

Deloitte.
University Press



Global risk management survey, 10th edition

Heightened uncertainty signals new challenges ahead

About Deloitte's global financial services industry group

A recognized leader in providing audit, consulting, tax, financial advisory, and risk advisory services to the financial services industry, Deloitte's clients include banks, securities firms, insurance companies, investment management firms, and real estate companies across the world.

Our financial services industry group brings together multidisciplinary capabilities and teams of client service professionals with diverse experience in serving both the industry and public sector.

For more information, please visit www.deloitte.com/fsi.

CONTENTS

Foreword	 	2
Executive summary	 	4
Introduction: Economic and business environment	 	9
Risk governance	 	17
Enterprise risk management	 	26
Economic capital	 	29
Stress testing	 	31
Sector spotlight: Banking	 	35
Sector spotlight: Insurance	 	37
Sector spotlight: Investment management	 	40
Management of key risks	 	46
Risk management information systems and technology	 	56
Conclusion	 	57
Endnotes	 	58

Foreword



Dear colleague,

We are pleased to present the 10th 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 77 financial institutions from around the world and across multiple financial services sectors, representing a total of \$13.6 trillion in aggregate assets. We wish to express appreciation to all the survey participants for their time and insights.

Overall, the survey found that leading risk management practices continue to gain wider adoption across the industry.¹ Boards of directors are devoting more time and taking a more active role in the oversight of risk management. The chief risk officer (CRO) position has become almost universal, and CROs are increasingly reporting directly to the board of directors and the chief executive officer (CEO). Enterprise risk management (ERM) programs designed to identify and manage risks across the enterprise are now the norm. Almost all respondents consider their institution to be effective in managing traditional risk types such as credit, market, and liquidity risk. These and other trends over the course of Deloitte’s *Global risk management survey* series are summarized below in the section “Evolution of risk management.”

The progress has been undeniable, but in the years ahead risk management is likely to face a different type of challenge. In the years since the global financial crisis, financial institutions have worked hard to address ever-increasing regulatory requirements. In 2017, however, the industry may be reaching an inflection point. After the fundamental reforms of the last several years, there are indications that going forward the trend of ever-broader and more stringent regulatory requirements may slow or actually be reversed in some areas. The US Federal Reserve has eliminated the qualitative review of capital plans and stress testing for large, noncomplex

firms; some European regulators and institutions have resisted recent so-called “Basel IV” proposals to establish a capital floor; and President Trump and members of the US Congress have announced steps to review and potentially cut back on requirements implemented by federal agencies under the Dodd-Frank Act.

There is also far more uncertainty than usual over the outlook for economic growth given the United Kingdom’s referendum to leave the European Union (EU); the rise of populist parties in France, Italy, and other European countries that oppose membership in the European Union; and President Trump’s decision to withdraw from the Trans-Pacific Partnership and his pledge to renegotiate trade agreements with China and Mexico. While all of these developments could depress growth, there is also the potential for increased business activity resulting from President Trump’s proposals during the campaign to reduce personal and business taxes, launch a major program of infrastructure investment, and cut regulations on businesses.

When it comes to the business environment, the more widespread emergence of fintech firms has substantially raised the level of strategic risk. These start-ups are threatening to disrupt financial sectors and services such as lending, payments, wealth management, and property and casualty products.

Financial institutions are also responding to two major emerging risks. Cybersecurity has become an ever-greater concern with breaches increasing in number and impact. Another area that has received closer attention from regulators is the need for financial institutions to take proactive steps to encourage ethical behavior among their employees and create a risk-aware culture.

Financial institutions are facing a fiercer battle for talent. The implementation of new and more stringent regulatory requirements has increased the demand for professionals that possess both risk management skills and experience in the financial industry.

The expansion of regulatory requirements over the last several years has led compliance costs to skyrocket, and financial institutions are looking to rationalize their processes and use technology applications to create greater efficiencies.

Viewed in combination, these trends mean that effective risk management is becoming increasingly important. In the current uncertain regulatory and business environment, financial institutions should consider taking their risk management programs in new directions and to a new level to meet the new challenges that lie ahead. At the same time, they will want to develop efficient business processes. This will be especially important as pressures build to restrain risk management spending in a low-growth and low-interest-rate environment. Most important, they will require agile processes and nimble risk information technology systems that will allow them to respond flexibly to potential changes in the direction of regulatory expectations or from disruption caused by fintech players.

We hope that this overall assessment of risk management at financial institutions around the world provides you with useful insights as you work to further enhance your organization’s risk management program.

Sincerely,

Edward T. Hida II, CFA

Risk & capital management leader

Financial services

Deloitte & Touche LLP

Executive summary

THE years since the global financial crisis have seen a wave of regulatory change that increased both the scope and the level of stringency of regulatory requirements. New legislation and regulations have included the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) in the United States, Basel 2.5 and III, the US Federal Reserve's Enhanced Prudential Standards (EPS), the European Market Infrastructure Regulation (EMIR), and Solvency II capital standards. In the years since the global financial crisis, financial institutions have had more time to understand the practical implications of these new regulations and what is required to comply.

Today, risk management is becoming even more important; financial institutions confront a variety of trends that have introduced greater uncertainty than before into the future direction of the business and regulatory environment. Economic conditions in many countries continue to be weak, with historically low interest rates. The UK referendum to leave the European Union (Brexit vote), coupled with US President Donald Trump's pledge to renegotiate trade agreements with China and Mexico, raises the possibility that trade volumes may decline.

The continual increase in regulatory requirements may abate or even be reversed in 2017 as President Trump, the US Congress, and others have questioned whether regulatory oversight has gone too far. Strategic risk is increasing as entrepreneurial fintech players are competing with traditional firms in many sectors. The rapidly

"The external micro and macroeconomic environment is getting more volatile."

— *Chief risk officer,
large diversified financial services company*

changing environment suggests that risk management programs may need to increase their ability to anticipate and respond flexibly to new regulatory and business developments and to emerging risks, for example, by employing predictive analytics tools.

Deloitte's *Global risk management survey, 10th edition* assesses the industry's risk management practices and the challenges it faces in this turbulent period. The survey was conducted in the second half of 2016—after the Brexit vote in the United Kingdom but before the US presidential election—and includes responses from 77 financial services institutions around the world that conduct business in a range of financial sections and with aggregate assets of \$13.6 trillion.

Key findings

Cybersecurity. Only 42 percent of respondents considered their institution to be extremely or very effective in managing *cybersecurity risk*. Yet, cybersecurity is the risk type that respondents most often ranked among the top three that would increase in importance for their institution over the next two years (41 percent). In recognition of the broad senior management and board awareness of cybersecurity risks, most respondents did not report challenges in securing funding or in communicating with senior management or the board. However, many boards of directors face the challenge of securing sufficient technical expertise to oversee the management of cybersecurity risk. The issues cited most often as extremely or very challenging were *hiring or acquiring skilled cybersecurity talent* (58 percent) and *getting actionable, near-real-time threat intelligence* (57 percent).

Institutions less effective at managing newer risk types. Roughly 80 percent or more of respondents said their institution is extremely or very effective at managing traditional risk types such as

liquidity (84 percent), *underwriting/reserving* (83 percent), *credit* (83 percent), *asset and liability* (82 percent), *investment* (80 percent), and *market* (79 percent). Newer risk types present more challenges, and fewer respondents rated their institution highly at managing *model* (40 percent), *third party* (37 percent), and *data integrity* (32 percent). Given the heightened geopolitical uncertainty and change during the period when the survey was conducted, as evidenced by the UK Brexit referendum and the discussion of US trade policies during the US presidential campaign, it is notable that the percentage of respondents who considered their institution to be extremely or very effective at managing *geopolitical risk* was only 28 percent, a sharp drop from 47 percent in 2014.

Significant challenges posed by risk data and IT systems. Few respondents considered their institution to be extremely or very effective in any aspect of risk data strategy and management, such as *data governance* (26 percent), *data marts/warehouses* (26 percent), and *data standards* (25 percent). Even fewer respondents rated their institution this highly in other areas including *data sourcing strategy* (16 percent), *data process architecture/workflow logic* (18 percent), and *data controls/checks* (18 percent). Many respondents also had significant concerns about the agility of their institution's risk management information technology systems. Roughly half of the respondents were extremely or very concerned about *risk technology adaptability to changing regulatory requirements* (52 percent), *legacy systems and*

antiquated architecture or end-of-life systems (51 percent), *inability to respond to time sensitive and ad-hoc requests* (49 percent), and *lack of flexibility to extend the current systems* (48 percent).

Battle for risk management talent. With the increase in regulatory requirements, there has been greater competition for professionals with risk management skills and experience. Seventy percent of respondents said *attracting and retaining risk management professionals with required skills* would be an extremely or very high priority for their institution over the next two years, while 54 percent said the same about *attracting and retaining business unit professionals with required risk management skills*. Since cybersecurity is a growing concern across all industries, the competition is especially intense for professionals with expertise in this area. As noted above, when asked how challenging various issues in managing cybersecurity risk were, the item cited third most often as extremely or very challenging was *hiring or acquiring skilled cybersecurity talent* (58 percent).

Greater use of stress testing. Regulators are increasingly using stress tests as a tool to assess capital adequacy and liquidity, and 83 percent of institutions reported using capital stress testing and the same percentage reported using liquidity stress testing. For both types of stress tests, more than 90 percent of institutions reported using it for *reporting to the board*, *reporting to senior management*, and for *meeting regulatory requirements and expectations*. For both capital and liquidity stress tests, the two issues most often rated

"You need a good combination of analytical (quant) people, especially for advanced analytics and big data. But you need people who do not blindly do advanced analytics. You need business insight and business judgment as well. I think one of the main requirements or expectations is to get much stronger rotations between business and risk management folks. You need to have a much more rotational career to foster mutual understanding."

— *Chief risk officer,
large diversified financial services company*

as extremely or very challenging concern IT systems and data: *stress testing IT platform* (66 percent for capital stress testing and 45 percent for liquidity stress testing) and *data quality and management for stress testing calculations* (52 percent for capital stress testing and 33 percent for liquidity stress testing).

Increased importance and cost of compliance. Thirty-six percent of respondents cited *regulatory/compliance risk* as among the three risk types that will increase the most in importance for their business over the next two years, the risk named second most often. Seventy-nine percent of respondents said that regulatory reform had resulted in an *increased cost of compliance* in the jurisdictions where it operates, and more than half the respondents said they were extremely or very concerned about *tighter standards or regulations that will raise the cost of doing existing business* (59 percent) and the *growing cost of required documentation and evidence of program compliance* (56 percent).

Increasing oversight by boards of directors. Eighty-six percent of respondents said their board of directors is devoting more time to the oversight of risk management than it did two years ago, including 44 percent who said it is devoting considerably more time. The most common risk management responsibilities of boards of directors are *review and approve overall risk management policy and/or ERM framework* (93 percent), *monitor risk appetite utilization including financial and non-financial risk* (89 percent), *assess capital adequacy* (89 percent), and *monitor new and emerging risks* (81 percent). However, there is more work to do in instilling a risk culture, where no more than roughly two-thirds of respondents cited as board responsibilities *help establish and embed the risk culture of the enterprise* (67 percent) or *review incentive compensation plans to consider alignment of risks with rewards* (55 percent).

CRO position almost universal. Ninety-two percent of institutions reported having a CRO position or equivalent, yet there remains significant room for improvement in the role. The CRO does not always report to the board of directors (52 percent), which provides important benefits and is

generally a regulatory expectation. Although the CRO meets regularly with the board of directors at 90 percent of institutions, many fewer institutions (53 percent) reported that the CRO meets with the board in executive sessions. The CRO is the highest level of management responsible for risk management at about half of the institutions (48 percent), with other institutions placing this responsibility with the CEO (27 percent), the executive-level risk committee (16 percent), or the chief financial officer (CFO) (4 percent). The most common responsibilities for the CRO were to *develop and implement the risk management framework, methodologies, standards, policies, and limits* (94 percent), *identify new and emerging risks* (94 percent), and *develop risk information reporting mechanisms* (94 percent). Despite the increasing importance of strategic risk and the related need for risk management of business strategy and decisions, fewer respondents said the CRO has the responsibility to *provide input into business strategy development and the periodic assessment of the plan* (65 percent), *participate in day-to-day business decisions that impact the risk profile* (63 percent), or *approve new business or products* (58 percent). And while regulators have placed greater focus on the importance of conduct and culture, *review compensation plan to assess its impact on risk appetite and culture* was identified as a responsibility by 54 percent of the respondents.

Steady increase in the adoption of ERM. Seventy-three percent of institutions reported having an ERM program, up from 69 percent in 2014 and more than double the 35 percent in 2006. In addition, another 13 percent of institutions said they are currently implementing an ERM program, and 6 percent said they plan to create one. An institution's ERM framework and/or policy is a fundamental document that should be approved by the board of directors, and 91 percent of institutions said this had occurred, up from 78 percent in 2014. Two of the issues frequently cited as extremely or very high priorities for their risk management programs over the next two years concerned IT systems and data: *enhancing risk information systems and technology infrastructure* (78 percent) and *enhancing the quality, availability, and timeliness of risk data* (72 percent). Another

issue considered to be an extremely or very high priority by a substantial majority of respondents was *collaboration between the business units and the risk management function* (74 percent), which is essential to having an effective three lines of defense model.

Evolution of risk management

Over the 20 years that Deloitte has been conducting its *Global risk management survey* series, the financial services industry has become more complex with the evolution of financial sectors, the increased size of financial institutions, the global interconnectedness of firms, and the introduction of new products and services. At the same time, regulatory requirements and expectations for risk management have broadened to cover a wider range of issues and also become more stringent, especially in the years since the global financial crisis. Deloitte's survey series has assessed how institutions have responded to these developments, the substantial progress that has occurred in the maturity of risk management programs, and their challenges. In general over this period, risk management programs have become almost universally adopted, and programs now have expanded capabilities. Boards of directors are more involved in risk management and more institutions employ a senior-level CRO position. The following are some of the key areas where the survey series has documented an increasing maturity in risk management programs.

