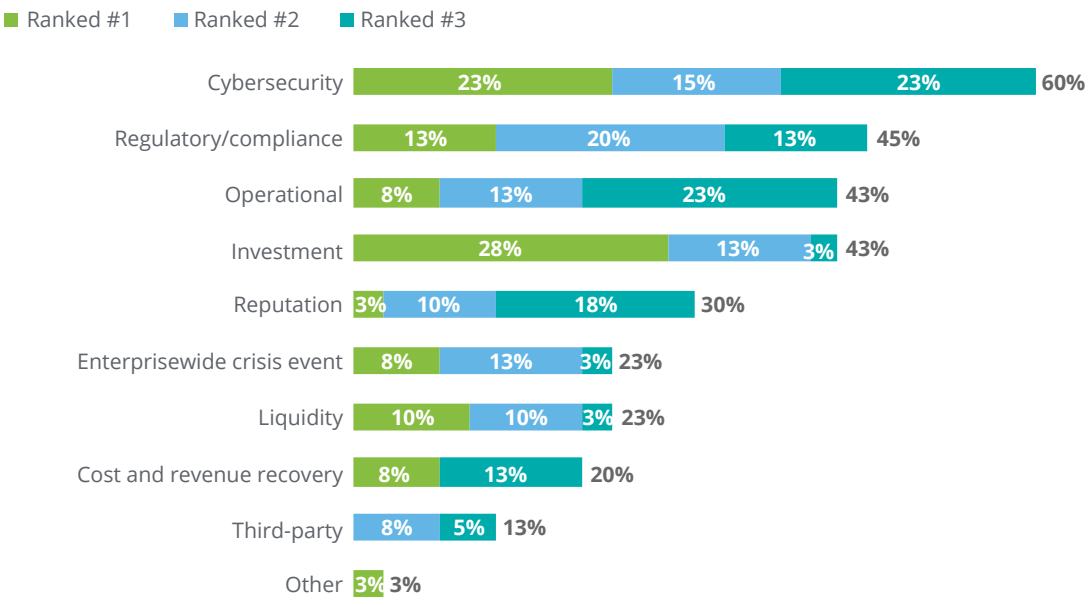
With the slower pace of new regulations being issued, 45 percent of respondents named *regulatory/compliance* as among the three most challenging risks, down from 81 percent two years ago, while 13 percent considered it to be the number one challenge, down from 28 percent. Despite the slower pace of new regulations, a number of regulations were passed in the last two years that affect the ability of investment management organizations to operate globally. These regulations require investment management firms to evaluate their businesses to respond and adopt programs to comply, including MiFID II, liquidity risk management regulations and guidance (for example, as issued in the United States, United Kingdom, Canada, and Hong Kong), and new privacy regulations (for example, General Data Protection Regulation in Europe and California's Consumer Privacy Act). In addition, enforcement activities continue to cause additional regulatory pressure points for investment managers, including but not limited to, conflicts of interest, disclosures, allocation of fees, and use of soft dollars for research.

The risk type that was rated third most often as among the three most challenging risk types to manage over the next two years was *investment risk* (43 percent), which was a sharp drop from 72 percent in 2016. However, 28 percent of respondents rated managing *investment risk* as their number one challenge, as it was in the 2016

FIGURE 16

Over the next two years, which are the three risk types that you believe will present the greatest challenges in your organization's investment management business?

Base: Organizations that provide investment management services



Note: Some percentages do not total due to rounding.

Source: Deloitte analysis.

survey, which is understandable since managing investment risk (portfolio construction, market risk, credit risk, and liquidity risk) is central to the business and value proposition for clients of investment management firms. Thirty percent of respondents considered *reputation* one of the three risk types that will present the greatest challenges over the next two years, while 43 percent ranked it in the top three.[53]

Emerging risks in investment management

Respondents ranked the top three emerging risks about which their firm is most concerned with respect to its investment management business. The issue that was most often ranked among the top three concerns was *fee pressure* (51 percent, with 22 percent ranking it as number one). Competitive pressures in investment management, coupled with changing investor preferences and aging organizational infrastructure, are likely to lead to a continued compression of margins at many investment management organizations. For example, there has been a pronounced and accelerated shift in assets toward low-cost passive management, and the fee wars between active and passive funds reached a new level in 2018 as firms begin to introduce index funds that do not have any management fees. To maintain profitability, it will be important for active managers to have a coherent business model and pricing response to the growing popularity of passive investments and be able to offer differentiated products that consistently deliver strong returns relative to passively managed alternatives. Fee disclosures are becoming more transparent, and asset managers will need to generate strong alpha to justify their charges to investors.

To combat margin compression, organizations continue to focus on enhancing activities that drive value creation such as developing products and solutions that deliver premium investment quality and innovative investment solutions to meet changing investor preferences. Investment firms continue to seek strategic acquisition or divestiture activities to improve profitability and increase margins. In addition, organizations continue to analyze the cost and resources dedicated to value-protective activities (such as compliance and operations) to determine whether those services are achieving the expected return. Many organizations may find that the resources they dedicate to compliance and operations have resulted in these processes being over controlled relative to the risks that they face from these and other processes, thereby impacting their margins. Matching risk to reward and expected returns, and allocating resources accordingly for value protective activities, can provide investment management organizations with the ability to be more agile in how they operate and maintain an acceptable level of risk that also results in potential cost savings.

In addition, organizations are looking at recovering potential costs and enhancing revenue recognition to improve their bottom line. In order to provide better transparency, improved performance, and the ability to recover overpaid expenses/underreported revenue and reduce future costs, organizations continue to focus on the extended enterprise (third-party) relationships, in addition to optimizing people, process, and technology.

These themes are consistent among the risks that investment management respondents frequently ranked among the top three emerging risks: *changing client preferences* (for example, demand for solutions in passive and alternative strategies) (51 percent) and *growth of digital investing platforms and advice* (robo-advisers) (43 percent). Both issues contribute to fee compression, which impacts an investment manager's strategic positioning and competitiveness.

Other emerging risks that were ranked by a significant portion of respondents as among their three greatest concerns with respect to investment management were *regulatory change* (49 percent), *reputation risks* (30 percent), and *distribution relationships/channels* (27 percent). In addition, somewhat surprisingly, 19 percent of respondents cited *global financial crisis* as one of the top three

concerns, including 14 percent who ranked it as their number one concern.

Oversight of investment risk

Respondents cited a wide range of roles and responsibilities assigned to the individual or individuals responsible for the oversight of investment risk in their firms. The responsibilities cited most often were *meet regularly with governance committees responsible for overseeing investment risk management* (83 percent, up from 72 percent in the prior survey) and *develop and implement the investment risk management framework, methodologies, standards, policies, and limits* (83 percent, up from 78 percent). Both results suggest that investment management firms are implementing more significant governance and oversight of the investment risk process. This should come as no surprise since there is growing attention on how firms govern, manage, and monitor their models, including algorithms. Many firms require improved governance and controls as investment managers are increasingly using models to drive their business. Firms should design a structured approach to managing model risk, whereby roles and responsibilities are defined, models are inventoried and documented, effective controls are designed and implemented, and policies and procedures are developed to establish protocols for change management, and for escalation and disclosures should a model issue arise.

Other responsibilities cited frequently were *monitor compliance with investment guidelines related to investment risk* (such as tracking error, value at risk, expected shortfall, and sector/industry exposures) (73 percent), *periodic re-assessment of investment risk to identify risk concentrations and potential style drifts* (70 percent), *prepare scenario analysis to provide forward looking analytics on risk exposures* (68 percent), and *manage stress testing process including governance, methodology, and reporting* (68 percent).

Firms were least likely to give the individual with oversight of investment risk the responsibility to *provide input to the day-to-day investment decisions (e.g., transactions) that impact the risk profile* (45 percent). At most firms, the executive responsible for investment risk is concerned with oversight of the investment risk management process and serving as an effective challenge mechanism to the portfolio management function.

Managing liquidity risk in investment management

Managing liquidity risk has received significant focus from shareholders, key stakeholders (such as investment consultants), fund boards, and global regulators. In addition, it has become a strategic focus because of the potentially devastating impact to fund and investment managers' brand and reputation if they fail to meet shareholder redemption requests. Liquidity risk management has become a greater focus of regulators of investment management firms. When the SEC adopted the Liquidity Rule (Rule 22e-4 under the Investment Company Act of 1940), it was designed to promote better liquidity risk management by registered investment companies, including exchange-traded funds (ETF). The Liquidity Rule requires funds to establish liquidity risk management programs and specifies the elements that such a program should include, although it exempts money market funds and certain ETFs from some of the requirements. Funds will be required to classify portfolio holdings into one of four buckets, based on how quickly the securities in each could be converted into cash. Investment complexes with more than US$1 billion in assets must comply with this provision beginning June 1, 2019, while smaller firms have until December 1, 2019. Investment management firms continue to advance in developing their programs. Among the issues that firms are facing is who within the firm should assess liquidity when there are one or more sub-advisers within a single portfolio.

Despite this array of challenges, liquidity risk for investment risk has become a more mature risk type, and relatively few respondents considered issues to be very challenging in this area currently. Three issues were rated by roughly one-quarter of respondents to be challenging or very challenging: *deploying system/technology capabilities to facilitate liquidity analysis (or selecting a vendor solution) necessary to facilitate liquidity calculations and ongoing monitoring* (26 percent), *classifying fund asset liquidity, including determining the assumptions and parameters used when bucketing holdings* (26 percent), and *developing methodologies to facilitate product liquidity assessments throughout the product lifecycle* (23 percent). Other issues were considered by even fewer respondents to be extremely or very challenging: *aggregating liquidity classification information* (18 percent), *identifying and memorializing liquidity risk management practices used to develop, monitor, and assess portfolio liquidity* (for example, policies, playbook) (13 percent), and *enhancing transparency to investors through additional disclosures and articulation of liquidity risk management practices* (13 percent).

As it relates to classifying fund asset liquidity, our experience shows that when classifying fund assets, having access to quality data is paramount. This requires centralizing certain fund data (such as portfolio holdings and fund flows) and enriching it with market data. In addition, classifying securities requires the investment risk management function, working in conjunction with the portfolio management function, to understand what it would reasonably expect to trade during normal and stressed periods, how long it would take to liquidate all or a portion of a position, transaction cost limits (how much liquidity is a fund willing to pay for), and the typical amount of time it takes to settle a transaction in any given security.