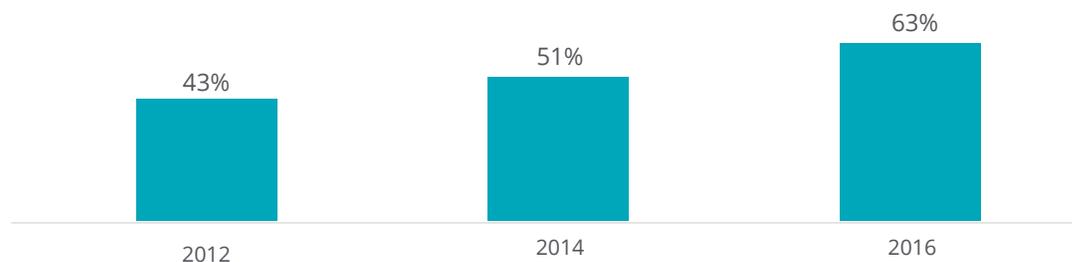
More active board oversight. In 2016, 93 percent of respondents said their board of directors reviews and approves the overall risk management policy and/or ERM framework, an increase from 81 percent in 2012.

More use of board risk committees. It is a regulatory expectation that boards of directors establish a risk committee with the primary responsibility for risk oversight. The use of a board risk committee has become more widespread, increasing from 43 percent of institutions in 2012 to 63 percent in 2016, although there is clearly room for further adoption (figure 1).

Increased adoption of CRO position. Over the years, there has been a continual increase in the percentage of institutions with a CRO position or equivalent, from 65 percent in 2002 to become almost universal with 92 percent in 2016 (figure 2). At the same time, the CRO is a more senior-level position reporting to higher levels of the organization. In 2016, 75 percent of respondents said the CRO reports to the CEO, a substantial increase from just 32 percent in 2002. Similarly, the CRO more often directly reports to the board of directors—at 52 percent of institutions in 2016 up from 32 percent in 2002. Seventy-seven percent of institutions reported that the CRO is a member of the executive management committee, an increase from 58 percent in 2010.

Wider set of responsibilities for the CRO. Over time, the CRO and the independent risk management program have been given a wider

Figure 1. Percentage of institutions placing primary responsibility for risk management at the level of the board of directors with a board risk committee



Source: Deloitte analysis.

Deloitte University Press | dupress.deloitte.com

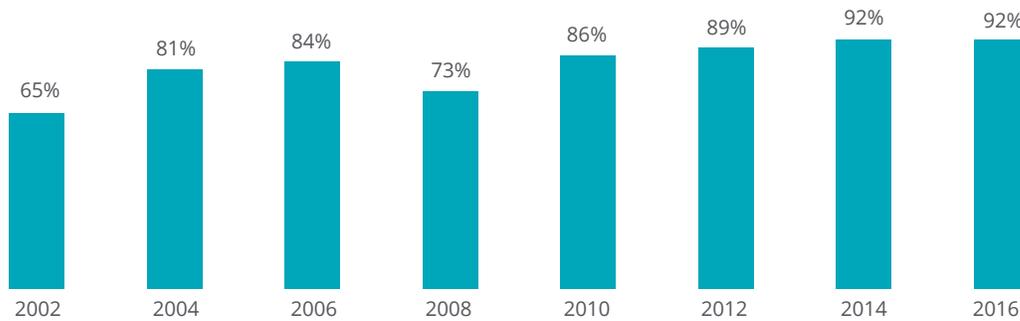
set of responsibilities at many institutions. For example, 92 percent of respondents said a responsibility of the CRO was to *assist in developing and documenting the enterprise-level risk appetite statement* compared with 72 percent in 2008. Similarly, 76 percent said a CRO responsibility is to *assess capital adequacy*, while this was the case at 54 percent of the institutions in 2006.

Widespread adoption of ERM program. The adoption of ERM programs has more than doubled, from 35 percent in 2006 to 73 percent in 2016

(figure 3). The implementation of ERM programs moved upwards in 2010, which was likely due to post-financial crisis focus on enhancing risk management.

While there has been considerable progress in the continued development and maturation of risk management programs, there remains considerable work to do. The specific areas where risk management programs need to further enhance their capabilities and effectiveness, and the likely future challenges, are detailed in the body of this report.

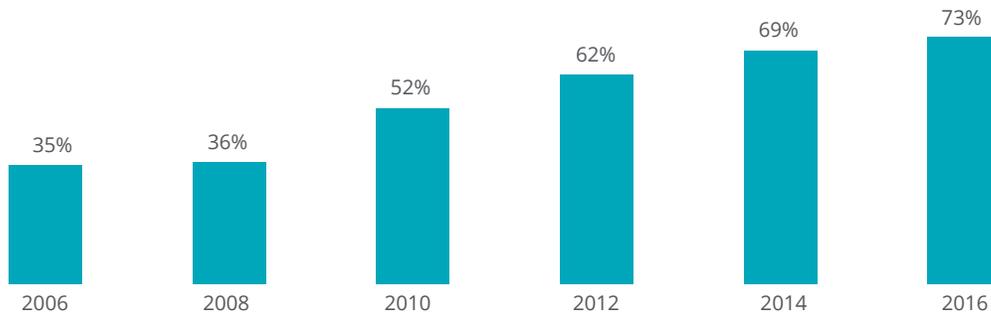
Figure 2. Percentage of institutions with a CRO or equivalent



Source: Deloitte analysis.

Deloitte University Press | dupress.deloitte.com

Figure 3. Percentage of institutions with an ERM program in place



Source: Deloitte analysis.

Deloitte University Press | dupress.deloitte.com

Introduction: Economic and business environment

DELOITTE'S *Global risk management survey, 10th edition* was conducted as a variety of trends were having a dramatic impact on the financial services industry, in some cases with their future direction difficult to predict.

Low-revenue environment

Financial institutions are struggling to generate returns in an environment of historically low interest rates and slow economic growth, coupled with increasing regulatory requirements. The weak economic conditions provide less opportunity to generate revenue and may also increase credit risk. The result has been a greater focus on controlling the cost of risk management programs, with institutions looking to increase efficiency by creating centers of excellence and by rationalizing and consolidating processes, especially in the second line of defense (the independent risk management function).

Global growth in 2016 was expected to be 3.1 percent and then increase to 3.4 percent in 2017, according to the International Monetary Fund (IMF).² The outlook was more modest for developed economies with growth projected to be 1.6 percent in 2016 and 1.8 percent in 2017.

The US economy was expected to grow 1.6 percent in 2016 and 2.2 percent in 2017, while the Euro area was expected to have growth of 1.7 percent and 1.5 percent in these two years. In the wake of the Brexit vote, the United Kingdom was projected to see its growth rate slow from 1.8 percent in 2016 to 1.1 percent in 2017. In Japan, growth was projected to be just 0.5 percent in 2016 and 0.5 percent in 2017. GDP growth in China was predicted to be 6.6

percent in 2016 but slow somewhat to 6.2 percent in 2017.

Weak economic conditions have created challenges for financial institutions. Return on average equity for US banks was 9.0 percent in the third quarter of 2016, compared to 12.2 percent in 2006–2007.³ The performance of European banks was even weaker, with average return on equity of 5.9 percent in the first quarter of 2016, which was below the cost of equity.⁴ An analysis by the IMF found that banks in the European Union were earning less than half of their average 2004–2006 profits.

The IMF found that more than one-quarter of the banks in advanced economies, with about \$11.7 trillion in assets, would remain weak and face continued structural challenges even if a cyclical recovery occurred, with the greatest problems at institutions in Europe and Japan.⁵ Similarly, the ongoing period of low interest rates could call into question the solvency of many insurers.

China has been undergoing a transition toward an economy that is more based on consumption and services and less dependent on manufacturing activity and investment. In addition, it has moved to rely more on markets to set interest rates and exchange rates. However, concerns remain over its rapid increase in debt, including a significant fraction considered at risk, often to state-owned enterprises.⁶

Increasing regulatory requirements for capital and liquidity

Capital requirements include Basel 2.5, III, and the US Federal Reserve's capital plan rule. From mid-2011 through the end of 2015, 91 leading banks

around the world have increased their common equity by \$1.5 trillion, with the ratio of equity to risk-weighted assets rising from 7.1 percent to 11.8 percent. This puts the equity capital ratios of banks substantially above the Basel III minimum of 4.5 percent.⁷

There have been wide variations across banks in the calculations of required capital due to each bank's choice of internal models, which raises questions about transparency and whether some calculations appropriately reflect underlying risk. The Basel Committee on Banking Supervision (Basel Committee) has issued several proposals (the so-called "Basel IV" proposals) to introduce enhanced standardized approaches to eliminate or reduce the role of internal models in calculating minimum capital charges and establish a minimum capital floor. The proposed changes could lead risk-weighted assets to rise by an average of 18 percent to 30 percent, requiring more capital, according to an analysis by Morgan Stanley.⁸

However, there has been some resistance to establishing a capital floor from European banks and officials who believe this would require European banks holding large amounts of low-risk assets such as mortgages to hold more capital, putting them at a competitive disadvantage.⁹ Concerns have also been expressed by the Japan Financial Services Agency (JFSA) and the Reserve Bank of India.¹⁰

US institutions and other global banks operating in the European Union also face a new proposal that would require their EU operations to have separate intermediate holding companies that will be subject to consolidated capital and liquidity requirements.

In the United States, the Federal Reserve has eliminated the qualitative examination portion of its annual Comprehensive Capital Analysis and Review (CCAR) for institutions with less than \$250 billion in assets, and \$75 billion in nonbank assets. The Federal Reserve has also indicated it will issue a proposed rule to effectively embed stress-test results into current capital requirement buffers and implement the surcharge buffer for global systemically important banks (GSIBs).

Among insurers, institutions active in Europe must comply with Solvency II capital requirements, which took effect on January 1, 2016. US insurers must comply with similar Own Risk Solvency Assessment (ORSA) capital requirements put in place by state regulators. US companies subject to ORSA are required to submit an annual filing to their state department of insurance detailing the company's own assessment of its risk profile, the processes in place to manage risks, the potential impact of those risks, and a view on solvency.¹¹ In January 2017, the Treasury Department, acting through the Federal Insurance Office and the Office of the US Trade Representative, announced the successful completion of negotiations for a "covered" agreement with the European Union on prudential measures regarding insurance and reinsurance.¹² Under the agreement, which covers three areas of insurance oversight—reinsurance, group supervision, and the exchange of insurance information between supervisors—US and EU insurers operating in the other market will only be subject to oversight by the supervisors in their home jurisdiction.¹³

Financial institutions have also faced an increasing set of liquidity requirements in the years since the global financial crisis. Liquidity requirements introduced or in the process of implementation include the liquidity coverage ratio (LCR) and the net stable funding ratio (NSFR) introduced in Basel III. Under the enhanced prudential standards (EPS), the US Federal Reserve recently implemented additional liquidity reporting requirements for both US and foreign banks operating in the United States with total consolidated assets of \$50 billion or more. These requirements impact treasury, risk, and operations, particularly around risk management, cash flow forecasting, contingency funding planning, limit setting, stress testing, liquidity buffer sizing and management, and governance, among other areas.¹⁴ In addition, the Federal Reserve 2052a reporting requirement places an additional emphasis providing detailed information to allow the Federal Reserve to monitor the overall liquidity profile of institutions.¹⁵ These and other liquidity requirements are still being finalized or fully implemented and their implications and linkages are still being studied.

Uncertain outlook for regulatory requirements

There are significant questions regarding whether the continual ratcheting up of regulatory requirements since the global financial crisis will continue. As noted above, some European regulators and financial institutions are pushing back on Basel plans to implement a regulatory capital floor as part of its proposed regulatory capital revisions. In the United States, President Trump criticized the Dodd-Frank Act during the presidential campaign, and in February 2017 issued an executive order instructing the Treasury Department to review financial regulations to determine whether they are consistent with the administration's goals such as enhancing the competitiveness of American companies.¹⁶ There have also been various proposals by the US Congress to scale back or eliminate the Dodd-Frank Act that are expected to be refined and re-introduced as legislation in 2017. Although repealing the Dodd-Frank Act would likely not be possible without some Democratic support (since new legislation would require 60 votes in the Senate to overcome a filibuster, and Republicans only have a 52–48 majority), the Trump administration could still make substantial regulatory changes through other means. These include attaching policy riders to appropriation bills or through the budget reconciliation process (which only requires a simple majority in the Senate); changes to agency rules or regulatory guidance within the limitations of the governing laws; and changes to the approaches to rulemaking, supervision, and enforcement at the federal level.

“We don't see regulatory change easing off in the next year to two years, so there's going to be a continuing need to catch up and stay up with that regulatory expectation.”

— *Chief risk officer,
large financial services company*

President Trump will also make a number of appointments to regulatory bodies that have substantial discretionary authority to change regulatory requirements, such as capital and liquidity requirements, including the Federal Reserve, the Securities and Exchange Commission (SEC), the Commodity Futures Trading Commission (CFTC), the Consumer Financial Protection Bureau, and the Financial Stability Oversight Council.

In February 2017, President Trump signed a memorandum instructing the Department of Labor to conduct an updated legal and economic analysis of the proposed Conflict of Interest rule, which had been slated for implementation in April 2017, and rescind or revise the rule if it is found to have adverse impacts.¹⁷ Among the other rules and guidance that fall under the discretionary authority of the various US regulatory agencies are the requirements of the CCAR/DFAST programs and designations of nonbank financial institutions as systemically important.

In another kind of regulatory uncertainty, institutions occasionally receive unexpected regulatory feedback. In their most recent review, the Federal Reserve and the Federal Deposit Insurance Corporation (FDIC) determined that certain resolution plans submitted by the eight GSIBs were “not credible or would not facilitate an orderly resolution” under the US Bankruptcy Code. The agencies provided explicit guidance regarding expectations for the next full resolution plan submissions due by July 1, 2017. The Federal Reserve also extended the resolution plan submission deadline for other filers.

Geopolitical uncertainty

In addition to the potential impact on financial regulations, the political developments in major western economies in 2016 have ushered in a period of geopolitical uncertainty, with potentially far-reaching implications for the future of globalization and trade.

The Brexit vote for the United Kingdom to leave the European Union could have substantial impacts on financial institutions, even those that do not have operations in this region, due to a slowdown in economic activity. In January 2017, UK Prime

Minister Theresa May indicated the intention to negotiate a clean break with the European Union.¹⁸ It is expected that there may be more trade friction between the United Kingdom and the European Union after separation, less free movement of people across these borders, and a more complex and uncertain regulatory environment. Among other impacts, the uncertainty may make it more difficult to predict returns on equity with confidence from UK and EU operations, earnings could decline due to weaker economic activity in Europe, and regulatory standards in the United Kingdom could diverge from those in the European Union.

One consequence of Brexit is that UK-based firms will lose the “passport” ability to distribute their products across the European Union, which is important to the United Kingdom’s role as a financial center. The potential remains that financial firms may be able to continue to distribute some products across the European Union where the UK regulatory regime is considered to be “equivalent.”¹⁹ If firms with UK-based operations lose the ability to distribute their products across the EU market, significant restructuring and relocation may be required across Europe, with firms needing to decide if the related expenditures and disruptions fit their strategic plans.

These impacts on trade would be heightened if other countries join the United Kingdom in deciding to leave the European Union. Populist parties that oppose EU membership have gained ground in France, the Netherlands, Austria, and Italy. In 2017, France will hold a presidential election, in which the National Front, which opposes EU membership, is one of the leading parties. In the wake of the rejection by Italian voters of a constitutional reform package, Italy may also hold an election in 2017, where the populist Five Star Movement that opposes Italy’s membership in the European Union has been gaining ground.

In his first days in office, President Trump signed an executive order withdrawing the United States from the TPP, while during the presidential campaign he supported renegotiating trade agreements with Mexico and China, and proposed placing a tariff on the goods of US companies that move operations outside the country.

Global trade in goods and services is far below its historical pace, having grown just 3 percent since 2012, less than half the average rate over the previous three decades, which may be the result of the simultaneous slowdown in economic growth across both developed and emerging economies. Another factor is the slowdown in China’s economy and the fact that it is coming to rely more on consumption and less on manufacturing investment, which has reduced Chinese imports of commodities and other goods. There had been a rapid increase in Chinese imports over the previous decade, and China now is among the top importers for more than 100 countries that account for roughly 80 percent of world GDP.²⁰ With the possibility that additional countries may leave the European Union and that the United States may renegotiate its trade agreements, it remains to be seen whether additional trade restrictions will be put in place that could further slow global trade and what impact this may have on economic growth.

Focus on role of business in risk management

Institutions are working to more effectively and efficiently implement the three lines of defense risk model governance framework. Under the model, business units (the first line of defense) manage the risks in their areas in order to increase accountability, while the risk management program (second line of defense) is responsible for oversight and challenge. Placing primary responsibility for managing risk in the business units as the first line of defense increases the effectiveness of risk management by leveraging their knowledge of their business activities and operations, while also helping to instill a culture of owning inherent risk in the business.

While this model is conceptually simple and appealing, over time the actual practices implemented have become inefficient, with redundancies and in some cases ineffective areas due to gaps. As a result, institutions are seeking to clearly define the roles and responsibilities of each line, ensure their business units carry out their risk management responsibilities, and align business activities with the institution’s risk appetite and risk management

policies. At the same time, institutions are looking to simplify and rationalize the risk management processes across the lines of defense.

Growing cybersecurity risk

Improving management of cybersecurity risks has been an increasing concern of financial services institutions and has also been receiving greater attention from regulators and policy setters. There is a wide range of types of cyber risks including attacks on operating systems; locking users out of their computers and data; theft or corruption of data and systems; and release of confidential data, intellectual property, or corporate strategy.

“Cyber risk is top of mind for everyone, and probably more the question of when, not if something hits.”

— *Chief Risk Officer,
large diversified financial services company*

Banks, securities companies, investment management firms, insurers, and payment and clearing systems are prime targets for cybercriminals looking to steal money or data, or compromise critical infrastructure, spurred by the large amounts of money involved and the increased use of online and mobile banking. Cyberattacks increased by 50 percent in the second quarter of 2016 compared to the second quarter of 2015, and the number of cyberattacks against financial institutions is estimated to be four times greater than against companies in other industries.²¹ A study in the first quarter of 2016 found that there had been a 40 percent increase in cyberattacks targeting financial institutions.²²

In 2016, the Federal Reserve, the FDIC, and the Office of the Comptroller of the Currency (OCC) issued an advanced notice of proposed rulemaking regarding enhanced cyber risk management and resilience standards for large banks, which may lead

to a more formal proposed rule in 2017. The regulators in the European Union are expected to follow suit. In insurance, in 2015 the National Association of Insurance Commissioners (NAIC) issued a document setting out principles for effective cybersecurity, and cybersecurity has now been integrated into insurance regulatory examinations. Also in the United States, the New York State Department of Financial Services (DFS) proposed prescriptive cybersecurity requirements for banks and insurance companies, which it describes as a “first-in-the-nation cybersecurity regulation.”²³

Managing cyberthreats is also a priority for regulators in Asia Pacific. In May 2016, the Hong Kong Monetary Authority (HKMA) launched the Cybersecurity Fortification Initiative, which includes a mandatory self-assessment of cybersecurity risks faced by financial services institutions, simulation exercises, a professional development program, and the launch of a Cyber Intelligence Sharing Platform.²⁴ The Cybersecurity Law of China, which will take effect on June 1, 2017, will impose obligations on “critical information infrastructure operators” and “network operators” to, among other requirements, keep personal information and important business data collected or generated in China within China, have appropriately qualified dedicated cybersecurity staff, report incidents to data owners and authorities, and conduct annual reviews and assessments of cybersecurity threats. Regulators in Japan, Singapore, and Australia are also focusing on the need for institutions to implement cybersecurity frameworks, predict potential threat scenarios, regularly test security measures, and address any weaknesses identified.²⁵

Central role of conduct and culture

Encouraging ethical conduct among employees and instilling a risk management culture throughout the organization has been a focus of regulators since the global financial crisis. Recently, there have been notable instances of inappropriate behavior at major financial institutions, both in retail markets and wholesale markets, which could lead regulators to give even more attention than before to

conduct and culture. Institutions need to address instances of poor culture, lack of accountability, and misaligned incentive compensation policies, or face the potential for intervention by regulatory authorities.

“This is a tricky area because the whole conduct risk topic itself is emerging, and there’s no established model as to how to get this right. We’ve created a separate area within the second line risk function to oversee conduct risk. We have focused on our risk appetite for conduct risk, our risk management framework for conduct risk, and making sure that that all is aligned with the board’s expectations.”

— *Chief risk officer,
large financial services company*

The European Banking Authority (EBA) has revised guidelines on internal governance, placing more emphasis on conduct, culture, and conflicts of interest. EBA’s stress tests in 2016 assessed an additional €71 billion in losses under an adverse conduct risk scenario, while the Bank of England’s stress tests identified £40 billion of additional conduct risk costs for the seven banks participating.

European insurers should prepare for the implementation of the Insurance Distribution Directive standards on product governance, disclosures, and conflicts of interest. The European Insurance and Occupational Pensions Authority (EIOPA) has made consumer protection a strategic priority for 2017.

In the United States, the Federal Reserve has placed an emphasis on the importance of financial institutions encouraging ethical behavior by their employees through hiring, incentives/compensation, and setting an appropriate ‘tone at the top.’ The Federal Reserve Bank of New York (FRBNY) has held three conferences on culture and behavior in the financial services industry and continues to stress the importance of the issues. US regulators have twice proposed rules on incentive compensation.

Australian regulators are also placing a heavy focus on conduct and culture in the financial services industry. The Australian Prudential Regulation Authority (APRA) released an information paper in late 2016 that assessed risk culture within the industry as being at a very early stage of maturity, called for a deeper analysis and understanding of risk culture across the entire sector, and set out a detailed regulatory work plan that will include pilot reviews and a stocktake of remuneration practices.²⁶

Hong Kong’s Securities and Futures Commission (SFC) recently articulated its expectations with regard to senior management accountability, including the designation of fit and proper individuals to be “managers-in-charge” of core functions and a requirement to submit management structure information and organizational charts.²⁷ The increased focus on this area has made it important for financial institutions to have a formal program for risk management conduct and culture with appropriate resources. To address the complex of conduct, culture, and ethics management, institutions may need to redouble their efforts to align their business practices and incentives/compensation with risk management and integrate risk management considerations throughout day-to-day business practices. Institutions can benefit from employing a risk control self-assessment (RCSA) process in these areas so that management and staff at all levels identify and evaluate the conduct and culture risks facing the institution and the effectiveness of the associated controls. Other institutions have improved their governance and oversight over key business areas that impact conduct. Some institutions are using predictive analytics tools to

identify employee behavior patterns that warrant further investigation.

Fintech disruption

Another source of strategic risk is the more widespread emergence of fintech start-ups, which leverage technology capabilities to compete with traditional banks, investment management firms, and insurers in such areas as loans, payment products, wealth management, and property and casualty insurance. Although still a small segment of the market, fintech firms are expanding at a rapid clip. The investment in fintech has grown from \$1.8 billion in 2010 to \$19 billion in 2015, and in 2015, Goldman Sachs estimated the market to be worth \$4.7 trillion.²⁸ Fintech firms have been able to innovate at a faster pace than traditional institutions, for example, creating loan origination platforms that pull information directly from customer tax records and other financial providers, resulting in a faster, cheaper, less burdensome, and yet more accurate process.

“Ultimately, I think fintech will merge with the banking industry. That could be both beneficial and detrimental to existing players. I think there’s an emerging realization that fintech will bring an awful lot of competition to the banking industry.”

— *Chief risk officer,
large financial services company*

Regulators around the world are examining the impact of fintech on financial regulation. The US OCC announced in December 2016 that it would develop a process for issuing limited special-purpose national bank charters for fintech firms and subject them to prudential supervision.

In Europe, the Financial Stability Board (FSB) is monitoring the potential risks and benefits to financial stability of fintech, with a particular focus on distributed ledger technologies (including blockchain), peer-to-peer lending, and artificial intelligence.²⁹ The European Commission established an internal task force on financial technology and plans to produce policy recommendations during 2017.³⁰ In the United Kingdom, the Financial Conduct Authority (FCA) has launched a “call for input” on crowdfunding, indicating its intention to consider rule changes on the risks in the sector, including the mismatch between the maturity of the loans and the promises of liquidity made to investors.³¹

Asia-Pacific regulators have launched a range of initiatives to nurture and manage the growth of fintech in the region. Many jurisdictions have taken a “regulatory sandbox” approach that allows fintech firms to carry out their activities in a more relaxed regulatory environment (for example, Australia, Hong Kong, Indonesia, Singapore, and South Korea). The Monetary Authority of Singapore is a leader in the region, and has outlined various innovation initiatives including regulatory sandbox guidelines, plans to consult on algorithms for robo-advisers, establishing a national “know-your-customer” utility, and partnering with R3 to develop blockchain.³² In December 2016, the Australian Securities and Investments Commission (ASIC) issued a licensing exemption for fintech firms that it described as “a world first.”³³

Traditional financial institutions are also partnering with fintech firms. For example, in 2015, JPMorgan Chase announced that it would make small business loans through OnDeck Capital, a fintech lending platform.³⁴ Other financial institutions are seeking to adopt the entrepreneurial ways of the fintech firms within their own organizations, for example, by creating online wealth management applications to compete with the new fintech players.

To respond to the shifting business environment brought by fintech and other disrupters, it will be important to have robust strategic risk programs, and some institutions may need to conduct their identification and response planning for strategic risks more frequently. These programs may also

need to develop a new mind-set that considers the potential for a greater degree of disruption than may have been seriously considered in the past. The goal

should be to focus on the ability to maintain stable earnings and survive potential disruption scenarios.

ABOUT THE SURVEY

This report presents the notable findings from the 10th edition of Deloitte’s ongoing assessment of risk management practices in the global financial services industry. The survey gathered the views of CROs or their equivalents at 77 financial services institutions around the world and was conducted from July to October 2016.

The institutions participating in the survey represent the major economic regions of the world, with most institutions headquartered in the United States/Canada, Europe, Asia Pacific, or Latin America (figure 4). Most of the survey participants are multinational institutions, with 61 percent having operations outside their home country.

The participating companies provide a range of financial services, including banking (61 percent), insurance (51 percent), and investment management (45 percent) (figure 5).³⁵

The institutions have total combined assets of \$13.6 trillion and represent a range of asset sizes (figure 6). Institutions that provide asset management services represent a total of \$6.5 trillion in assets under management.

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

Figure 4. Participants by headquarters location

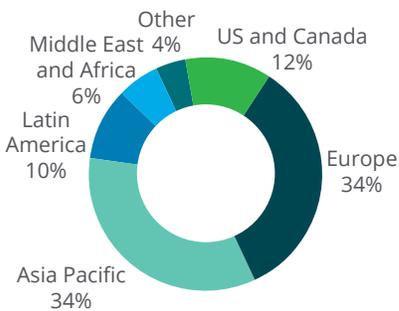


Figure 5. Participants by financial services provided

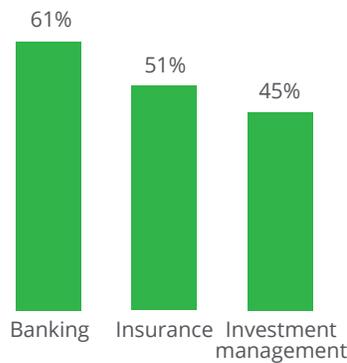
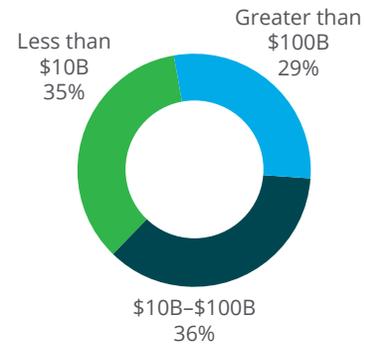


Figure 6. Participants by asset size



Source: Deloitte analysis.