In addition, classifying securities and performing ongoing monitoring of liquidity risks are best facilitated via a technology or application that can bucket the securities, provide workflow tools to identify and escalate issues, and offer reporting and ongoing trend analysis on the liquidity profile of a fund. Based on our experience, fund managers are building applications and data warehouses to facilitate the ongoing monitoring of liquidity risks and connecting them to third-party analytic tools that facilitate the asset classification. Having a clear understanding of the needs of the various upstream and downstream stakeholder groups, and documenting those requirements, is critically important to determine if the organization will build its own solution or subscribe to a third-party solution.

Operational risk management for investment management

When asked to name the top three risk types that will pose the greatest challenges to their organization's investment management business over the next two years, 43 percent of respondents cited *operational risk*. In specific aspects of operational risk management, by far the issue most rated as being extremely or very challenging was managing cybersecurity risk: *responding to rising threat of cybersecurity risk and its impact on the confidentiality, availability, and integrity of data and information* (73 percent). Concerns over hackers and other cybersecurity risks have been growing rapidly as indicated by this issue rising from 50 percent in the 2016 survey. Data is a key challenge for the organization and a potential source of risks when not properly managed. Defining, establishing, and monitoring data governance and management principles are imperative to provide "gold standard" data as a trusted asset to portfolio managers and clients, supporting business operations and desired analytics use cases. Key principles include the implementation of a dedicated data platform, fully integrated with other systems, the formalization of a well-defined data management strategy (for example, sourcing and distribution), and establishment of strong governance.

The issue cited next most often as extremely or very challenging concerned data: *maintaining reliable data to quantify operational risk and drive*

risk-based decisions (45 percent, up from 33 percent in 2016). Several other operational risk issues were considered by one-quarter of respondents or more to be extremely or very challenging: *identifying emerging risks and risk trends to allow for nimble and effective response* (33 percent), *securing the appropriate resources to address risks with the highest priority* (33 percent), *understanding and managing operational risk associated with new business initiatives* (28 percent), and *designing procedures and measuring the effectiveness of internal controls to manage operational risks* (25 percent).

Extended enterprise risk

Investment management firms rely on a variety of third-party service providers, and many firms in the sector employ a heavily outsourced model. For example, participants in the sector may outsource the day-to-day management of client investments to investment sub-advisers, relying on third-party providers to manage whole or discrete operational processes, or employing a number of service providers that provide technology applications, data, and data enrichment services. It is common for a firm's third-party service providers, in turn, to subcontract to additional providers. If a risk event occurs at any of these providers or subcontractors, it can disrupt the investment management firm's operations and potentially inflict severe financial, operational, and reputational damage. Among the many risks and reputation-impacting crises that can arise from a firm's third-party relationships are business disruption, misuse of information, theft of intellectual property, service failure, or a regulatory breach. If one of its vendors or their subcontractors fails to execute their responsibilities, or engages in inappropriate conduct, the investment management firm would likely be affected by customer and investor perception and lead to reputational harm.

Three-quarters of investment management respondents said they considered oversight over third parties to be challenging, including 40 percent who said it was challenging or very challenging, up from 25 percent in 2016. Regulators are increasingly focused on the risks involved in these third-party service provider relationships, and 49 percent of respondents considered *increasing oversight over third-party service providers regarding the availability and timeliness of data* to be extremely or very challenging.

Effectively managing third-party risk requires a comprehensive ongoing monitoring program to review the risks from these relationships and the effectiveness of the controls that are in place. Respondents most often said their firms review the risks from these relationships annually, with this being most common for intermediaries (46 percent), administrators (45 percent), application technology vendors (44 percent), reference data providers (39 percent), infrastructure technology vendors (39 percent), and custodians (38 percent). Reviewing the risks from these relationships monthly or quarterly was most often mentioned for prime brokers (36 percent) and transfer agents (36 percent). (See the section "Operational risk," which discusses management of third-party risk across financial sectors.)

Data and analytics

Emerging technologies such as RPA, big data, cloud computing, cognitive analytics, natural language processing, and machine learning promise greater efficiency and also increase the ability to identify potential risk events (for example, by analyzing employee communications to identify potential insider trading). Recent advances have improved the feasibility of advanced analytics, making this a primary focus area for many asset management firms seeking profitable and sustainable growth. Gains in computing power and software have made it easier to manipulate both internal and external data sets while visualization and mobile tools allow firms to present insights more quickly in an accessible format. Ultimately, advanced analytics provides faster access to key insights and

information to enable improved decision-making and enhance the business value for investment managers, by evolving the focus from hindsight (what happened), to insight (what should we do), to foresight (what will happen). In addition to being seen as a powerful tool to streamline processes and reduce operational costs, firms that invest in advanced analytics are seeking retention and growth of client relationships, as well as enhanced portfolio management decision-making (for example, leveraging collective intelligence).

> "The information explosion creates the need for more quants, data scientists, and analysts in the risk group of the future. We will need to change the makeup of our team to bring on professionals who have these skills and are digitally native."
>
> —Chief risk officer, major asset management company

Most respondents said their investment management firms were extremely or very likely to enhance their data and analytics capabilities to improve performance in a number of areas of their investment management businesses. The area where respondents most often said this was extremely or very likely was *portfolio management* (74 percent), which is understandable since this is central to the business of investment management firms. The other areas cited often were *client engagement* (66 percent), *operations* (such as back and middle office) (56 percent), and *product innovation* (54 percent). In two additional areas, just under one-half of respondents thought it was extremely or very likely their firms would enhance data and analytics capabilities: *market research* (49 percent) and *capital market activities* (49 percent).

Management of key risks

Key risks looking forward

GIVEN THE RAPIDLY evolving risk environment and the focus on the future of risk management, respondents were asked which three risk types they believed would increase the most in importance for their institution over the next two years. There was broad consensus: *Cybersecurity* was named by 67 percent of respondents as one of the three risk types that would increase the most in importance, including 40 percent who named it as number one, far more than for any other risk type. Cybersecurity risk has received increased attention from regulatory authorities recently, spurred by numerous cases of hacking and other misconduct, often targeting financial institutions. (See the section, "Cybersecurity risk.")

Forty percent of respondents named cybersecurity as the risk type that would increase the most in importance—far more than any other risk type.

Although *cybersecurity* was also named most often in 2016, in the current survey more respondents considered it as one of the three risk types that would increase most in importance (67 percent, up from 41 percent) and respondents cited it as the number one risk more frequently (40 percent, up from 18 percent).

The risk type named next often as one of the three that would increase the most in importance over the coming two years was *strategic* (27 percent, with 12 percent naming it as number one). The heightened focus on strategic risk is consistent with the current uncertainty and unevenness in the global business environment and markets. *Regulatory/compliance* was named third most often among the top three risk types (25 percent), although this was down from 36 percent in the prior survey. While the financial services industry must comply with extensive regulatory requirements, the pace of regulatory change has abated in the current environment.

With the need for access to quality, timely data for risk management, 23 percent of respondents cited *data integrity* among the top three risk types that would grow in importance, up from 13 percent in the prior survey. Another area that has received more regulatory focus is *conduct and culture*, which was cited by 20 percent of respondents as among the three risk types that would grow the most in importance.

Effectiveness of risk management

When asked to assess the overall effectiveness of their institution in managing risk, 82 percent of respondents considered it to be extremely or very effective, an increase from 69 percent in 2016. This may reflect that institutions have now had more experience in implementing the changes to risk management that have been put in place in the post-crisis period in response to a series of new or revised regulatory mandates or guidance.

Confidence was highest in the United States/Canada, where 89 percent of respondents con-

sidered their institutions to be extremely or very effective in managing risk, compared to 79 percent in Europe and 63 percent in Asia-Pacific.

Respondents most often rated their institutions as extremely or very effective when it came to managing financial risk types such as *market* (92 percent), *credit* (89 percent), *asset and liability* (87 percent), and *liquidity* (87 percent). Institutions have lengthy experience managing these financial risks, with well-developed models and analytics, and access to relevant data.

When it came to the broad category of nonfinancial risks, however, respondents gave their institutions lower ratings. Although risk management programs have addressed the nonfinancial risks grouped as *operational risk* for some time, fewer respondents (56 percent) felt their institutions were extremely or very effective in this area. Managing operational risks has posed ongoing challenges in gaining access to required data and developing models, risk assessments, and controls.

Other nonfinancial risk types pose even greater challenges. Regulatory expectations are less well-defined, methodologies are less sophisticated, and gaining access to relevant data even more difficult. Some risk types are inherently difficult to define and quantify, such as reputation or strategic risk.

In managing these nonfinancial risk types, respondents were less likely to consider their institutions extremely or very effective. These include *reputation* (57 percent), *business resilience* (54 percent), *cybersecurity* (52 percent), *model* (51 percent), *conduct and culture* (50 percent), *strategic* (46 percent), *third-party* (40 percent), *geopolitical* (35 percent), and *data integrity* (34 percent).

Reflecting on the investments that have been made to enhance risk management, respondents were more likely to consider their institutions to be extremely or very effective today in managing a number of risk types than in the previous survey: *market* (92 percent, up from 79 percent), *country/sovereign* (76 percent, up from 53 percent), *longevity* (71 percent, up from 58 percent), *morbidity* (65 percent, up from 48 percent), *business resilience* (54 percent, up from 40 percent), *cybersecurity* (52 percent, up from 42 percent), and *model* (51 percent, up from 40 percent).[54]

Financial risks

CREDIT RISK

With economic conditions strengthening in many economies around the world, *credit risk* was less likely to be named among the top three risk types growing in importance (16 percent, down from 32 percent in the prior survey). Roughly the same percentage of respondents in Europe (13 percent) and the United States/Canada (11 percent) considered *credit risk* to be one of the top three risk types growing in importance, compared to 21 percent among respondents in Asia-Pacific.