Deloitte University Press | dupress.deloitte.com

Analysis by asset size

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

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

Risk governance

Role of the board of directors

Regulators expect a financial institution's board of directors to play a fundamental role in providing oversight of the risk management program. The Basel Committee has issued principles specifying that a bank's board of directors should have overall responsibility for risk management and that a bank should have an effective independent risk management function.³⁶ The EPS rule issued by the Federal Reserve in March 2014 requires that US publicly traded banks with consolidated assets of \$10 billion or more have a risk committee of the board of directors chaired by an independent director.³⁷ For US banks with consolidated assets of \$50 billion or more, EPS requires that the risk committee must be a stand-alone committee of the board that meets at least quarterly and has at least one independent director knowledgeable of risk management in large, complex banks.³⁸ The US OCC has issued standards requiring large banks to have a board-approved risk-governance framework. For US insurers, in 2014 the NAIC approved a framework for adoption by the state insurance commissioners that requires insurers to file an annual disclosure about their corporate governance practices including the policies and practices of their board of directors.³⁹

In Australia, APRA Prudential Standard CPS 220 Risk Management sets out requirements for regulated institutions (for example, banks and insurers). These requirements include stipulations that boards have a risk management framework for addressing material risks, that the framework include strategic and business planning, and that there is a clearly articulated risk appetite statement that is actively developed and reviewed by the board and communicated appropriately throughout the business operations. Additional requirements are that the regulated institutions have a risk management function, a separate board risk committee, a designated CRO who reports directly to the CEO, and a sound

risk management culture that includes ongoing risk education and processes to ensure behavior is monitored and managed within the risk appetite.⁴⁰

Boards of directors are expected to provide active oversight including approving the risk management framework and risk appetite. Rather than merely receiving periodic briefings, they should be prepared to challenge management decisions and recommendations where appropriate.

Given the increased scope and intensity of regulatory requirements, coupled with a volatile economic environment, most respondents reported that their board of directors is devoting more time to the oversight of risk management compared to two years ago. Forty-four percent of respondents said their board spends considerably more time overseeing risk management than it did two years ago, while 42 percent said it spends somewhat more time.

Respondents at banks were more likely to report their board of directors is spending considerably more time on risk management than it did two years ago (57 percent) than those at investment management firms (43 percent) and insurance companies (44 percent). This is not surprising given the pace and scope of changing regulatory requirements and

"The important change that we worked on is streamlining and optimizing the materials the board gets and moving away from pure reporting to the board towards a substantive discussion of the issues."

— *Chief risk officer,
large diversified financial services company*

Figure 7. Which of the following risk oversight activities does your organization's board of directors or board risk committee(s) perform?



Source: Deloitte analysis.

Deloitte University Press | dupress.deloitte.com

guidance in the banking sector, a large part of which either is focused specifically on risk management or else has large effects on risk management.

Boards of directors, and their risk committees, have a wide range of risk management responsibilities. A number of traditional risk management functions are responsibilities of boards at almost all institutions including *review and approve overall risk management policy and/or ERM framework* (93 percent), *monitor risk appetite utilization including financial and nonfinancial risk* (89 percent), *assess capital adequacy* (89 percent), and *monitor new and emerging risks* (81 percent) (figure 7).

On the other hand, there is room for improvement at many institutions on a number of issues that have recently received attention. Strategic decisions can have a substantial impact on an institution's risk profile, and one might have expected that more than about two-thirds of institutions would say their board's activities include *review corporate strategy for alignment with the risk profile of the organization* (68 percent). And while regulators have recently placed greater focus on the important role that culture plays in effective risk management, the board oversight activities at many institutions did not include *help establish and embed the risk culture of the enterprise* (67 percent) or *review*

incentive compensation plans to consider alignment of risks with rewards (55 percent).

Board risk committees

Placing oversight responsibility for risk management with a board risk committee is a general regulatory expectation and has come to be seen as a leading practice. The Basel Committee issued guidance in 2010 that stressed the importance of a board-level risk committee, especially for large banks and internationally active banks, and revised guidance in 2015 specifying the appropriate role of the risk committee.⁴¹ As noted above, the EPS issued by the Federal Reserve establishes certain requirements for US banks to have a risk committee of the board of directors, with some requirements phased in based on size of institution.

Sixty-three percent of institutions reported they have a risk committee of the board of directors with primary responsibility for risk oversight, up from 51 percent in 2014. As a result of the ascendance of the board risk committee, only 16 percent said the full board has primary responsibility, down from 23 percent in the prior survey. Some respondents said oversight was a combined responsibility of the board audit and risk committees (8 percent) or other board committees (9 percent).

Placing primary responsibility in a board risk committee is much more common in the United States/Canada (89 percent, up from 61 percent in 2014), than in Europe (65 percent), Asia Pacific (52 percent), or Latin America (63 percent). This may

be a response to the requirements of the Federal Reserve’s EPS and OCC’s heightened standards regarding board risk committees.

A prominent role for board risk committees is more common at banks (74 percent compared to 56 percent in 2014), although it also rose at investment management firms (65 percent up from 44 percent) and insurers (61 percent up from 49 percent).

As noted, there has been a trend for regulators to require that financial institutions include independent directors in their board risk committees. The Federal Reserve’s EPS requires that the risk committee include at least one independent director, while the US OCC regulations increased the required number to two independent directors.

The survey found that the trend toward independent directors on the board risk committee has become pronounced. Forty-five percent of institutions reported that their board risk committee includes two or more independent directors (as well as other directors), while 36 percent said it is composed entirely of independent directors (figure 8). Only 5 percent of institutions said their board risk committee contains only one independent director, while at 13 percent of institutions the risk committee does not contain any independent directors.

Having the risk committee chaired by an independent director and having the participation of a risk management expert are becoming regulatory expectations for larger institutions. Many institutions find that in practice it is easier to have independent

Figure 8. 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 due to rounding.

Source: Deloitte analysis.

Deloitte University Press | dupress.deloitte.com

directors as members of their risk committee, or even be chaired by an independent director, than to secure the participation of an identified risk management expert. Seventy-two percent of institutions reported that their board risk committee is chaired by an independent director, while 67 percent have a risk management expert on their committee.

Having an identified risk management expert is most common in the United States/Canada (78 percent), Asia Pacific (72 percent), and Latin America (86 percent) and is less common in Europe (52 percent). One reason for the lower prevalence in Europe is that European regulations contain a more general requirement that risk committee members “...shall have appropriate knowledge, skills and expertise to fully understand and monitor the risk strategy and the risk appetite of the institution.”⁴²

Role of the CRO

Having an independent risk management function headed by a CRO is a regulatory expectation. The Basel Committee guidance on governance recommends that large banks and internationally active banks have a risk management function and a CRO position with “sufficient authority, stature, independence, resources and access to the board.”⁴³

Adoption of a CRO position is almost universal, with 92 percent of institutions reporting that they have a CRO or equivalent position. The CRO position is more common at institutions in the United States/Canada (89 percent) and Europe (92 percent) than in Asia Pacific (73 percent) or Latin America (63 percent).

There are significant benefits, and a general regulatory expectation, for the CRO to report directly to the board of directors as well as to the CEO, but this is not the case at many institutions. The CRO reports to the board of directors at 52 percent of the institutions surveyed, up slightly from 48 percent in 2014. Further, the CRO reports to the CEO at 75 percent of institutions, meaning that at one quarter of the institutions the CRO does not report to the most senior management executive in the organization. It appears that many institutions have more

work to do to improve the reporting structure for their CRO.

At 90 percent of institutions, the CRO meets regularly with the board of directors or board committees responsible for risk management, although fewer (53 percent) reported that their CRO meets in executive sessions with the board. Affording the CRO the opportunity to meet with the board of directors or the board risk committee without the CEO or other members of senior management present can provide the board with an opportunity to receive a frank assessment of the state of the risk management program and the specific challenges the institution faces.

Latin American institutions were least likely to say their CRO reports to the board of directors (14 percent), compared to 50 percent or greater in other regions, and 52 percent of Latin American institutions said their CRO reports to the CEO, while this figure is more than two-thirds in other regions. Twenty-nine percent of respondents at Latin American institutions said the CRO reports to the CFO, while this is the case with less than 10 percent of institutions in other regions.

It is a leading practice for the CRO to be the most senior management position responsible for the risk management program, but the CRO does not universally have this role. Only 48 percent of institutions reported that the CRO or equivalent is the highest level of management responsible for the risk management program, similar to the percentage in 2014. Other common responses were the CEO (27 percent), the executive-level risk committee (16 percent), or the CFO (4 percent). Assigning primary responsibility for risk management to the CRO is more common among institutions in the United States/Canada (78 percent) than in Europe (50 percent), Asia Pacific (38 percent), or Latin America (25 percent).

Institutions assign a broad range of responsibilities to the firm-wide, independent risk management group headed by the CRO. Many oversight activities were nearly universal including *develop and implement the risk management framework, methodologies, standards, policies, and limits* (94 percent), *identify new and emerging risks* (94 percent), and

develop risk information reporting mechanisms (94 percent).

However, a number of other important oversight activities are in place at no more than two-thirds of institutions including *provide input into business strategy development and the periodic assessment of the plan* (65 percent) and *participate in day-to-day business decisions that impact the risk profile* (63 percent). Risk management considerations need to be infused into both strategy and business decisions to consider their risk implications, and more progress still needs to be made in these areas.

Another area that a relatively low percentage of respondents said was a responsibility of the risk management program was *approve new business or products* (58 percent). This may be partly explained by the fact that relatively few new products are being introduced in the current economic and regulatory environment.

Finally, regulators and industry leaders have devoted considerable attention to the role that incentive compensation and culture play in risk management, yet the activity *review compensation plan to assess its impact on risk appetite and culture* was identified as a responsibility by 54 percent of respondents. This was more often a risk management responsibility at institutions in the United States/Canada (75 percent) and Europe (62 percent) than in Asia Pacific (38 percent) and Latin America (43 percent).

Risk appetite

A written risk appetite statement provides guidance for senior management when setting an institution's strategic objectives, and for lines of business when making business decisions. The idea of a risk appetite has been around for some time but has received renewed attention since the global financial crisis. The FSB issued principles for an effective risk appetite framework in November 2013.⁴⁴ In 2015, the Basel Committee issued guidance that stressed the role of the board of directors in establishing, along with senior management and the CRO, the institution's risk appetite.⁴⁵

There is now wide adoption of a written, enterprise-level risk appetite statement approved by the board of directors. Eighty-five percent of institutions reported they have such a statement approved by the board of directors, up from 75 percent in 2014. The regulatory focus on risk appetite began in banking, where 91 percent reported either having a risk appetite statement approved by their board of directors or being in the process of developing a statement and securing approval. But risk appetite statements have now also become common in investment management firms (83 percent) and insurance companies (85 percent).

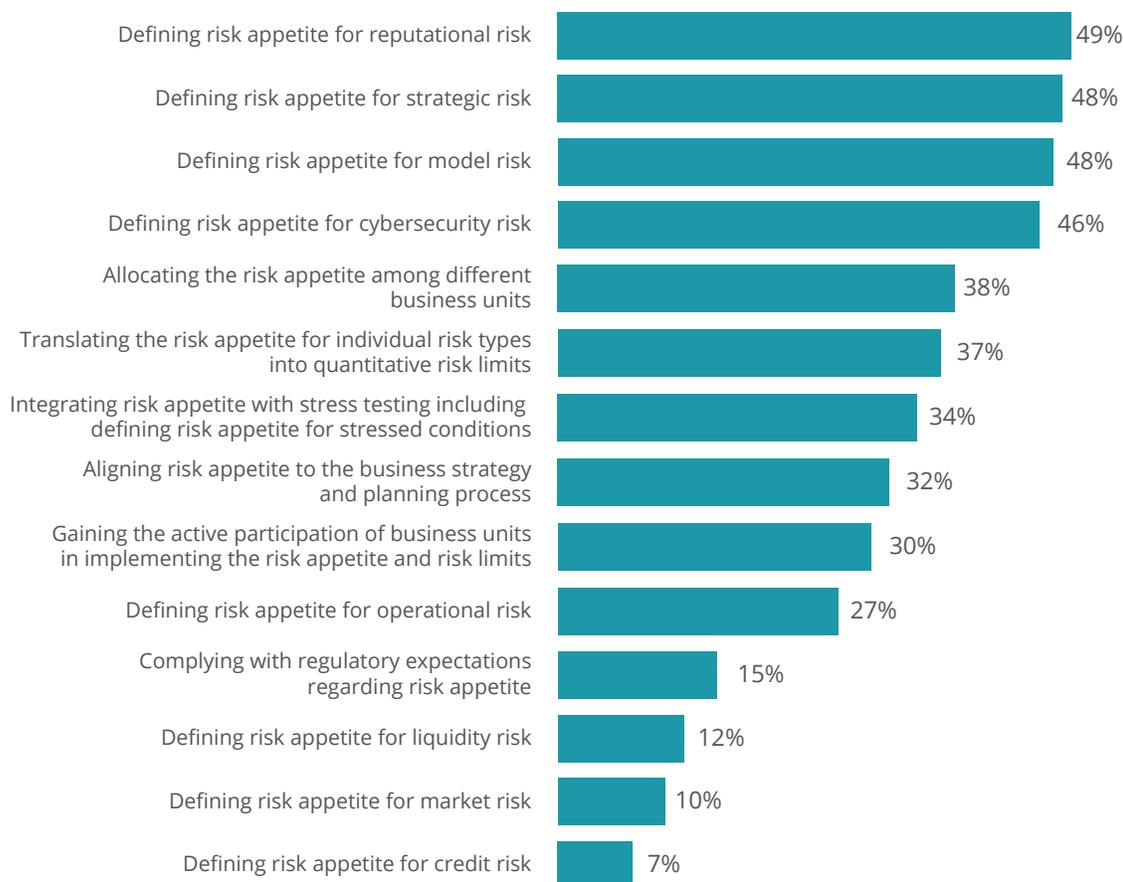
"We revised our risk appetite statement and introduced a lot more qualitative description of our risk appetite and the different risk categories and how that fits with the corporate purpose. That qualitative aspect was absent from our previous risk appetite. The second big change was that we revised the quantitative metrics."

— **Chief risk officer,**
large financial services company

There are challenges in developing a risk appetite statement that provides useful guidance to the business. Respondents most often said that it is extremely or very challenging to define risk appetite for newer risk types such as *reputational risk* (49 percent), *strategic risk* (48 percent), *model risk* (48 percent), and *cybersecurity risk* (46 percent) (figure 9). Each of these risk types poses challenges in defining and measuring risk. For example, strategic risk requires an assessment of the risk posed by an institution's business strategy, while reputational risk is typically a secondary risk that results from market, credit, operational, or other types of

Figure 9. How challenging is each of the following in defining and implementing your organization's enterprise-level risk appetite statement?

Percentage responding extremely challenging or very challenging



Source: Deloitte analysis.

Deloitte University Press | dupress.deloitte.com

risk events that spread to have wider impacts to the organization and is thus difficult to measure and establish limits for.

Operational risk has been an area where many institutions had struggled to develop appropriate analytical approaches that would allow them to measure and set risk limits. However, more attention has been paid to this area, and it appears that progress is being made. Twenty-seven percent of respondents said that defining risk appetite for *operational risk* is extremely or very challenging, down from 38 percent in 2014.

In contrast, the issues that were least often seen as extremely or very challenging were defining risk

appetite for traditional risk types such as *liquidity risk* (12 percent), *market risk* (10 percent), and *credit risk* (7 percent). Institutions generally have many years of experience in these areas and have developed data and analytical methods that allow them to quantify the risk and set appropriate risk limits.

Respondents at European institutions were more likely than those in other regions to say that a number of issues were extremely or very challenging including *defining risk appetite for strategic risk* (58 percent compared to 38 percent in United States/Canada) and *defining risk appetite for reputational risk* (63 percent compared to 38

percent in United States/Canada and 36 percent in Asia Pacific). On the other hand, *defining risk appetite for operational risk* was more often seen as extremely or very challenging by institutions in the United States/Canada (50 percent) and Latin America (43 percent) than those in Europe (24 percent) and Asia Pacific (19 percent).

It is also challenging to further allocate and delegate risk appetite from the overall risk appetite statement down to risk limits in the various operations and business unit activities of an institution. In some institutions, the development of risk appetite allocations and delegations to business units remains a work in progress as more granular measures are developed. Other important activities were less often considered to be extremely or very challenging but still pose difficulties for many institutions such as *allocating the risk appetite among different business units* (38 percent), *translating the risk appetite for individual risk types into quantitative risk limits* (37 percent), and *integrating risk appetite with stress testing including defining risk appetite for stressed conditions* (34 percent).

Three lines of defense risk governance model

A “three lines of defense” risk governance model is a regulatory expectation and has been accepted as a leading practice so that business units, the risk management program, and internal audit each play their appropriate role in risk management. 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

The three lines of defense model is now essentially universally adopted, with all the institutions participating in the survey reporting that they employ it.

Although this model is conceptually sound, practical implementation can present difficulties, especially in large institutions with multiple business units and locations. For a start, an institution needs to have enough skilled personnel in each line of defense. The industry-wide competition for experienced risk management professionals has made it more difficult to hire employees with risk management skills. Business units in particular may find it difficult to attract professionals who have experience both in risk management and also in the business. In fact, *having sufficient skilled personnel in all three lines of defense* (64 percent) was the issue most often considered to be a significant challenge in implementing the three lines of defense risk governance model.

The other issues rated as significant challenges revolved around the business units (Line 1) and their interaction with risk management (Line 2). The issue cited next most often as extremely or very challenging was *defining and maintaining the distinction in roles between Line 1 (the business) and Line 2 (risk management)* (55 percent, up from 51 percent in 2014). Business units need to buy into the process and have good collaboration with the risk management function. Too often the three lines of defense model can result in duplication of controls and reviews across the three lines (resulting in so-called “checkers checking the checkers”), and eliminating this redundancy requires clarifying the roles and responsibilities of each group involved.

A third issue cited frequently as extremely or very challenging was *getting buy-in from Line 1 (the business)* (44 percent up from 36 percent in 2014). The business unit executives in Line 1 need to assume responsibility for risk in their daily activities, rather than simply delegating risk management to specific personnel in “risk” roles. Business units need to ensure that material risks associated with their activities are assessed and that there are adequate control mechanisms to manage them, including compliance and conduct testing processes, quality assurance procedures, and problem escalation processes.

Yet, getting buy-in from business units can be difficult since business units are measured on the

revenue generated rather than specifically on risk management activities. Overcoming this resistance requires instilling a culture throughout the organization that communicates that identifying and managing risks is an important responsibility of the businesses.

There is a longer tradition of employing the three lines of defense model in the United States/Canada and Europe, which was reflected in the survey. For example, *having sufficient skilled personnel in all three lines of defense* was more often cited as extremely or very challenging by respondents at institutions in Asia Pacific (77 percent) and Latin America (75 percent) than those in United States/Canada (56 percent) or Europe (46 percent). Similarly, respondents less often considered *getting buy-in from Line 1 (the business)* to be extremely or very challenging for the United States/Canada (44 percent) and Europe (42 percent) than in Latin America (63 percent). On the other hand, institutions in the United States/Canada are still struggling with *defining and maintaining the distinction in roles between Line 1 (the business) and Line 2 (risk management)*, where 78 percent rated it as extremely or very challenging compared to less than 60 percent in other regions.

Institutions have taken different approaches to the three lines of defense model, with some centralizing more activities and others decentralizing more activities into the business units. One of the decisions that institutions need to make is where to locate the enterprise control testing function of the risk and control framework. Institutions that take a more decentralized approach have, in effect, split Line 1 into business unit risk management activities (Line 1A) and testing activities (Line 1B), with Line 2 handling monitoring, policy, and challenge, and Line 3 conducting additional testing. However, this can lead to redundancy in the testing program.

A strict interpretation of the three lines of defense model would suggest that the testing function should be centralized in internal audit (Line 3), but this is only the case at 31 percent of institutions. The remaining institutions take a variety of approaches: *embedded within the second line of defense centralized control testing function* (23 percent),

performed in various functions (20 percent), *embedded within the second line of defense risk team* (17 percent), and *embedded within the first line of defense in the business unit* (7 percent).

“Our focus has been on simplifying the operating model for operational risk, pushing more accountability into the true front line, and making sure that we don’t have redundant effective challenge functions.”

— **Senior risk executive,
large diversified financial services company**

A similar organizational challenge is presented by specific risk types. For management of each risk type (or “stripe”), should there be executive accountability where a single individual is responsible for oversight of the risk across the organization or should responsibility be decentralized to individual business units? Most institutions have a single individual accountable for risk oversight of traditional risk types such as *liquidity risk* (76 percent), *regulatory/compliance risk* (76 percent), *market risk* (75 percent), and *credit risk* (72 percent). Banks are more likely to have a single individual accountable for these traditional risk types—*liquidity* (87 percent), *regulatory/compliance* (84 percent), *market* (89 percent), and *credit* (81 percent)—compared to less than 80 percent for investment management firms and insurance companies. This established executive accountability is logical, given the greater regulatory focus on bank risk management programs.

Substantial majorities of institutions also have a single individual accountable for *cybersecurity risk* (67 percent) and *operational risk* (65 percent). Cybersecurity risk has received increased attention recently, and 100 percent of the institutions in the United States/Canada reported having a single individual responsible compared to fewer in

Europe (62 percent), Asia Pacific (60 percent), and Latin America (75 percent). The risk where oversight is least likely to be centralized is *third-party risk*, where 44 percent of institutions have a single

individual accountable for oversight, including just 26 percent of European institutions and only 32 percent of insurance companies.

Enterprise risk management

AN ERM program is designed to create an overall process to identify and manage risks facing an institution. Establishing an enterprise-wide program helps prevent important risks from being overlooked, identifies interrelationships among risks in different lines of business or geographic areas, and aligns risk utilization with the organization's risk appetite. Regulatory authorities are encouraging financial institutions to implement ERM programs and leverage their insights when setting business strategy or making important business decisions.

The adoption of ERM programs is widespread, with 73 percent of institutions reporting they have an ERM program. In addition, another 13 percent of institutions said they are currently implementing an ERM program, while 6 percent said they plan to create one in the future.

ERM programs are more common in the United States/Canada (89 percent) and Europe (81 percent), where this has been a focus of regulatory authorities, than in Asia Pacific (69 percent) or Latin America (38 percent). However, 50 percent of the respondents at institutions in Latin America said their institution is currently implementing an ERM program.

The ERM framework and policy are fundamental documents governing risk management in an institution and should be reviewed and approved by the board of directors or the board risk committee, and this now occurs at almost all institutions. Ninety-one percent of institutions reported having an ERM framework and/or policy that has been approved by the board of directors, indicating the maturity of the large majority of ERM programs. The board role in approving the ERM framework and/or policy is less common in Latin America (71 percent) than in the United States/Canada (100 percent), Europe (95 percent), and Asia Pacific (91 percent).

Institutions have a wide range of priorities for their risk management programs over the next two years. Two of the issues rated frequently by respondents as extremely or very high priorities involved IT systems and data: *enhancing risk information systems and technology infrastructure* (78 percent) and *enhancing the quality, availability, and timeliness of risk data* (72 percent) (figure 10).

“What we need to do over the next two years or so, is consolidation of those practices, streamlining of processes that will enhance effectiveness of the risk management organization.”

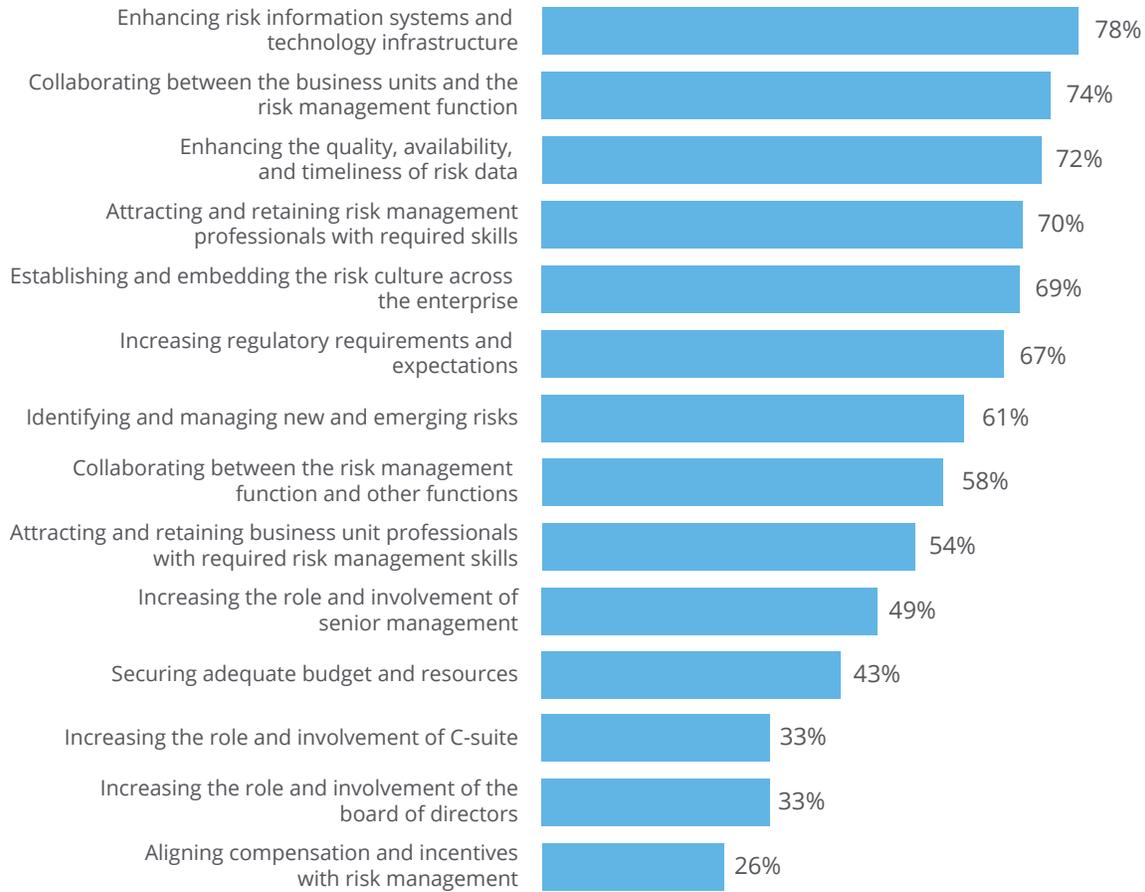
— *Chief risk officer,
large diversified financial services company*

Another issue considered to be an extremely or very high priority by a substantial majority of respondents was *collaboration between the business units and the risk management function* (74 percent), which is essential to having an effective three lines of defense model. This result is consistent with the fact that 55 percent of respondents said that *defining and maintaining the distinction in roles between Line 1 (the business) and Line 2 (risk management)* was a significant challenge in implementing the three lines of defense risk governance model. (See the section “Three lines of defense risk governance model.”)

With the increase in regulatory requirements, financial services institutions have expanded their risk management personnel both in the risk management function and in business units, and as a result

Figure 10. Over the next two years, how much will each of the following be a priority for your organization in risk management?

Percentage of institutions responding extremely high priority or very high priority



Source: Deloitte analysis.

Deloitte University Press | dupress.deloitte.com

the competition for these professionals has been intense. Seventy percent of respondents said that *attracting and retaining risk management professionals with required skills* would be an extremely or very high priority for their institution.

Reflecting the fact that regulatory authorities have increased their attention to the importance of instilling a risk management culture, 70 percent of respondents cited *establishing and embedding the risk culture across the enterprise* as a high priority.

In the current low-revenue environment for financial institutions, there is pressure to reduce risk management costs, and 43 percent of respon-

dents said that *securing adequate budget and resources* will be an extremely or very high priority. Institutions are looking for opportunities to increase efficiency by rationalizing and consolidating their risk management programs. An emerging trend is for institutions to leverage new technologies in this effort such as cognitive and advanced analytics techniques to identify behavior patterns and predictive analytics to identify emerging risks. Robotics process automation (RPA), such as automated workflow and decisioning tools triggered by a robot function, is also being used to reduce costs and improve quality by automating routine tasks. The use of these new technology tools is still nascent, although some institutions are pursuing the use of

“We are making focused investments in automation, for example, in scoring models for some of our small and medium enterprise businesses, and investments in workflow management tools and so on.”

— **Chief risk officer,
large diversified financial services company**

fully automated compliance testing by leveraging these RPA technologies.