While credit conditions have strengthened, financial institutions would do well not to underestimate the potential for credit risk events. Both the Financial Reserve Board and the OCC have noted that banks have eased their underwriting standards over the past couple of years, moving from a conservative posture after the fiscal crisis to an increased appetite for credit risk to spur loan growth. One concern noted by the OCC is the greater concentration of commercial real estate loans at many institutions and the potential deterioration in credit quality for these loans if the Federal Reserve were to raise interest rates at a faster rate than expected in response to an overheated economy and an acceleration in inflation.[55] This would cause an increase in commercial real estate cap rates, driving down collateral values and could increase defaults. In addition, institutions have seen a deterioration in leveraged lending portfolios as well as a move away from leveraged deals by the private equity sector.

When asked about specific issues related to credit risk, roughly 30 percent of respondents felt it would be very challenging for their institutions to manage each of these issues over the next two years. And for many types of credit exposures, respondents saw these as presenting less of a challenge than was the case in the 2016 survey.

Credit risk was seen most often as being extremely or very challenging to manage in *commercial real estate* (31 percent). The strength of the US economy is reflected by only 11 percent of respondents in the United States/Canada expecting that credit risk for commercial real estate would be extremely or very challenging to manage, compared to 45 percent in Europe and 36 percent in Asia-Pacific.

Collateral valuation was considered by 25 percent of respondents to be extremely or very challenging, which was down from 38 percent in the prior survey. Again, respondents in Europe (37 percent) and Asia Pacific (36 percent) were more likely to believe it presented this level of challenge than were those in the United States/Canada (5 percent).

Managing credit risk for other types of credit exposures was considered to be extremely or very challenging by less than one-quarter of respondents, and by fewer respondents than in 2016. Among the types of credit exposures that were less likely to be considered extremely or very challenging in the current survey compared to the previous survey were *unsecured credit* (20 percent, down from 33 percent), *commercial credit* (16 percent, down from 27 percent), *credit to emerging market countries and organizations* (28 percent, down from 13 percent), and *mortgages/home equity lines of credit* (18 percent, down from 30 percent).

Respondents reported that substantial progress has been made to comply with the new impairment measurement approaches being introduced under the US Financial Accounting Standards Board's Current Expected Credit Loss (CECL) model and under IFRS 9.[56] Both CECL and IFRS 9 are meant to address the delayed recognition of credit losses that is seen as a weakness of the current incurred loss accounting guidance for the Allowance for Loan and Lease Losses. Instead, CECL and IFRS 9 change the accounting requirement from an incurred loss approach to an expected loss approach. Under CECL, institutions will be required to estimate expected credit losses over the life of the loan, using all currently available information, including "reasonable and supportable forecasts." IFRS 9 does not require immediate recognition of all expected losses but proposes recognition over time.

While CECL and IFRS 9 represent a significant change in accounting for expected credit losses, current credit risk measurement approaches used for Basel regulatory capital calculations, economic capital, and stress testing (CCAR/ Dodd-Frank Act Stress Test) provide some elements that can be potentially leveraged. Seventy-one percent of respondents said they expected their institution's existing credit risk management approaches will be fully or mostly aligned with the new CECL model, compared to only 26 percent in the prior survey. Similar progress was evident concerning IFRS 9, with 80 percent of respondents expecting their institution's credit risk management approaches to be fully aligned with the new standard, compared to 38 percent in 2016.

For IFRS 9, there was a dramatic difference across regions. While 80 percent of respondents in the United States/Canada and 100 percent of those in Europe anticipated that their institution's credit risk management approaches will be fully or mostly aligned with the new impairment approach being introduced under IFRS 9, only 22 percent of respondents at institutions in Asia-Pacific had the same expectation.

MARKET RISK

Most institutions have mature risk management methodologies and policies to manage market risk, and relatively few respondents considered any issues to be very challenging in this area. The issues that respondents most often considered to be extremely or very challenging when managing market risk were *obtaining sufficient, timely, and accurate market risk data* (30 percent), *calculating specific risk for all positions* (27 percent), and *consistently aggregating the results of market risk calculations across portfolios and business areas* (22 percent).

Banks have now had two additional years to prepare for compliance with the Basel Committee's final framework for Minimum Capital Requirements for Market Risk resulting from the FRTB. The issue of *complying with the Basel Committee's revised Minimum Capital Requirements for Market Risk* was considered to be extremely or very challenging by 21 percent, which was down from 31 percent in the prior survey when it was cited more often as a challenge than any other issue.

The progress in this area was even greater for the largest institutions compared to the prior survey. While 55 percent of respondents from large institutions said *complying with the Basel Committee's revised Minimum Capital Requirements for Market Risk* was extremely or very challenging in 2016, that figure dropped to 32 percent in the current survey.

European banks are farther along than their counterparts in the United States/Canada in complying with the Basel Committee requirements. Nineteen percent of respondents in Europe considered compliance with these requirements to be extremely or very challenging, compared to 31 percent of respondents in the United States/Canada. Similar to other mature financial risk types, most institutions are addressing the remaining challenges in market risk management. For several aspects of market risk management, fewer respondents considered them to be extremely or very challenging than in the prior survey: *using the results of market risk calculations for capital and stress testing purposes* (11 percent, down from 17 percent), *monitoring market risk appetite utilization* (5 percent, down from 18 percent), and *aligning market risk management with overall ERM program* (7 percent, down from 23 percent).

However, more respondents considered *obtaining sufficient, timely, and accurate market data* to be extremely or very challenging than in the prior survey (30 percent, up from 21 percent), which is consistent with the broad trend of institutions continuing to find it difficult to access the high-quality, timely data needed for effective risk management.

LIQUIDITY RISK

Since the global financial crisis, there has been increased regulatory focus on managing liquidity risk. Basel III introduced the NSFR and LCR, the Basel Committee introduced its minimum total loss-absorbing capacity (TLAC) standard for global systemically important banks (G-SIBs) and globally active banks, and liquidity stress testing has become more common.

Relatively few respondents considered issues related to liquidity risk management would be very challenging over the next two years, with no single issue being cited by more than one-quarter of respondents. In many institutions, these issues were seen as less challenging than they were in the prior survey, which suggests that institutions are gaining more experience in complying with the new liquidity requirements. Only 11 percent of respondents considered *investment in operational and other capabilities to comply with the Basel III NSFR* to be extremely or very challenging, down from 23 percent in the prior survey. Similarly, 8 percent of respondents had the same assessment about *investment in operational and other capabilities to comply with the Basel III LCR*, which was a decrease from 23 percent in 2016.

Other liquidity risk issues that fewer respondents considered to be extremely or very challenging compared to the prior survey were *obtaining sufficient, timely, and accurate liquidity risk data* (17 percent, down from 26 percent), *internal allocation of the cost of liquidity buffers across the organization* (18 percent, down from 31 percent), *developing and documenting a credible set of systemic and idiosyncratic liquidity stress scenario*s (14 percent, down from 27 percent), and *controlling the consumption of liquidity on a daily basis across the whole organization* (18 percent, down from 31 percent).

ASSET LIABILITY MANAGEMENT

Asset liability management is another mature financial risk type, and less than 30 percent of respondents considered any issue in this area to be especially challenging. The issues that were most often rated as extremely or very challenging for asset liability management were *integrating the modeling of IRRBB and credit risk within the banking book to stress scenarios* (29 percent), *ability to model on a dynamic basis the impact on net interest income of changing interest rates and changing balance sheet* (27 percent), and *obtaining sufficient, timely and accurate asset and liability data* (24 percent). The issue cited least often was *risk measures consistent with board risk appetite*, which was considered to be extremely or very challenging by 9 percent of respondents, down from 20 percent in the prior survey.

Nonfinancial risks

There has been a broad acknowledgment by regulators and many financial institutions that there should be increased focus on nonfinancial risks, which can cause substantial financial and reputational impacts. In fact, the emergence of the term "nonfinancial risk" itself suggests both an expansion beyond the traditional view of operational risk as well as a grouping of related risks.[57] These risks include cybersecurity, regulatory, and conduct and culture risks, many of which have grown significantly in focus and importance. In recognition that nonfinancial risks merit increased attention, firms would be well advised to enhance their governance structure and risk management capabilities to monitor and manage these risks. To help address interrelationships among nonfinancial risks, some firms have begun to group their nonfinancial risk management capabilities within a nonfinancial risk function under the CRO.

> "Nonfinancial risks are growing in size and importance. The focus has moved beyond traditional operational risks to risks like cyber, conduct and culture, and third-party risk management. Dealing with the challenges posed by these risks has required additional resources."
>
> —Senior risk executive, large diversified financial services company

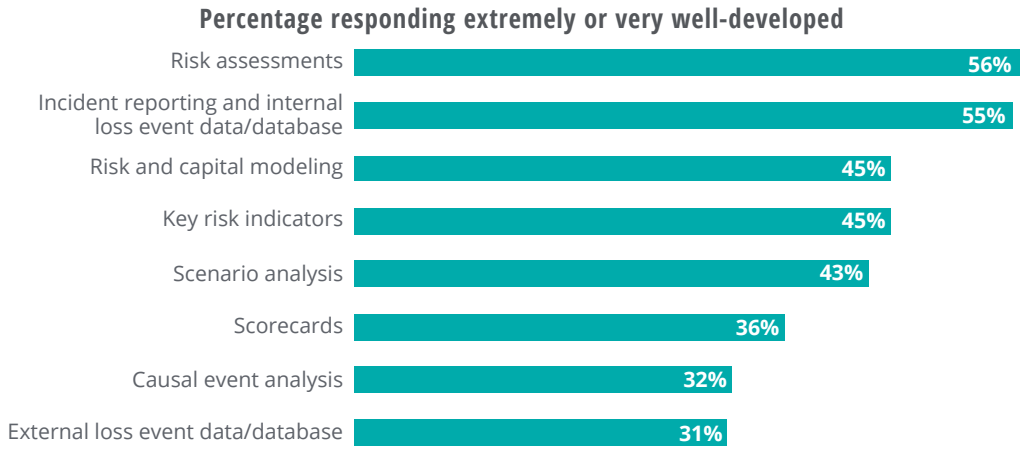
OPERATIONAL RISK

The Basel Committee has made fundamental changes to how operational risk capital is calculated by replacing the model-based advanced measurement approach (AMA) with the Standardized Measurement Approach (SMA). The SMA is based on two variables: the Business Indicator Component, which is, in turn, based on selected financial data intended to be representative of the bank's business volume in different aspects, and the Internal Loss Multiplier, which is, in turn, based on the bank's actual operational risk loss history. As a result, banks will need to ensure their internal loss databases are as accurate as possible and supported by effective IT systems, processes, and controls. Under the new approach, banks will have the opportunity to reduce their required operational risk capital by taking steps to reduce their actual operational losses.[58] The final rule is to be implemented by January 1, 2022.

In fact, only 56 percent of respondents felt their institution was extremely or very effective when it came to managing operational risk, reflecting the inherent difficulties in measuring and managing operational risk. Fewer than one-half of respondents considered most operational risk management methodologies to be extremely or very well-developed at their institutions, although the percentages grew from the prior survey: *key risk indicators* (45 percent, up from 30 percent), *scorecards* (36 percent, up from 12 percent), *causal event analysis* (32 percent, up from 16 percent), and *external loss event data/database* (31 percent, up from 19 percent) (figure 17).

FIGURE 17

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



Source: Deloitte analysis.

Maintaining an accurate internal loss event database will be essential to complying with the proposed changes to operational risk capital in Basel III, and it appears that progress is being made, with 55 percent of respondents considering *incident reporting and internal loss event data/database* to be extremely or very well-developed compared to 45 percent in the prior survey.

However, when respondents were asked about the maturity of specific aspects of their organization's internal loss data that will be needed to employ the SMA as required under the changes to Basel III, it is clear that much work remains to be done. The issue that was most often considered to be extremely or very well-developed was *consistent mapping of loss events to operational risk loss event types* (44 percent). A second set of issues was considered by a little more than one-third of respondents to be extremely or very well-developed: *sufficient duration of internal loss data* (39 percent), *completeness of loss data events* (37 percent), *consistency of loss event capture across different organizational units* (36 percent), *sufficiency and granularity of legal loss data information* (34 percent), and *quality of loss data information* (34 percent). Two additional items were even less likely to be considered extremely or very well-developed: *coverage of tail events* (26 percent) and *treatment of boundary risk items* (19 percent).

Most institutions said they had completed or were currently implementing changes or enhancements to a variety of aspects of their operational risk programs. The areas most often cited as being addressed were *operational risk reporting* (72 percent) and *operational risk assessment* (70 percent).

In preparation for the impending changes to operational risk management in Basel III, 65 percent of respondents said their institutions had, or were in the process of, changing or enhancing *incident reporting and internal loss event data/database*. Surprisingly, only 31 percent of respondents said their institutions were changing or enhancing *preparing for the Basel Committee's proposed guidance on the Standardized Measurement Approach for operational risk*. This result may reflect either or both of two factors: the length of the anticipated implementation period through January 1, 2022 and a view that existing loss databases will be highly leverageable. However, we would recommend that organizations conduct a broader readiness analysis, understand the impact of SMA, and develop an implementation plan.

More than one-half the institutions also reported making changes or enhancements to a number of other operational risk areas: *operational risk governance* (62 percent), *operational risk framework* (60 percent), *operational risk analytics* (58 percent), and *operational loss data set* (50 percent).

Third-party relationships present a special set of operational risks including nonperformance, theft of intellectual property, violations of laws and unethical conduct, data breaches, and the inability to provide services when faced with an infrastructure breakdown or disaster. Vendors are not under the direct control of the financial institution and may themselves subcontract work to additional vendors. Weak controls and ineffective operational risk frameworks at some vendors can allow issues to grow undetected. The actions of third parties can cause significant financial loss and reputational damage, and regulators have made it clear that a financial institution retains the responsibility for the actions of its vendors.

The actions of third parties can cause significant financial loss and reputational damage, and regulators have made it clear that a financial institution retains the responsibility for the actions of its vendors.

Only 40 percent of respondents felt their institution was extremely or very effective at managing the risks from their relationships with third-party service providers. Further, relatively few respondents considered their institutions to be extremely or very effective at managing specific types of risk in their third-party relationships. The risk types where respondents most often considered their institution to be extremely or very effective in managing third-party risks were *financial* (60 percent) and *regulatory/compliance* (54 percent). Respondents gave their institutions much lower ratings in other areas. Only 34 percent of respondents considered their institutions extremely or very effective when it came to managing the *reputational risk* in third-party relationships and 44 percent for *performance and operations*.

CYBERSECURITY RISK

Among financial institutions and regulators around the world, there has been increased attention on the importance of managing cybersecurity risk, and this focus is only expected to increase. The losses from cyberattacks were an estimated US$445 billion across all industries in 2016, up 30 percent from three years before, and banks and other financial institutions are prime targets of hackers.[59] The number of cyberattacks against financial institutions is estimated to be four times greater than against companies in other industries.[60]

Cyber threats continue to increase in sophistication and hackers can now obtain confidential information such as client data, install ransomware, initiate unauthorized payments, conduct espionage, and disrupt online systems, among other threats. The US Treasury Department has named cyberattacks as one of the top risks facing the US financial sector.[61] In November 2017, the Society for Worldwide Interbank Financial Communications (SWIFT) warned banks around the world that cyber risk was on the rise, saying that hackers had advanced their capabilities since a hacker stole US$81 million from Bangladesh Bank in February 2016.[62] The Cobalt hacking group has been tied to cyberattacks against at least 100 banks around the world since 2016, stealing approximately one billion euros.[63]

In July 2017, an Italian bank had confidential data from 400,000 customer accounts stolen by hackers.[64] The potential for hackers to steal confidential customer data raises additional regulatory

issues for institutions required to comply with GDPR and other consumer privacy regulations. As the industry comes to embrace open banking, there will be the additional challenge of determining responsibility when customer data is handed off and subsequently misused or disclosed inappropriately.

> "Cyber risk has become a standing agenda item on every board risk committee meeting. Our biggest challenge in cyber is the all-out sprint to continually manage patches and updates to stay ahead of vulnerabilities. We also have ongoing contingency planning to manage potential incidents."
>
> —Chief risk officer, large multinational insurance company and financial services provider

Regulators will increasingly require financial institutions to demonstrate that their controls and recovery plans have been robustly developed and thoroughly tested against sufficiently severe scenarios, and institutions may be subject to fines or other disciplinary measures if regulators find that deficiencies are not appropriately addressed.

In 2016, the US federal banking agencies issued an advance notice of proposed rulemaking regarding enhanced cyber risk management standards, although it is not certain whether the new leadership at these agencies may choose instead to employ an existing standard such as the National Institute of Standards and Technology Cybersecurity Framework.

In May 2018, the ECB published a framework for testing the resilience of the financial sector to cyberattacks.[65] In July 2018, the Bank of England and the UK Financial Conduct Authority announced requirements that UK financial services institutions report to them on their exposure to cybersecurity risk and how they would respond to an attack.[66] The application of the EBA's new Guidelines on Information and Communication Technology risk within the Supervisory Review and Evaluation Process may result in additional (Pillar 2) capital requirements for unaddressed deficiencies in cyber risk management as part of operational risk assessments.

Insurance regulators are at an earlier stage of developing their approach to cybersecurity. EIOPA has indicated that it will look to incorporate qualitative elements related to cyber risk into its 2018 stress test.

In addition to their supervision of individual institutions, regulators are beginning to address the risks that cyberattacks could pose to the financial system as a whole. Given the increasing interconnections among financial institutions, their technology partners, and financial markets around the world, a cyberattack has the potential to quickly damage the global financial system. The International Organization of Securities Commissions (IOSCO) has called cybersecurity risk "a growing and significant threat to the integrity, efficiency, and soundness of financial markets worldwide."[67] The EC has proposed to strengthen the mandate of the European Agency for Network and Information Security, the EU's cybersecurity agency, as part of a broad package of measures that span individual financial institutions and sectors. Regulators in Hong Kong and Singapore have launched programs, such as the HKMA's Cyber Security Fortification Initiative, to build industrywide resilience against cyberattacks.[68]

Sixty-seven percent of respondents named *cybersecurity* as one of the three risk types that would increase the most in importance, with 40 percent naming it as number one, far more than for any other risk type. Only 52 percent of respondents said their institutions are extremely or very effective at managing this risk, although this increased from 42 percent in 2016, which may reflect the increased attention to this risk type.

Respondents most often considered their institutions to be extremely or very effective in managing cybersecurity threats and risks in the areas of *disruptive attacks* (58 percent), *financial losses or fraud* (57 percent), *cybersecurity risks from customers* (54 percent), *loss of sensitive data* (54 percent), and *destructive attacks* (53 percent).

Respondents were less confident in their institution's risk management efforts when it came to other threats. Only 31 percent of respondents felt their institutions were extremely or very effective at managing *cybersecurity risks from third-party providers*, the lowest-rated item. There have been a number of recent cyberattacks attributed to nation states, and only 37 percent of respondents believed their institutions were extremely or very effective at addressing *threats from nation state actors*. Other threats where less than one-half the respondents considered their institutions to be extremely or very effective were *insider threats* (44 percent) and *threats from skilled hacktivists* (43 percent).