The drive to restrain costs is challenged by increased regulatory expectations for risk management. Forty-four percent of respondents expected their institution’s annual spending on risk management would increase by 10 percent or more over the next two years, including 13 percent who expected an increase of more than 25 percent. These figures are an increase from 2014, when 37 percent of respondents expected an increase of 10 percent or more and 9 percent expected an increase of 25 percent or more.⁴⁶

The issues that relatively few respondents rated as challenging were also instructive. Only 33 percent of respondents said that *increasing the role and involvement of C-suite in risk management* was an extremely or very high priority, and the percentage was the same for *increasing the role and involvement of the board of directors in risk management*, suggesting that most institutions have already addressed these issues. The lowest-rated issue was *aligning compensation and incentives with risk management* (26 percent). Although there had been considerable attention paid to compensation issues in the immediate aftermath of the global financial crisis, it appears that most institutions have decided that other issues are more pressing. Given the continuing focus on conduct and culture, more focus may be needed on compensation and incentives.

There were a number of interesting differences in the priorities for risk management across regions. In the United States/Canada (100 percent) and Europe (81 percent), respondents were more likely to cite *increasing regulatory requirements and expectations* as a priority over the next two years than were respondents in Asia Pacific (52 percent) and Latin America (25 percent), which reflects the pace of regulatory change in these regions. *Enhancing the quality, availability, and timeliness of risk data* is also more often a priority in the United States/Canada (100 percent) and Europe (88 percent) than in Asia Pacific (56 percent) and Latin America (50 percent). *Increasing the role and involvement of the board of directors* was most often cited as a priority in Europe (42 percent) and least often in the United States/Canada (11 percent), where this has been a focus of attention for the last several years.

The issue most often cited as a priority by respondents in Asia Pacific (71 percent) was *establishing and embedding the risk culture across the enterprise*, which was also named often in the United States/Canada (78 percent) and Latin America (75 percent) but less often in Europe (58 percent).

In Latin America, respondents most often cited *collaboration between the business units and the risk management function* (100 percent) compared to roughly three-quarters in the United States/Canada and Europe and 60 percent in Asia Pacific.

When it came to financial sectors, respondents at banks were more likely to cite *securing adequate budget and resources* (50 percent) as a priority, than were those in investment management firms (44 percent) and insurance companies (42 percent), which is expected given the low-revenue environment for the banking industry. The role of compensation and incentives in risk management has received attention from bank regulators, and respondents at banks were also more likely to cite as a priority *aligning compensation and incentives with risk management* (37 percent) than were those in investment management firms (18 percent) or insurance companies (18 percent).

Economic capital

ECONOMIC capital is a tool employed by many financial institutions to assess their risk-adjusted performance and allocate capital, and all the financial institutions participating in the survey said they calculate economic capital. Institutions most often calculate economic capital for traditional risk types including *credit* (93 percent, up from 68 percent in 2014), *operational* (82 percent, up from 62 percent), *market* (79 percent, up from 72 percent), and *counterparty credit* (64 percent, up from 51 percent) (figure 11).

Economic capital is used much less often for some newer risk types, where it is more challenging to model risks, including *cybersecurity risk* (15 percent), *reputational risk* (13 percent), and *systemic risk* (7 percent).

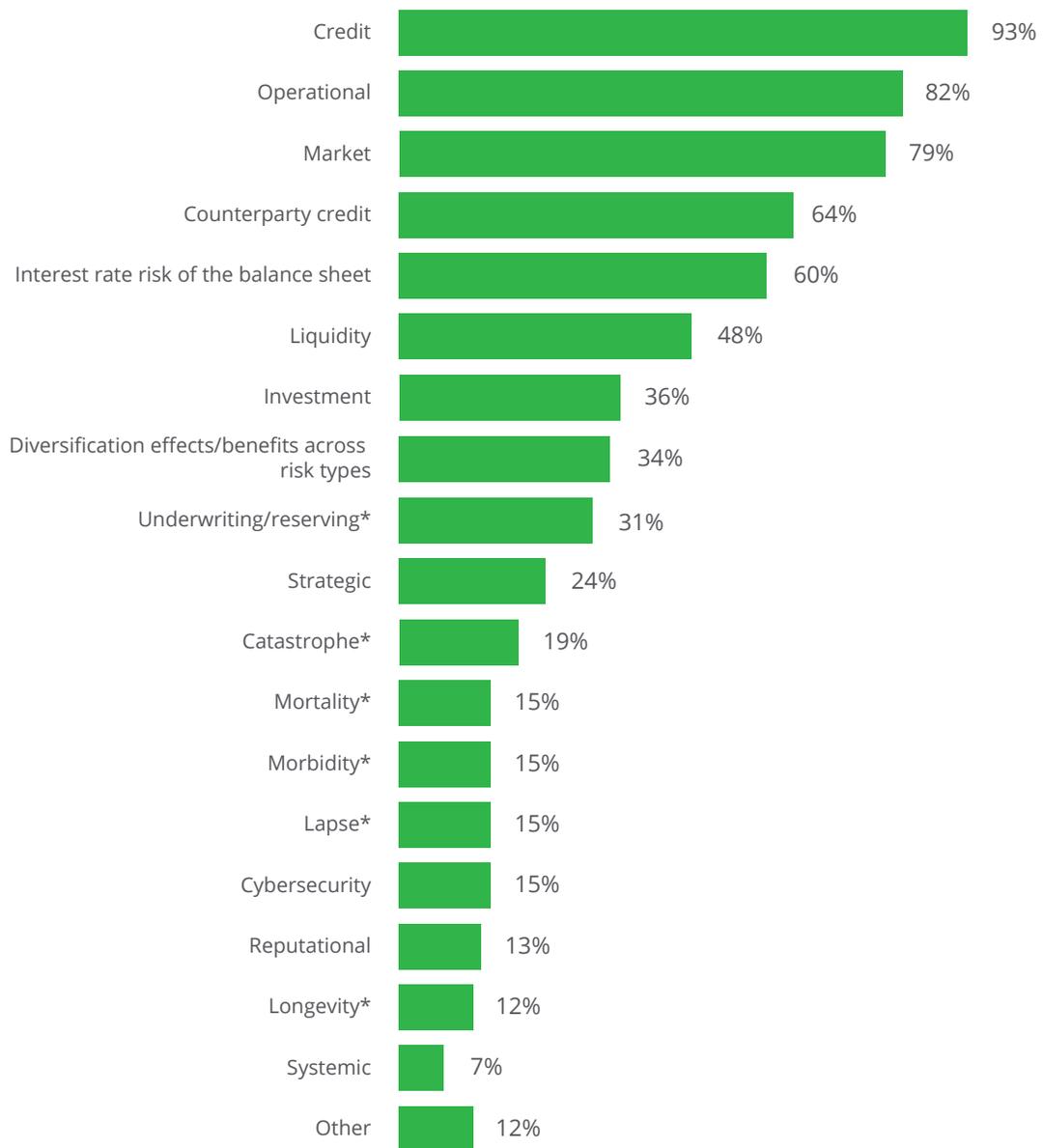
When asked how their institution used economic capital, respondents most often said it is used *at the enterprise level to evaluate/allocate economic capital* (76 percent), *at the senior management level for strategic decision making* (69 percent), and *at the board level for strategic decision making* (64 percent). It is used less often at lower levels for business decisions although somewhat more than in the prior survey including *at the customer level to support risk-based profitability analysis* (41 percent, up from 32 percent in 2014), *at the busi-*

ness unit level to evaluate risk-adjusted performance (53 percent, up from 45 percent), *at the desk/product level for risk/return optimization of product mix* (50 percent, up from 37 percent), and *at the transaction level for risk-based pricing* (53 percent, up from 44 percent).

However, fewer respondents than in 2014 said economic capital was used *extensively* in several areas including *at the enterprise level to evaluate/allocate economic capital* (27 percent, down from 34 percent), *at the senior management level for strategic decision making* (20 percent, down from 24 percent), and *at the board level for strategic decision making* (16 percent, down from 23 percent).

Economic capital received criticism after the global financial crisis for not performing as well as expected. Although economic capital was introduced as a more sophisticated approach than the regulatory capital requirements current at the time, regulatory capital requirements, and specifically stressed capital requirements, such as for CCAR, have subsequently become more sophisticated and a greater focus by many institutions, especially large banks. (See “Sector spotlight: Banking” and “Sector spotlight: Insurance.”)

Figure 11. For which of the following risk types does your organization calculate economic capital?



*Only asked of institutions that provide insurance services.

Source: Deloitte analysis.

Deloitte University Press | dupress.deloitte.com

Stress testing

Capital stress testing

Since the global financial crisis, there has been an increased reliance by regulatory authorities on stress tests to determine whether a financial institution has sufficient capital. The Federal Reserve, the European Central Bank, the Bank of England, and EIOPA for insurers are among the regulatory authorities that require financial institutions to conduct stress tests. The Federal Reserve had indicated that it will issue a proposed rule to effectively embed stress-testing results into current capital requirement buffers, although it is not clear whether the proposal will be finalized.⁴⁷ In addition, in the United States, the Federal Reserve's capital plan rule goes beyond stress tests and capital adequacy to address a range of issues such as risk appetite, risk identification, data quality, model validation, and financial planning projections. In Australia, the APRA is tasked with ensuring bank capital ratios remain the top quartile of internationally active banks, and it has extended stress testing to the life insurance sector.⁴⁸ In Japan, the JFSA has already commenced supervisory stress testing for systemically important banks using the regulator's stress-test scenarios.⁴⁹ The JFSA has also provided examples of advanced, standard, and limited stress-testing approaches for insurers, and has announced that it will expect larger Japanese insurers to incorporate advanced stress-testing practices going forward.⁵⁰

Eighty-three percent of institutions reported using capital stress testing, with this tool more common in the United States/Canada (89 percent) and Europe (92 percent) than in Asia Pacific (77 percent) or Latin America (75 percent).

Almost all institutions reported using the results of capital stress tests in *reporting to senior management* (94 percent including 49 percent that use it extensively) and in *reporting to the board* (94 percent, including 46 percent that use it extensively).

“Stress testing has evolved where we’re not just thinking about the balance sheet under stress, but also the income statement. Historically we’ve been very balance-sheet focused and haven’t really spent much time thinking about business model risk, and I see that as a focus for the future.”

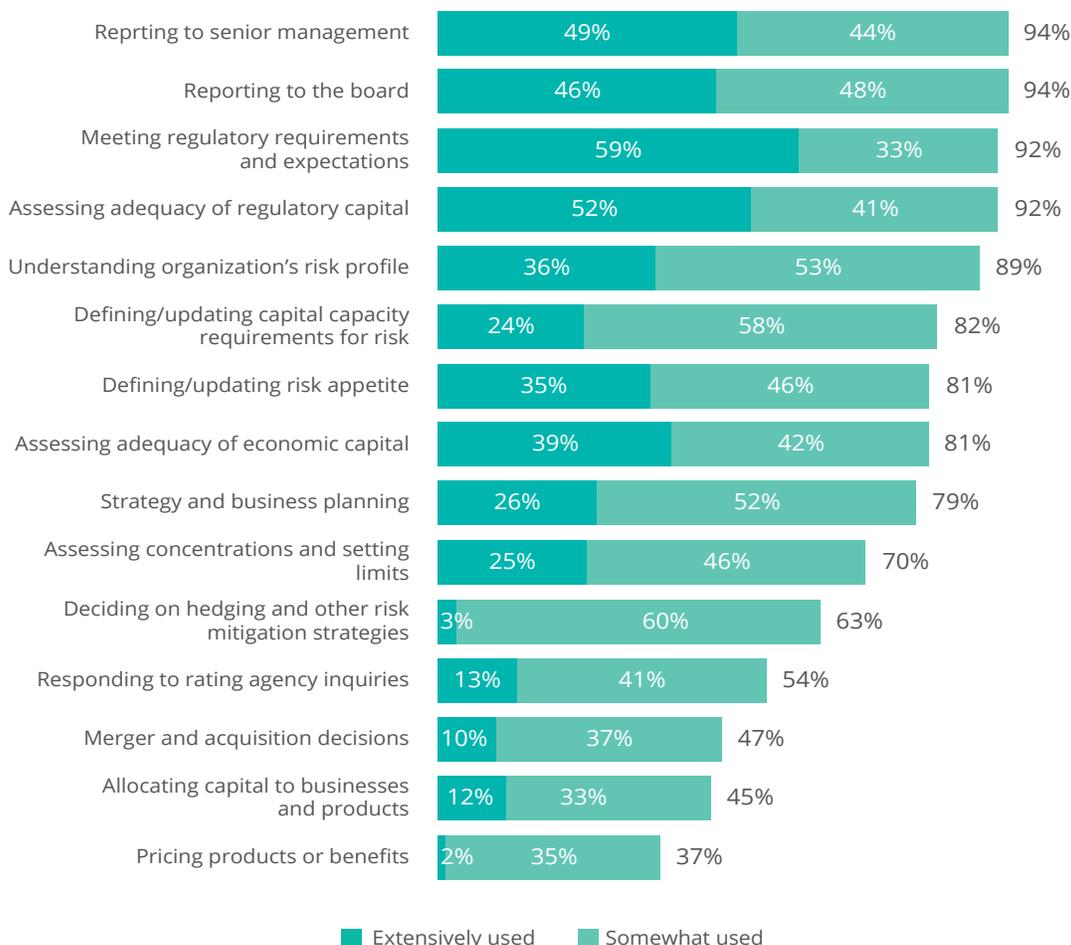
— *Senior risk executive,
large diversified financial services company*

It is apparent that regulatory requirements are the primary driver in the use of capital stress tests. In the United States, for many large banks, the post-stress requirements of the Federal Reserve's capital plan rule have become the binding regulatory capital constraint. More than 90 percent of institutions reported using the results of capital stress tests in *meeting regulatory requirements and expectations* (92 percent, including 59 percent that use it extensively) and *assessing adequacy of regulatory capital* (94 percent, including 52 percent that extensively use it) (figure 12).⁵¹

Regulatory stress-testing requirements, such as under the Federal Reserve's capital plan rule, contain both quantitative and qualitative requirements. The quantitative methodologies require that an institution has sufficient capital to pass capital ratio thresholds under the current and the post-stress environment. Institutions are also required to have qualitative procedures in place that indicate an effective risk management program such as strong

Figure 12. To what extent are the results of capital stress tests used by your organization for each of the following purposes?

Base: Respondents at institutions using capital stress testing



Note: Percentages may not total due to rounding.

Source: Deloitte analysis.

Deloitte University Press | dupress.deloitte.com

internal controls, effective management challenge, documentation of policies and procedures, model validations, strong IT systems, and quality data, among others. When in the past regulators failed capital plans of banks, it tended to be for weak quantitative post-stress capital levels, whereas more recently they have been focusing on the need for stronger qualitative controls and capabilities.

Many qualitative issues in capital stress testing were rated as being extremely or very challenging including *capital stress testing IT platform* (66 percent) and *data quality and management for*

capital stress-testing calculations (52 percent), which were the two highest-rated issues.

Capital stress testing requires that information and data be integrated from across the organization including from business units and from functional areas such as finance. Many respondents rated as extremely or very challenging *coordinating multiple functional areas and activities required to conduct capital stress tests* (for example, risk, treasury, business units, IT, developing and implementing models, validating models) (48 percent).

There are no off-the-shelf, end-to-end capital stress-testing and planning platforms that institutions can employ to integrate the wide variety of required inputs. Instead, they need to develop custom systems and then use data warehouses to integrate data across the institution, which can lead to significant challenges in maintenance.

Other issues that were considered by many respondents to be extremely or very challenging in capital stress tests were *implementing formal validation procedures and documentation standards for the models used in capital stress testing* (47 percent), *developing capital stress-testing methodologies/models accepted by regulatory authorities, as part of supervisory stress-testing exercises* (44 percent), *active engagement by senior management and the board of directors in setting capital stress-testing objectives, defining scenarios, and challenging methodologies and assumptions* (40 percent), and *capital-stress-testing analytics* (39 percent).

Liquidity stress testing

Liquidity stress testing has recently emerged as an additional priority for the regulators, complementing their existing focus on capital stress testing. The focus on liquidity emerged in the Basel III requirements for the liquidity coverage ratio and the net stable funding ratio (NSFR). The US Federal Reserve has also recently implemented additional liquidity reporting requirements for large banks. Now more regulatory authorities are including liquidity stress testing requirements, and as a result, more institutions are conducting liquidity stress tests, especially banks. Liquidity stress testing remains a new area where regulatory expectations are expected to become clearer over time and where institutions are gaining experience.

Eighty-two percent of institutions reported that they conduct liquidity stress tests, with this being more common at banks (91 percent) than at investment

management firms (80 percent) or insurance companies (74 percent). A number of regulatory developments suggest that liquidity stress tests could increase in importance for investment managers in the future. The FSB has recommended that regulators require or provide guidance on liquidity-stress-testing for funds, and the International Organization of Securities Commissions (IOSCO) has announced that it is considering developing additional guidance on liquidity stress testing.⁵²

Almost all institutions reported using the results of liquidity stress tests in reporting to senior levels: *reporting to the board* (98 percent, including 51 percent that use it extensively) and *reporting to senior management* (95 percent, including 52 percent that use it extensively) (figure 13).

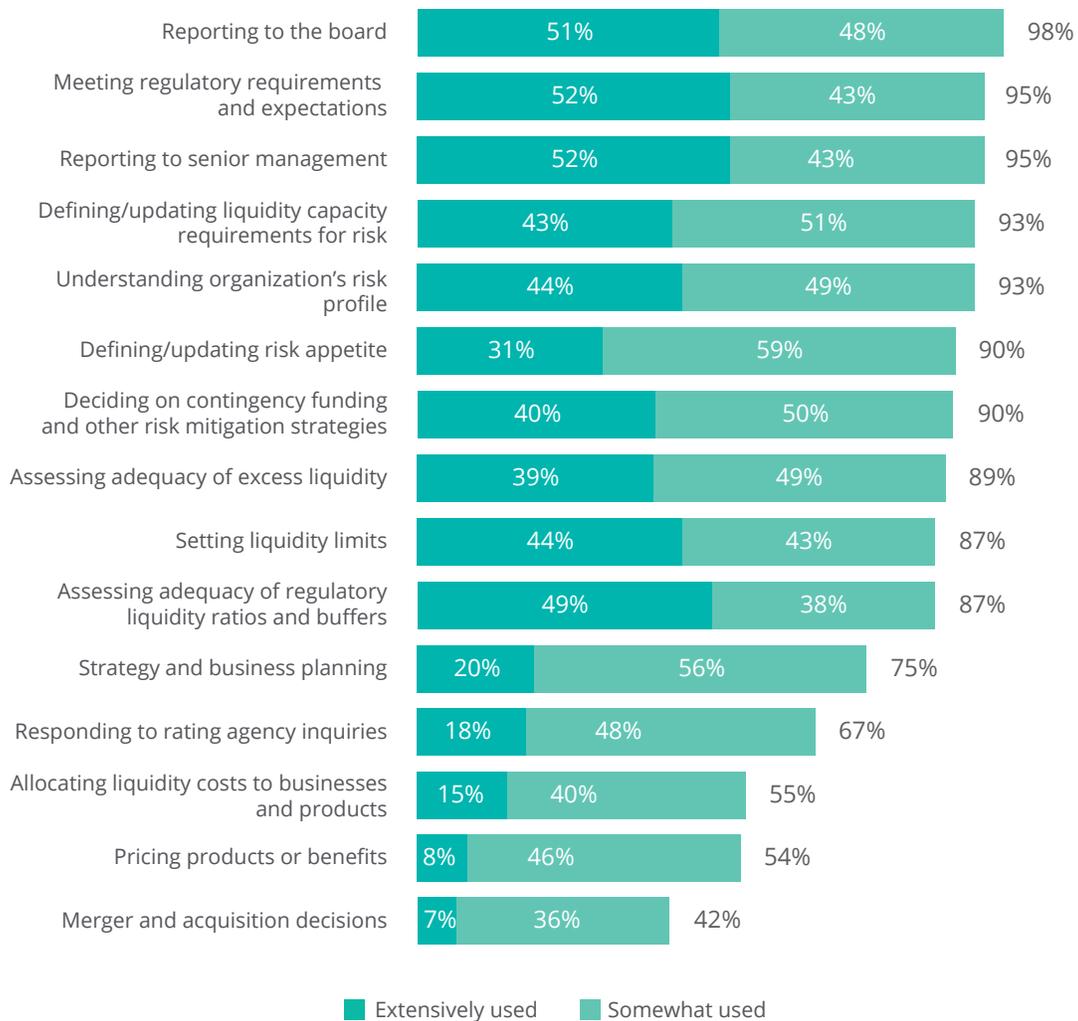
Institutions also use the results of liquidity stress tests in *meeting regulatory requirements and expectations* (95 percent, including 52 percent that use it extensively) and *assessing adequacy of regulatory liquidity ratios and buffers* (87 percent, including 49 percent that use it extensively).⁵³

Other areas where substantial percentages of institutions use liquidity stress testing results are *defining/updating liquidity capacity requirements for risk* (93 percent, including 43 percent that use it extensively), *understanding the organization's risk profile* (93 percent, including 44 percent that use it extensively), and *setting liquidity limits* (87 percent, including 44 percent that use it extensively).

As with capital stress testing, the two issues most often rated as extremely or very challenging in using liquidity stress testing concern IT systems and data: *liquidity-stress-testing IT platform* (45 percent) and *data quality and management for stress-testing calculations* (33 percent). The issues cited next most often were *coordinating multiple functional areas and activities* (31 percent) and *implementing formal validation procedures and documentation standards for models used in stress testing* (30 percent).

Figure 13. To what extent are the results of liquidity stress tests used by your organization for each of the following purposes?

Base: Respondents at institutions using liquidity stress testing



Note: Percentages may not total due to rounding.

Source: Deloitte analysis.

Deloitte University Press | dupress.deloitte.com

Sector spotlight: Banking

THE Basel Committee is in the process of proposing revisions to its capital rules for market, credit, and operational risk, with a general goal of providing an enhanced set of standardized approaches to lessen the reliance on internal models in the advanced approaches. Collectively, this group of revised risk-weighted asset (RWA) capital rules has been called Basel IV. These efforts are at varying stages of progress, with the market risk rules now finalized.⁵⁴

For credit risk, revisions to the standardized approach have been proposed, along with constraints on the use of internal models.⁵⁵ The Basel Committee has proposed removing the option to use internal-ratings-based approaches for certain exposures where it has concluded that the model parameters cannot be estimated sufficiently reliably. For portfolios where internal-ratings-based approaches remain available, it has proposed adopting exposure-level, model-parameter floors to ensure a minimum level of conservatism and providing greater specification of parameter estimation practices to reduce variability in risk-weighted assets.⁵⁶ These potential regulatory changes could spur some institutions to undertake a substantial revision of their methods and systems.

For operational risk, a new Standardised Measurement Approach (SMA) has been proposed, which would replace the current existing approaches.⁵⁷ The SMA would provide a single non-model-based method for estimating operational risk capital that incorporates in a standardized fashion a bank's financial statement information and internal loss experience.

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) sets out how banks will have to assess

their capital requirements for their trading portfolios. The initiative is intended to ensure that capital requirement approaches are better aligned with the trading book's underlying risks and to reduce the variability in modeling outcomes from firm to firm.

Europe is furthest ahead in implementing the FRTB, with many institutions having already begun implementation, even though legislation to implement the FRTB has only recently been proposed. The United States has not yet proposed a corresponding rule and implementation at US banks is still in the early stages. It is currently expected that the FRTB effective date will be in 2019, which means that institutions should begin to implement the required procedures in 2017 and conduct a parallel run in 2018. Implementing the new FRTB rules will require institutions to make progress in developing data, analytics, and processes in a number of different areas and these present significant challenges.

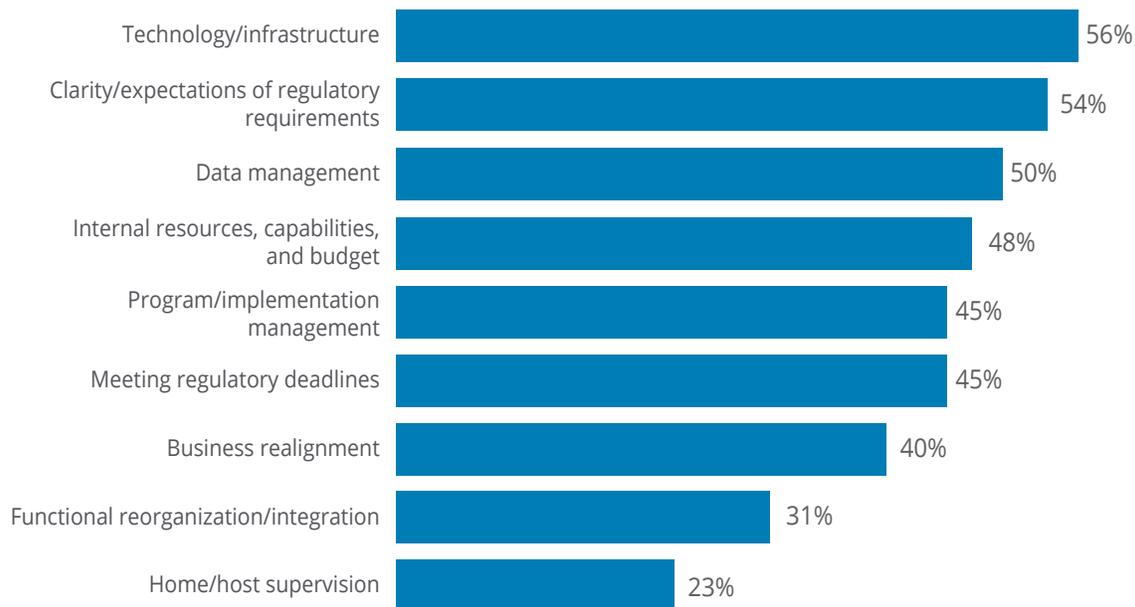
“There will be quite a hit from a capital perspective from the Basel Committee proposals but it will impact everyone, so it should level the playing field.”

— *Chief risk officer,
large diversified financial services company*

The issues most often considered by respondents to be extremely or very challenging in implementing FRTB were *technology/infrastructure* (56 percent), *clarity/expectations of regulatory requirements* (54 percent), and *data management* (50 percent) (figure 14).

Figure 14. For your organization, how challenging 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)?

Percentage of institutions responding extremely challenging or very challenging



Source: Deloitte analysis.

Deloitte University Press | dupress.deloitte.com

With the United States/Canada not as far along as in Europe, US/Canadian institutions are much more likely to rate many issues as extremely or very challenging, including *technology/infrastructure* (100 percent in the United States/Canada compared to 55 percent in Europe), *data management* (75 percent in the United States/Canada compared to 45 percent in Europe), and *internal resources, capabilities, and budget* (100 percent in the United States/Canada compared to 36 percent in Europe).

The Basel Committee’s new Total Loss Absorbing Capacity (TLAC) requirements for global systemically important banks (G-SIBs) are designed to increase the capital and leverage ratios of these banks so they are better able to withstand adverse financial conditions. TLAC is scheduled to take effect in 2019. As a result, the implications are still being understood. Issues often cited by respondents as extremely or very challenging in complying with TLAC include *clarity/expectations of regulatory requirements* (42 percent), *data management* (41 percent), and *strict deadlines* (38 percent).

Sector spotlight: Insurance

Regulatory and economic capital

Insurance companies across the globe have been facing increased regulatory capital requirements for some time. The most influential capital adequacy regime has been Solvency II (SII), which was developed by EU regulators for insurance companies and is now being considered by insurance companies around the world. Eighty percent of the companies participating in the survey are either subject to SII requirements (38 percent), subject to similar regulatory capital requirements (40 percent), or not subject to SII or similar requirements but have voluntarily adopted SII (3 percent). Other regulatory regimes are looking to SII as a guidepost as they evolve their capital adequacy standards as reflected in the fact that 40 percent of insurance companies are subject to similar regulatory requirements. Even when not a regulatory requirement, SII is becoming more accepted as a standard when companies develop the assumptions and methods in their internal economic capital models.