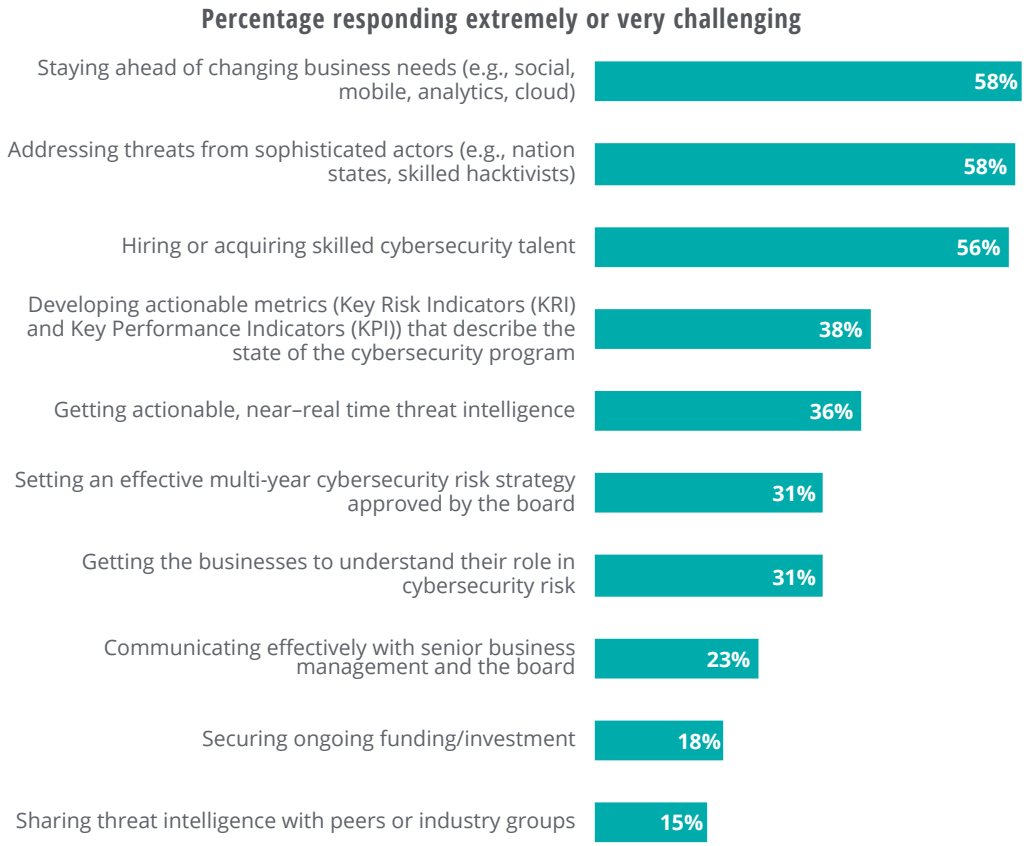
Institutions face a variety of challenges in enhancing their risk management programs to effectively manage the complex cybersecurity threats they face. Respondents most often considered *staying ahead of changing business needs* (such as social mobile, analytics, and cloud) (58 percent) and *addressing threats from sophisticated actors* (nation states, skilled hacktivists) (58 percent) extremely or very challenging (figure 18).

As cyber threats have proliferated and become more sophisticated, there has been a fierce competition for talented professionals with relevant experience. The issue named second most often as being extremely or very challenging was *hiring or acquiring skilled cybersecurity talent* (56 percent).

Given the massive number of cybersecurity incidents, institutions are likely to supplement their cybersecurity professionals with an increased use

FIGURE 18

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



Source: Deloitte analysis.

of predictive analytics and automation. Institutions too often react to hacks and breaches after they have occurred. Instead, analytics can predict and screen threats and take automated corrective actions before they occur, although human intervention will also be needed to confirm and investigate threats, particularly when they are internal.[69]

In a number of areas, institutions appear to be making progress in their cybersecurity efforts. Institutions have invested in cybersecurity, and fewer respondents considered several issues to pose important challenges than in the previous survey: *getting the businesses to understand their role in cybersecurity risk* (31 percent, down from 47 percent), *setting an effective multi-year cybersecurity risk strategy approved by the board* (31 percent, down from 53 percent), and *securing ongoing funding/investment* (18 percent, down from 38 percent).

Respondents were also more confident about the operation of their cybersecurity risk management programs, with fewer considering operational issues to be extremely or very challenging than two years ago: *developing actionable metrics (Key Risk Indicators (KRI) and Key Performance Indicators (KPI)) that describe the state of the cybersecurity program* (38 percent, down from 55 percent) and *getting actionable, near-real time threat intelligence* (36 percent, down from 57 percent).

CONDUCT AND CULTURE

After a series of instances of misconduct and unethical behavior at individual financial institutions around the world, there has been a global trend to focus more intently on conduct and culture risk, and to stress the importance of individual accountability, particularly for senior management. The United Kingdom's Senior Managers and Certification Regime has been established for some time, and the FSB is prioritizing ways to increase individual accountability of senior managers and promote governance frameworks that address cultural risk. New guidelines from the European Securities and Markets Authority and the EBA are designed to improve firms' internal governance and their suitability assessments of senior managers.

Established in December 2017, Australia's Royal Commission into Misconduct in the Banking, Superannuation, and Financial Services Industry delivered an interim report in September 2018 that found widespread misconduct among financial institutions as well as inadequate supervision of conduct risk by the APRA and the Australian Securities and Investments Commission.[70] The final report is expected in February 2019, and it is anticipated there will be significant changes in regulatory oversight of conduct risk in Australia, which could become a model for regulators in other jurisdictions. Regulatory initiatives to strengthen the management of conduct and culture risk by enhancing accountability have also been taken in the United States, the United Kingdom, and Hong Kong, among others.[71]

Financial institutions are expected to sell products in a way that is clear, fair, and not misleading. There is particular attention to their treatment of vulnerable customers who are less able to protect their own financial interests. Defining such customers can depend on a variety of factors and is dynamic, with the group of vulnerable customers continually changing as their personal situations evolve. Regulatory initiatives that address the responsibilities of financial institutions when interacting with vulnerable customers have been undertaken by a variety of regulatory authorities including IOSCO, the Financial Conduct Authority in the United Kingdom, the European Systemic Risk Board, and the EIOPA.[72]

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

Advanced analytics and AI technologies offer the opportunity to substantially improve effectiveness at managing conduct risk. For a start, institutions can employ these technologies to automatically identify vulnerable customers and periodically update this analysis. Analytical tools, coupled with natural language processing, can also be used to analyze the sentiment and tone of unstructured data such as emails, texts, and chat messages to detect, and potentially prevent, instances of conduct risk, such as fraud or insider trading activities.

Many financial institutions find it challenging to manage conduct and culture risk. When asked how effective their institutions were in managing individual risk stripes, 50 percent of respondents considered their institutions to be extremely or very effective at managing conduct and culture risk, placing it 25 out of 31 risk stripes. Although there could be a reduction in conduct risk in sales activities as financial institutions employ AI bots to replace sales staff, misconduct that does occur could be on a much larger scale due to the efficiency and increased speed and volumes resulting from AI.[73]

Fifty percent of respondents did not cite *monitor conduct risk* as a board responsibility, which may reflect that many institutions see this as more of a task for management. However, 67 percent of respondents said that a board responsibility was to *help establish and embed the risk culture of the enterprise/promote open discussions regarding risk*. When it came to risk management priorities, 55 percent of respondents cited *establishing and embedding the risk culture across the enterprise* as an extremely high or very high priority for their institutions, yet only 28 percent of respondents named *establishing a formal conduct and culture program* as a top priority. These results suggest that there may be greater awareness of the broad need for strong risk culture than in addressing specific conduct risks.

Monitoring conduct risk and embedding a risk culture across the organization are increasingly important risk management responsibilities, and institutions will need to have their boards play an appropriate role in this effort. In addition, they may find a need to formalize their activities into an explicit conduct and culture program to raise its profile, communicate its importance to all employees, and list specific steps that should be taken to identify and manage this risk.

> "For conduct risk, we have an embedded process where compliance, risk, and audit assess the control environment of each of the businesses and functions. Based upon those ratings, we develop an overall rating for an organizational unit and their compensation is impacted by that."
>
> —Chief risk officer, large diversified financial services company

REGULATORY RISK

Although the overall pace of regulatory change has slowed, financial institutions often still face substantial regulatory examinations and supervisory comments, which has led many to feel that regulatory intensity has not abated. There also continues to be a number of important regulatory policy developments. The Basel Committee has pronounced the end of its post-crisis regulatory reform agenda with the finalization of Basel III; however, this end will have a relatively long tail as the implementation of Basel III is not targeted until 2022, and further until 2027 for the phase-in of the full output floor. In fact, some believe that the 2022 deadline is in doubt, given the required legislative approvals in the European Union. Additionally, specific implementation will depend on how and when national and regional regulators adopt these international standards. There are increasing signs of governments and regulators around the world being prepared to diverge from globally agreed upon standards to take account of their own interests and needs, which 37 percent of the respondents to the survey were extremely concerned or very concerned about.

The IAIS is continuing work on developing international capital standards for insurance companies, and several important issues still need to

be resolved. (See "Sector spotlight: Insurance.") In 2018, a number of regulations took effect in Europe such as MiFID, the Insurance Distribution Directive (IDD), and the GDPR. Regulators around the world are also focusing more on newer nonfinancial risk topics including cybersecurity, conduct and culture, third-party risk, and risk data quality and availability.

> "It's sometimes hard for us to assess and keep pace of the overall regulatory environment given the constant drumbeat of changing regulatory expectations."
>
> —Chief risk officer, large multinational insurance company and financial services provider

Reflecting these developments, 83 percent of respondents expected the regulatory requirements on their institutions to increase over the next two years, with one-third expecting a significant increase.

Given the regulatory focus on cybersecurity, respondents most often said they were extremely or very concerned about the impact on their institutions of regulatory efforts in the area of *cyber resilience* over the next two years, (59 percent) (figure 19). (See the section, "Cybersecurity.")

Safeguarding the privacy of customer data has been another regulatory concern. *Data privacy requirements* was cited second most often, with 54 percent of respondents saying they are extremely or very concerned about the potential impact on their institutions of regulations on this issue.

With increasing concerns over the use of personal data and data privacy, regulators are increasing their scrutiny of how financial institutions use consumer data. The EU's GDPR placed new data protection requirements on all institutions that hold the data of EU citizens, wherever the institutions are located, including the need to obtain consumer consent before collecting personal data, among other provisions. Institutions subject to GDPR were required to complete Data Protection Assessments, and if necessary, put in place remediation plans by its May 2018 implementation date. In 2017, the Indian Supreme Court ruled in favor of a fundamental right to privacy, and in July 2018, the Srikrishna Committee proposed the Personal Data Protection Bill, 2018.[74] In 2017, the Chinese government also identified a right to privacy in the General Provisions of the Civil Law, and the Cybersecurity Law placed a renewed emphasis on data protection.[75]

The use of analytics and AI solutions to design and deliver products is based on the use of large sets of customer data, and this can be challenging while complying with new consumer privacy regulations. Under GDPR, for example, consumer consent must be obtained to gather personal data, and consumers have the right to request an explanation for, and object to, decisions based on automated processing that has a legal effect on them. Institutions will need to obtain the required consents and provide clear explanations in response to customer inquiries. This can be difficult when an institution employs deep learning or neural network AI technologies since it may not be clear what data is driving an automated decision.

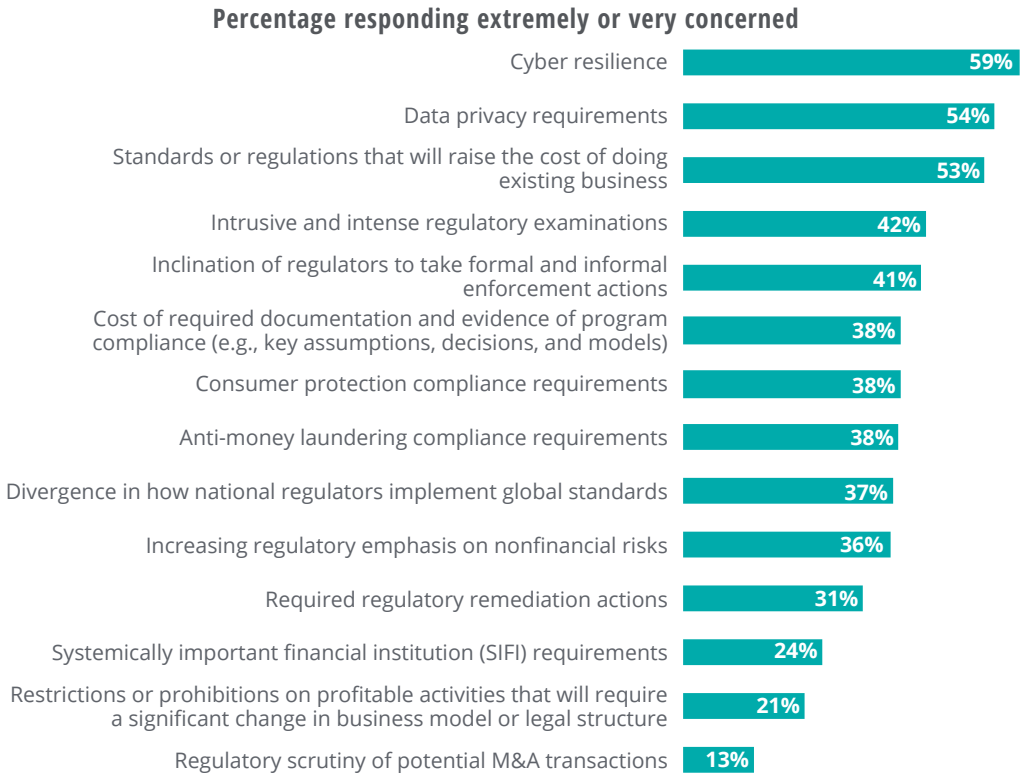
The final issue that more than one-half of the respondents were concerned about regarding regulatory impacts on their institutions was *standards or regulations that will raise the cost of doing existing business* (53 percent). Increasing compliance costs is one important driver leading financial institutions to turn to technologies such as RPA and cognitive analytics to increase efficiency.

Although regulatory authorities have increased their attention on the management of nonfinancial risks, only 36 percent of respondents were extremely or very concerned about the impact on their institutions of regulations in this area.

Similarly, only 38 percent of respondents had this level of concern regarding *anti–money laundering compliance requirements*. However, this could prove to be overly optimistic; some anticipate increased anti-money laundering actions, especially in Europe, in the wake of recent violations of regulatory requirements in this area. After concerns about inadequate enforcement in Malta and Denmark of

FIGURE 19

Over the next 2 years, how concerned are you about the potential impact on your organization of each of the following regarding supervisory and regulatory processes?



Source: Deloitte analysis.

anti-money laundering regulations, the EBA now plans to review the supervision of anti-money requirements in all EU member states.

"The bar for regulatory expectations is constantly being raised, and I don't think anybody expects it to be lowered materially. While there have been clear areas of regulatory overreach, there is no question that many of the processes established to respond to regulatory expectations were an exponential improvement over previous practices."

—Senior risk executive, large global financial services company

Risk management information systems and technology

RISK DATA STRATEGY and IT systems have presented challenges to financial institutions for some time, and they are assuming even greater importance today as institutions look to leverage the latest technologies to increase efficiency while also improving their ability to monitor and take preventive action against potential risk events.

Beyond ensuring regulatory compliance, risk data and IT systems have become more important given the potential of new technologies to improve both the efficiency and effectiveness of risk management.

No more than one-third of respondents considered their institutions to be extremely or very effective in any aspect of risk data strategy and infrastructure. The issues where respondents most often felt their institutions were extremely or very effective were *data governance* (34 percent) and *data controls/checks* (33 percent). For other issues, even fewer respondents rated their institutions as extremely or very effective including *data management (KPIs and KRIs)* (25 percent), *data standards* (28 percent), and *data quality* (19 percent).

Regulators have been requiring financial institutions to improve their risk data. The Basel Committee's principles for effective risk data aggregation and risk reporting (BCBS 239), which were released in 2013 for implementation by G-SIBs, have provided a benchmark against which regulators around the world are measuring the adequacy of risk data programs within the financial sector more generally. The core principles of BCBS 239 are strong data governance; data architecture and IT infrastructure that fully supports capabilities and practices; accurate, complete, timely, and adaptable aggregation; and accurate, comprehensive, clear, and useful reporting. The most recent progress report on BCBS 239, released in June 2018, concluded that banks had found it "challenging to comply with the principles" and that "the expected date of compliance has slipped back for many banks."[76]

In the United States, regulators have stated their expectations that banks have an integrated data environment that supports external and management reporting across financial, legal entity, liquidity, capital, and resolution planning areas.

In Australia, the APRA has cited the need for improvements in risk data at deposit-taking institutions and is proposing an increase in the amount and granularity of data collected from larger institutions. The Reserve Bank of India has expressed similar sentiments and has stepped up scrutiny of data governance, as well as on the source and quality of data points.[77]

Many financial institutions will require significant work to implement an integrated data

architecture and put in place an effective data controls framework. As part of this effort, institutions are moving from having data independently managed and stored in each business line to one where data is viewed as an enterprise asset that is managed by the C-suite. Assigning responsibility for managing data throughout the organization is key, and more institutions are creating a chief data officer (CDO) position.

Beyond ensuring regulatory compliance, risk data and IT systems have become more important given the potential of new technologies to improve both the efficiency and effectiveness of risk management. Machine learning and cognitive analytics tools can make predictions and decisions without the need for explicit programming, and when combined with natural language processing applications, can interpret unstructured data such as emails and texts and transform them into structured data that can be analyzed to identify and address potential risk events before they occur. RPA can be used to test 100 percent of a set of transactions and flag exceptions rather than having humans test a sample. Regulatory compliance may be improved by using natural language processing applications to extract regulatory requirements and then map them to control activities.[78]

While the benefits promise to be substantial, institutions will need to be ready to manage the increased risks that these technologies can create. While automated solutions can reduce the potential for human error, they can also make transactions faster and more numerous, and as a result, potentially increase the exposure when errors or control breakdowns happen. Institutions may have a greater need to test the results of a machine-learning algorithm rather than the reviews performed by a middle manager.

Further, as institutions come to rely more heavily on AI tools, such as machine learning and neural networks, in pricing and product development, they will need to adapt their risk management frameworks and risk appetite to address the additional risks these applications create, such as the potential for inadvertent bias, rogue programs, or inaccurate automated results.

The standards for the quality, timeliness, and regulatory-compliant usage of data will also need to increase. In particular, it is more difficult to effectively employ such technology tools while still complying with the requirement in GDPR that consumer consent be obtained. (See the section, "Regulatory risk.") In addition, the adoption of these technologies will further increase the importance of effectively managing model risk and cyber risk.

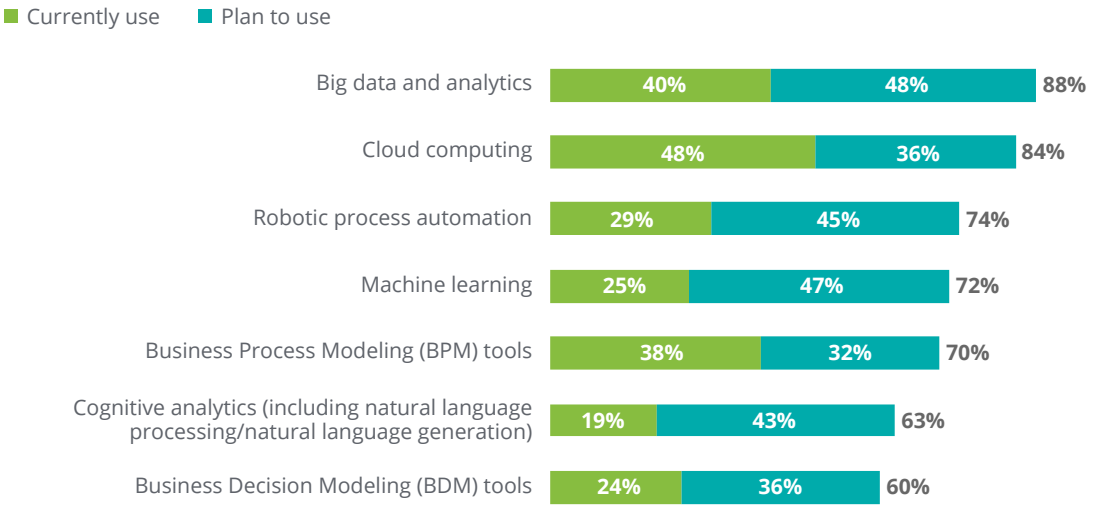
Most institutions are either already using, or plan to use, a number of emerging technologies in their risk management function, although the overall adoption of these technologies today is relatively limited (figure 20). The technologies that respondents most often said are being used currently are *cloud computing* (48 percent), *big data and analytics* (40 percent), and *Business Process Modeling (BPM) tools* (38 percent).

> "We are using natural language processing in areas where there are huge amounts of paper documents that need to be read and analyzed. It is becoming an essential tool."
>
> —Senior risk executive, large global diversified financial services company

Surprisingly, given the attention paid to the potential of *RPA* to reduce costs and improve accuracy by automating repetitive manual tasks without human involvement, only 29 percent of respondents said their institutions are currently using it.[79] For more emerging technologies, fewer than 30 percent of respondents said their institutions were employing them; these include *machine learning* (25 percent), *Business Decision Modeling (BDM) tools* (24 percent), and *cognitive analytics* (including natural language processing/natural language generation) (19 percent). Clearly, there remains substantial opportunity to leverage these technologies to enhance risk management programs.

FIGURE 20

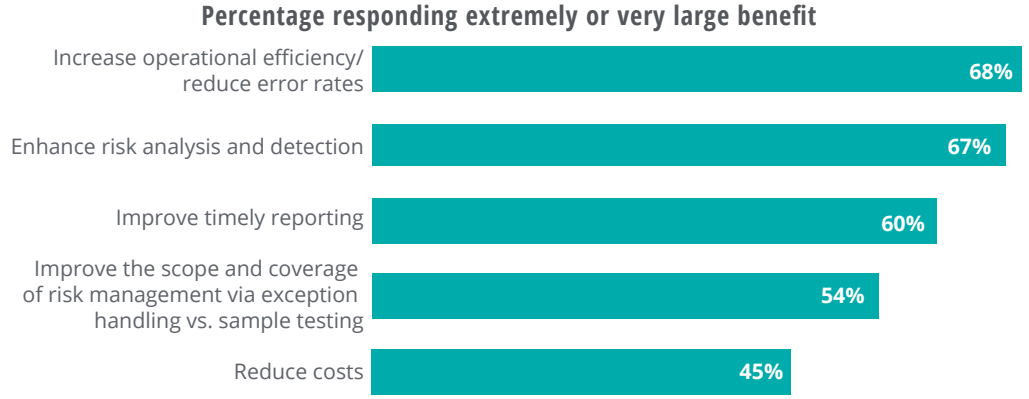
Does your organization use or plan to use any of the following emerging technologies in the risk management function?



Note: Some percentages do not total due to rounding.

FIGURE 21

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



Source: Deloitte analysis.

Although the adoption of these technologies is in its early stages, respondents were optimistic about their potential benefits. Roughly two-thirds of respondents expected emerging technologies would deliver a very large or large benefit to *increase operational efficiency/reduce error rates* (68 percent), *enhance risk analysis and detection* (67 percent), and *improve timely reporting* (60 percent) (figure 21). Roughly one-half the respondents expected new technologies to provide this level of benefit to *improve the scope and coverage of risk management via exception handling vs. sample testing* (54 percent) and *reduce costs* (45 percent).

Considering the challenges that institutions face regarding their risk management technology systems, respondents most often said they were extremely or very concerned about their institution's *risk data quality and management* (53 percent, up from 41 percent in 2016). The demands on institutions to maintain accessible, comprehensive, and quality risk data only continues to grow. The next two issues which respondents said they were most often extremely or very concerned about relate to modernizing the IT architecture: *legacy systems and antiquated architecture or end-of-life systems* (48 percent) and *lack of integration among systems* (47 percent). Many institutions have multiple legacy IT systems for different lines of business or geographies, often the result of growth by acquisition, which lack robust capabilities and cannot easily be integrated.

In contrast, respondents were least likely to be concerned about a *lack of technology or IT strategy approved by board* (19 percent), a *lack of product and asset class coverage* (17 percent), and *lack of aggregation of trading and banking books* (16 percent).

Conclusion

FACING SIGNIFICANT ECONOMIC dangers and nonfinancial risks, financial institutions will need to fundamentally re-examine and re-engineer their risk management functions. Among the many uncertainties are national prudential regulators' final implementation of the regulatory requirements for capital adequacy, the increasing fragmentation of regulation across jurisdictions, the uncertainties in the global economy, especially the economic slowdown and increasing debt levels in the Chinese economy and trade-related volatility, and the final terms of the United Kingdom's withdrawal from the European Union.

It has become more important than before for institutions to ensure that their risk appetite and risk utilization are key considerations when strategic goals are set. In addition, management should carefully consider the impacts of business strategy on capital and liquidity in light of increased regulatory requirements.

Now that the pace of regulatory change has abated, institutions have the opportunity to reconsider how risk management is structured and managed. The three lines of defense risk governance model should be re-examined to eliminate overlapping responsibilities and to ensure that the business units in Line 1 have a clear understanding of their responsibilities to manage the risks they assume.

Risk management will need to expand its view from traditional financial risks to enhance its capabilities in managing a wider range of nonfinancial risks, which can be just as damaging. First on the list of priorities is to improve the ability of risk management to identify and either prevent or address sophisticated cyberattacks, from both individuals and nation states. Even more challenging, institutions also need to manage cybersecurity risks that can originate from third-party service providers.

It has become more important than before for institutions to ensure that their risk appetite and risk utilization are key considerations when strategic goals are set.

The many other nonfinancial risks that must be managed effectively include third-party risk, conduct and culture, reputation, data integrity, geopolitical risk, and model risk. Institutions will require a comprehensive approach to identify and manage them.

Digital technologies hold the potential to fundamentally re-engineer virtually every aspect of risk management. A first step is to employ RPA to increase efficiency and cut costs by automating repetitive manual tasks. Technologies such as cognitive analytics, machine learning, and natural language processing hold even greater potential. Activities that currently require human judgment can be automated, with exceptions flagged for review by human professionals. Testing can be automatically conducted on 100 percent of a set of transactions, rather than by humans on only a sample. The first draft of risk reports could be generated automatically, with only review and selected input needed by the risk analyst. A wide range of signals could be automatically scanned continuously to identify impending risk events or misconduct. Big data analytics could provide greater insight into the interactions of risks and their causal factors.

These changes, which are already beginning to be implemented, mark a fundamental break with traditional approaches. In institutions that seize this opportunity, a risk-aware culture will infuse the organization, flowing from senior management as they devise strategy for business units to make day-to-day business decisions. The risk management function should have robust capabilities to manage a wide range of nonfinancial risks, especially cybersecurity, conduct, and third-party risk. Risk management could be powered by digital tools that provide early warning of impending risk events, offer insight into the factors that increase risk, and free risk professionals from repetitive tasks, allowing them instead to concentrate on identifying emerging risks and adding value.

Endnotes

1. About the term "leading practice": For purposes of this paper, we consider industry practices to fall into a range, from leading to lagging. Some industry practices may be considered leading practices, which are generally looked upon favorably by regulators, industry professionals, and observers due to the potentially superior outcomes the practice may attain. Other approaches may be considered prevailing practices, which are seen to be widely in use. At the lower end of the range are lagging practices, which generally represent less-advanced approaches and which may result in less-than-optimal outcomes. Items reflected as leading practices herein are based on survey feedback and the editor's and contributors' experience with relevant organizations.
2. The economic statistics in the section are from the International Monetary Fund, *World economic outlook: October 2018*.
3. Martin Wolf, "China's debt threat: time to rein in the lending boom," *Financial Times*, July 25, 2018.
4. *Economist*, "Gateway to the globe," July 28, 2018.
5. Keith Bradsher, "Trump's tariffs are changing trade with China. Here are 2 emerging endgames," *New York Times*, August 8, 2018.
6. Mark Landler and Alan Rappeport, "Trump hails revised NAFTA trade deal, and sets up a showdown with China," *New York Times*, October 1, 2018.
7. Kevin Liptak, "Trump and top European leader agree to work toward zero tariffs," CNN, July 26, 2018.
8. International Monetary Fund, *Global financial stability report*, October 2018.
9. Matt Phillips and Karl Russell, "The next financial calamity is coming. Here's what to watch," *New York Times*, September 12, 2018.
10. Reuters, "US bank profits up 27.5 percent in Q1 2018 versus year-ago—FDIC," May 22, 2018; Matt Egan, "American banks had their most profitable quarter ever," CNN, May 22, 2018.
11. European Banking Authority, *Risk dashboard: Data as of Q1 2018*, accessed November 19, 2018.
12. David Keohane, Martin Arnold, and Nicholas Megaw, "European banks fall further behind their US rivals," *Financial Times*, May 4, 2018.
13. Baker Donelson, "LIBOR phaseout: What happened and what's next?", February 2, 2018.
14. Silvia Amaro, "The UK government wants a 'new arrangement' for its banks after Brexit," CNBC, July 12, 2018.
15. For a discussion of open banking, see Deloitte, *How to flourish in an uncertain future: Open banking*, 2017.
16. Reuters, "Jack Ma's Ant Financial adds two new money market funds to its platform," May 4, 2018; Ian Fraser, "Chinese payment giants are lightyears ahead," Raconteur.net, September 25, 2018.
17. Financial Conduct Authority website, "Global Financial Innovation Network," July 8, 2018; Monetary Authority of Singapore, "FinTech regulatory sandbox," MAS website, accessed November 19, 2018; Australian Securities & Investments Commission, "Regulatory sandbox," ASIC website, accessed November 19, 2018.
18. European Commission, "FinTech: Commission takes action for a more competitive and innovative financial market," press release, March 8, 2018.
19. Office of the Comptroller of the Currency, "OCC Begins Accepting National Bank Charter Applications From Financial Technology Companies," press release, July 31, 2018.

20. Sylvan Lane, "Trump signs Dodd-Frank rollback," *Hill*, May 24, 2018.
21. Shu Zhang and Se Young Lee, "China to merge regulators, create new ministries in biggest overhaul in years," Reuters, March 12, 2018.
22. Reuters, "EU watchdog criticizes Malta for anti-money laundering shortcomings," July 11, 2018; Reuters, "EU bank watchdog examining Danish handling of Danske," October 8, 2018.
23. For a discussion of these regulatory developments, see Deloitte, *Financial services regulatory outlook 2018: Facing the future: An evolving landscape*, Deloitte Centre for Regulatory Strategy, Asia Pacific, 2017.
24. For a discussion of model risk management in insurance, see Deloitte, *Model risk management: A practical approach for addressing common issues*, 2017.
25. Reuters, "U.S., EU fines on banks' misconduct to top $400 billion by 2020: Report," September 27, 2017,
26. In this report, some percentages do not total due to rounding.
27. Percentages total more than 100 percent since some institutions provide more than one type of service. 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).
28. Basel Committee on Banking Supervision, *Guidelines: Corporate governance principles for banks*, July 2015.
29. Deloitte, "Senate passes financial services regulatory reform bill, would amend key Dodd-Frank thresholds," March 14, 2018; Deloitte, *Final and proposed enhanced prudential standards (EPS)*, 2018.
30. National Association of Insurance Commissioners, "NAIC committee adopts corporate governance models," press release, August 18, 2014.
31. International Association of Insurance Supervisors, *Draft application paper on the composition and the role of the board*, June 29, 2018.
32. Federal Register, "Proposed guidance on supervisory expectation for boards of directors," August 9, 2017.
33. For a discussion of the role of boards of directors in risk governance and the Federal Reserve proposal, see Val Srinivas, Steve Fromhart, and Urval Goradia, *What's next for bank board risk governance?*, Deloitte Insights, October 31, 2017.
34. Basel Committee on Banking Supervision, *Principles for enhancing corporate governance*, October 2010; Basel Committee on Banking Supervision, *Guidelines: Corporate governance principles for banks*, July 2015.
35. For a discussion of the role of boards of directors in risk governance and the Federal Reserve proposal, see Srinivas, Fromhart, and Goradia, *What's next for bank board risk governance?*.
36. Note: Among the investment management firms participating in the survey, 70 percent also provide banking services.
37. Board of Governors of the Federal Reserve System, *SR 11-7: Guidance on model risk management*, April 4, 2011.
38. Board of Governors of the Federal Reserve System, *Comprehensive capital analysis and review 2018 summary instructions*, February 2018; European Central Bank, *Guide for the targeted review of internal models (TRIM)*, February 2017.
39. Financial Stability Board, *Principles for an effective risk appetite framework*, November 2013; Basel Committee on Banking Supervision, *Guidelines: Corporate governance principles for banks*.

40. Deloitte, *The future of risk management in financial institutions*, 2017.
41. Caroline Binham, "EBA stress test to gauge banks' response to doomsday Brexit, EU contraction," *Financial Times*, January 31, 2018.
42. Alan Rappeport and Emily Flitter, "Congress approves first big Dodd-Frank rollback," *New York Times*, May 22, 2018.
43. The percentages in this section are of respondents who reported that their institutions use capital stress tests.
44. The percentages in this section are for respondents who reported that their institutions use liquidity stress testing.
45. Basel Committee on Banking Supervision, *Minimum capital requirements for market risk*, January 2016.
46. Luis M. Linde, "Transformation of the banking business model", (speech given at the VII Expansión-KPMG Financial Meeting, Madrid, October 4, 2016).
47. Andrea Resti, *Banks' internal rating models—time for a change?*, European Parliament, November 9, 2016.
48. European Central Bank, "What is the targeted review of internal models?," February 15, 2017 (updated April 16, 2018).
49. International Monetary Fund, "Euro area policies: Financial sector assessment program-Technical note-Insurance, investment firm, and macroprudential oversight," July 19, 2018.
50. Deloitte Centre for Regulatory Strategy EMEA, *Bringing it all together: Financial markets regulatory outlook 2018*, 2017.
51. Deloitte, *IFRS 17: What does it mean for you?*, 2018.
52. The 2016 survey did not ask about the use of alternative data types.
53. *Reputation risk* was not included in this question in the 2016 survey.
54. *Longevity* and *morbidity* were only rated by respondents at companies that provide insurance services.
55. Office of the Comptroller of the Currency, *Semiannual risk perspective*, spring 2018.
56. Financial Standards Accounting Board, *Financial instruments—credit losses; measurement of credit losses on financial instruments*, June 2016.
57. For a discussion of the issues surrounding nonfinancial risk, see Deloitte, *The future of non-financial risk in financial services: Building an effective non-financial risk management program*, 2018.
58. For a discussion of the issues in operational risk management, see Deloitte, *The future of operational risk in financial services*, 2018.
59. McAfee, *Economic impact of cybercrime—No slowing down*, February 2018; Stacy Cowley, "Banks adopt military-style tactics to fight cybercrime," *New York Times*, May 20, 2018,
60. Warwick Ashford, "Financial institutions on high alert for major cyber attack," ComputerWeekly.com, February 11, 2016.
61. Office of Financial Research, US Department of the Treasury, *2017 annual report to Congress*, December 5, 2017.
62. Jim Finkle, "SWIFT warns banks on cyber heists as hack sophistication grows," Reuters, November 28, 2017.
63. Europol, "Mastermind behind Eur 1 billion cyber bank robbery arrested in Spain," press release, March 26, 2018.
64. Sofia Petkar, "Italy's largest bank HACKED in major security breach as data from 400,000 accounts stolen," *Express*, July 27, 2017.

65. European Central Bank, "ECB publishes European framework for testing financial sector resilience to cyber attacks," press release, May 2, 2018.

66. Alison DeNisco Rayome, "UK banks must detail plans to avoid cyberattacks, tech disruptions by the fall," TechRepublic, July 6, 2018.

67. IOSCO, *Cyber security in securities markets—An international perspective report on IOSCO's cyber risk coordination efforts*, April 2016.

68. Cybersecurity Fortification Initiative, *HKMA circular B1/15C B9/29C*, May 24, 2016.

69. Tom Davenport and Adnan Amjad, *The future of cybersecurity: Analytics and automation are the next frontier*, Deloitte Insights, September 26, 2016.

70. Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry homepage; Stephen Letts, "'Unprofessional' banks need tougher policing, APRA admits," Australian Broadcasting Corporation, October 11, 2018.

71. For a discussion of these regulatory developments, see Deloitte, *Bringing it all together: Financial markets regulatory outlook 2018*, 2017, and Deloitte Centre for Regulatory Strategy, Asia Pacific, *Financial services regulatory outlook 2018: Facing the future: An evolving landscape*, 2017.

72. For a discussion of this issue, see Deloitte, *Bringing it all together: Financial markets regulatory outlook 2018*, 2017.

73. For an analysis of the impact of artificial intelligence on financial services, see World Economic Forum, *The new physics of financial services*, August 2018.

74. Julie McCarthy, "Indian supreme court declares privacy a fundamental right," National Public Radio, August 24, 2017; Sindhuja Balaji, "India finally has a data privacy framework—what does it mean for its billion-dollar tech industry?," *Forbes*, August 3, 2018.

75. For a discussion of data protection regulations and their implications, see Deloitte Centre for Regulatory Strategy, Asia Pacific, *Financial services regulatory outlook 2018: Facing the future: An evolving landscape*, 2017.

76. Basel Committee on Banking Supervision, *Progress in adopting the principles for effective risk data aggregation and risk reporting,* June 2018.

77. Shri S. S. Mundra, "Information technology & cyber risk in banking sector—the emerging fault lines," Reserve Bank of India, September 7, 2016.

78. For a discussion of the use of RPA and cognitive intelligence to streamline regulatory reporting, see Deloitte, *Modernizing regulatory reporting in banking & securities*, Deloitte Center for Regulatory Strategies, 2017.

79. For a discussion of the role of RPA in compliance, see Deloitte, *Compliance modernization—Focus on 5: Robotics process automation (RPA)*, 2017.

About the author

EDWARD HIDA leads Deloitte's financial risk community of practice and is a Risk and Financial Advisory partner at Deloitte & Touche LLP in the United States. He has substantial experience consulting on a variety of financial risk management and capital markets issues and has completed a wide range of risk management consulting assignments for US and global financial services organizations.

Contacts

GLOBAL FINANCIAL SERVICES INDUSTRY LEADERSHIP

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

Anna Celner
Global leader | Banking & 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

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

SURVEY EDITOR

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

Acknowledgments

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

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

- **Katherine Smith**, senior manager, Deloitte Services LP
- **Ulyana Stoyan**, manager, Deloitte & Touche LLP
- **Connor Keenan**, senior consultant, Deloitte & Touche LLP
- **Ludwig Reimmer**, senior consultant, Deloitte & Touche LLP

SUBJECT MATTER ADVISORS

- **Neal Baumann**, New York, nealbaumann@deloitte.com
- **Michael Bolan**, Chicago, mbolan@deloitte.com
- **Andrew Bulley**, London, abulley@deloitte.co.uk
- **J.H. Caldwell**, Charlotte, North Carolina, jacaldwell@deloitte.com
- **Anna Celner**, Zurich, acelner@deloitte.ch
- **Eric Clapprood**, Hartford, Connecticut, eclapprood@deloitte.com
- **Michael Fay**, Boston, mifay@deloitte.com
- **Anthony Frame**, Charlotte, North Carolina, aframe@deloitte.com
- **Ray Gonzalez**, Houston, rgonzalez@deloitte.com
- **Walter Hoogmoed**, Parsippany, New Jersey, whoogmoed@deloitte.com
- **Nitish Idnani**, New York, nidnani@deloitte.com
- **Marin Knight**, Boston, marinknight@deloitte.com
- **Dilip Krishna**, New York, dkrishna@deloitte.com
- **Stephen Lucas**, London, stelucas@deloitte.co.uk
- **Kent Mackenzie**, Edinburgh, kemackenzie@deloitte.co.uk
- **Quentin Mosseray**, London, qmosseray@deloitte.co.uk
- **Garrett O'Brien**, New York, gobrien@deloitte.com
- **Francisco Porta**, Madrid, fporta@deloitte.es
- **Martin Prince**, Stamford, Connecticut, maprince@deloitte.com
- **Michael Quilatan**, New York, mquilatan@deloitte.com
- **Ash Raghavan**, New York, araghavan@deloitte.com
- **Mike Ritchie**, Sydney, miritchie@deloitte.com.au
- **Markus Salchegger**, Munich, msalchegger@deloitte.de
- **David Sherwood**, Stamford, Connecticut, dsherwood@deloitte.com
- **Christopher Spoth**, Washington, D.C., cspoth@deloitte.com
- **David Strachan**, London, dastrachan@deloitte.co.uk
- **David Wilson**, Charlotte, North Carolina, daviwilson@deloitte.com

Deloitte.
Insights

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

Follow @DeloitteInsight

Deloitte Insights contributors

Editorial: Karen Edelman, Blythe Hurley, Preetha Devan, Rupesh Bhat, and Abrar Khan

Creative: Sonya Vasilieff

Promotion: Hannah Rapp

Cover artwork: Christina Chung

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

About Deloitte