Insurance companies employing SII or similar requirements were overwhelmingly outside the United States/Canada, where 80 percent of companies said they were not subject to SII or similar requirements and have not adopted them. As would be expected, insurers are more likely to be complying with SII or similar requirements (82 percent) than are investment management firms (74 percent) or banks (56 percent).

When asked which areas respondents expected their company to focus on related to SII or similar regulatory capital requirements over the next two years, respondents most often named *scenario analysis* (66 percent).⁵⁸ One of the most significant functions of an economic capital scenario analysis is to model

stressful scenarios to determine if an organization is sufficiently well capitalized to withstand these adverse conditions and remain solvent.

SII calculations require a wide array of data from multiple sources, and *data infrastructure and data handling requirements* (63 percent, down from 87 percent in 2014) was cited as a focus by many respondents. The fact that fewer respondents cited this issue than did so in the 2014 survey may indicate that more companies are improving their capabilities in this area.

A third issue that was often cited as a focus for SII was *enhancements to risk tolerance and risk appetite* (59 percent). Many companies are enhancing their risk appetite statements and using them to inform strategic business decisions as risk exposures evolve over time.

The International Association of Insurance Supervisors (IAIS) is developing global regulatory capital standards. Respondents felt that a number of the potential requirements could have at least a somewhat significant impact on their company, although relatively few expected the impact would be extremely or very significant: *recovery and resolution planning* (59 percent, with 31 percent extremely or very significant), *Insurance Capital Standard* (54 percent, with 26 percent extremely or very significant), *broader ComFrame requirements of risk management and governance* (59 percent, with 31 percent extremely or very significant), and *capital requirement and high loss absorbency standards* (59 percent, with 31 percent extremely or very significant). In Japan, the JFSA has urged the IAIS to be careful of creating a framework that has unintended impacts, such as hindering internal risk management efforts, causing excessive risk-aversion, or leading to similar investment strategies.⁵⁹

Assessing insurance risk

The most common methods used by insurance companies as a primary methodology to assess insurance risk are *actuarial reserving* (72 percent) and *regulatory capital* (59 percent) (figure 15).⁶⁰ Actuarial reserving has traditionally used best estimate assumptions to determine the expected present value of future cash flows related to insurance risk, while *regulatory capital* represents the amount of additional capital a company should set aside to cover an extreme insurance risk event. These are prescribed metrics based on traditional actuarial, financial, and statistical principles, and are widely accepted as methods to determine insurance risk.

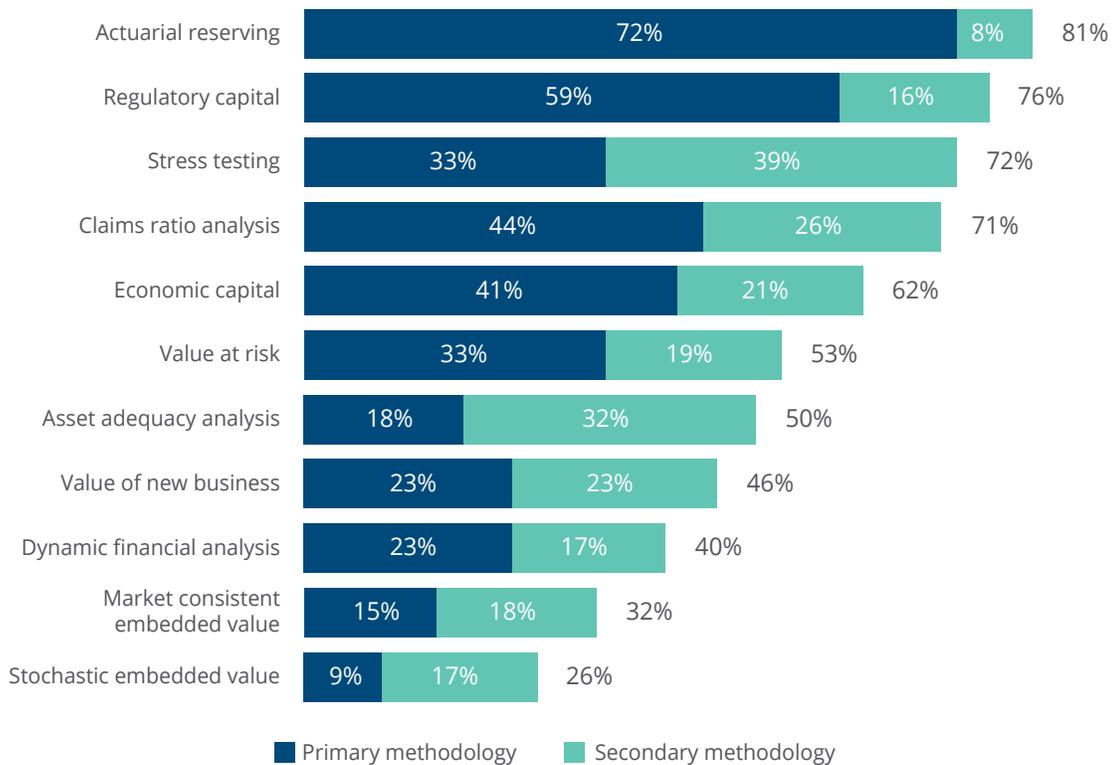
Stress testing is used by 72 percent of insurance companies to assess insurance risk, with 33 percent

using it as a primary methodology and 39 percent as a secondary methodology. This is consistent with the regulatory focus on stress testing. (See the discussion above in this section.)

Companies of different sizes vary significantly in the methods they use to assess insurance risk. *Economic capital* is used as either a primary or secondary methodology to assess insurance risk more often by large (82 percent) than by mid-size (50 percent) or small insurers (54 percent). Larger insurers tend to have the more sophisticated capabilities required to create robust internal capital modes, which are often either loosely or tightly based on SII. The somewhat rote, but still complicated calculations in the value-at-risk analysis are used more often by mid-size insurers (67 percent) as a primary or secondary methodology than by large (45 percent) or small insurers (45 percent). The simplistic *claims*

Figure 15. To what extent does your organization use each of the following methods to assess insurance risk?

Base: Companies that provide insurance/reinsurance services



Note: Percentages may not total due to rounding.

Source: Deloitte analysis.

Deloitte University Press | dupress.deloitte.com

“The biggest challenge is actually thinking through, developing and implementing plans of business model changes in the face of these short- and medium-term drivers. It’s increasingly difficult to adapt a successful and profitable business based on historical capital and margins expectations.”

— **Chief risk officer,
major global insurance and asset management company**

ratio analysis is used more often as either a primary or secondary methodology by mid-size (75 percent) and small insurers (83 percent) than by larger insurance companies (50 percent).

What are the most common risk factors that insurance companies are stressing? Among the insurers that conduct stress testing, stress tests are conducted most often on *interest rate* (83 percent) and *property and casualty cost* (76 percent). The other items cited were *mortality* (59 percent), *lapse* (55 percent), *expense* (55 percent), and *morbidity* (52

percent). However, few small companies perform stress testing on mortality (10 percent), lapse (20 percent), expense (30 percent), and morbidity (10 percent), which is likely due to a lack of resources.

Seventeen percent of respondents said they performed stress testing on other factors, such as strategic risk. Across the insurance industry, there is a heightened awareness of the importance of managing strategic and operational risk, and companies are grappling with how to credibly measure and manage these risks.

Sector spotlight: Investment management

The investment management sector comprises firms of many sizes, organizational structures, product portfolios, and target customers. These firms share the fundamental processes of engaging with customers, determining investment goals and risk tolerances, and managing customer financial assets in an effort to meet or exceed the customer's investment goals. Investment management firms often adopt a range of approaches to implementing these common investment management processes.

As fiduciaries, investment managers are fundamentally the guardians of the financial assets of their customers. They have a responsibility to place client interests ahead of their own. Clients range from sophisticated financial firms to individuals with limited financial knowledge, and this diversity leads to a complicated set of risks to manage, with firms adopting risk management priorities that match their individual strategies.

Respondents were asked how challenging were a series of issues today for their firm in managing risk in its investment management business. The items most often rated as extremely or very challenging concerned IT systems and data: *IT applications and systems* (50 percent, down from 55 percent in 2014) and *data management and availability* (36 percent, down from 42 percent in 2014)⁶¹ (figure 16).

As the survey results indicate, the challenges and leading practices related to managing risk for investment managers begins with data and technology. Having an established “golden source” of data is difficult to maintain due to data replication and redundancy across multiple applications within the overall operating systems architecture. Many organizations have difficulty effectively managing the data divergences across the systems architecture. The result is often diminished confidence in

the automated checks critical to efficient management of risk for an investment manager.

The solution to these problems begins with treating data as a valuable organizational asset. The first step is to create a comprehensive data dictionary, including sources and uses of the data, which many investment management firms lack. Another leading practice is to create a formal data governance committee with the responsibility to catalog data requirements and to develop a data dictionary. Once these elements are implemented, firms should create a data model to track the usage and flow of data into and through the organization. With these steps in place, firms can begin to tailor their risk management technology infrastructure while also streamlining the technology architecture, rather than adding to its complexity to address each new risk management function. Firms that treat data as a fundamental risk management asset and enhance their overall data governance framework can realize significant opportunities to enhance management of key risks.

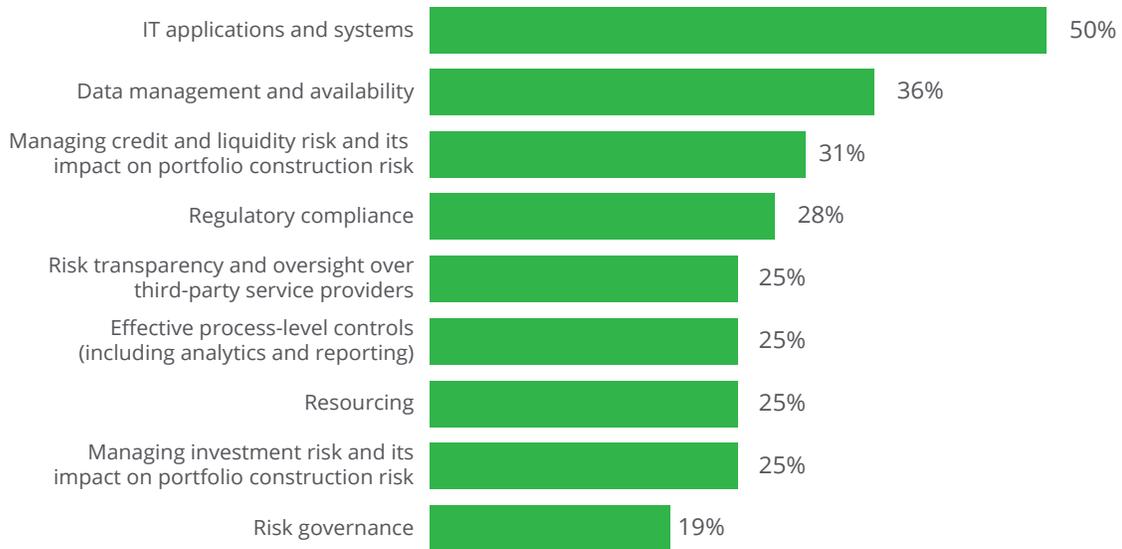
The areas where respondents felt their institutions had a more mature program to manage risk in their investment management business and were less challenging were *resourcing* (25 percent, down from 33 percent in 2014), *managing investment risk and its impact on portfolio construction risk* (25 percent),⁶² and *risk governance* (19 percent, down from 24 percent in 2014).

The relatively small percentage of respondents who considered *risk governance* to be extremely or very challenging for their investment management business is a positive development. Given its cornerstone role in risk management, excellence in risk governance needs to be a strategic priority for firms,

Figure 16. In managing risks in your organization's investment management business, how challenging is each of the following?

Base: Firms that provide investment management services

Percentage of respondents that responded extremely challenging or very challenging



Source: Deloitte analysis.

Deloitte University Press | dupress.deloitte.com

and governance practices are increasingly being reviewed by regulators.

The risk governance approach implemented at an investment management firm represents that firm's strategic approach to organizing, reporting, controlling, and mitigating risk. Everything a firm does across all three lines of defense to manage and report risk, either wittingly or unwittingly, falls under risk governance.

Risk governance leads to:

- A risk management framework
- Consistent capture, measurement, and reporting of risk data
- Improved understanding of risk throughout the organization

Within the risk management framework, strong governance practices enable identification of high risks, which enables prioritization of risk mitigation efforts on the areas of greatest exposure. Leading practices also assign or identify clear owners of each risk in the first and second lines of defense. Finally,

the risk reporting component of governance can enable an enterprise-wide view of risk that provides a clear basis for assessing the strength of the risk controls as well as the overall state of compliance.

Risks posing the greatest challenges

Looking forward over the next two years, respondents were asked to identify the three risk types that will present the greatest challenges for the investment management business in their firm. *Regulatory/compliance* (81 percent), which is a constantly moving target that requires a robust compliance risk management program, was cited most often as among the top three risk types that will present the greatest challenges. Regulatory compliance can be especially challenging since investment management firms are often subject to the jurisdiction of multiple regulatory authorities.

In the United States, significant regulatory changes cover reporting modernization, liquidity risk management, and use of derivatives. In addition,

the use of derivatives is facing increased regulation across the globe, including derivatives trade reporting requirements in Canada, the Hong Kong Monetary Authority's market reform, and the European Markets and Infrastructure Reform (EMIR). While there is considerable consistency in the overall direction of regulation, firms with a large geographic footprint have an even more difficult task in keeping up with varying regulatory requirements across countries.

The risk that was rated second most often by respondents as among their top three risks over the next two years was *investment* (72 percent), which includes portfolio construction risk, credit risk, market risk, and liquidity risk. Over the past couple of years, the investment management industry has been challenged by tightening operating margins driven by changes to investor behavior and expectations, new regulations, and advanced technologies. These changes have caused a strain on an already aging investment risk management infrastructure (that is, people, process, technology, data, governance, and culture). As a result, investment managers are facing more pressure for greater infrastructure efficiency and effectiveness in trying to meet day-to-day business needs.

In many firms, the investment compliance management function (ICM) plays a critical role in managing investment, financial, regulatory, operational, and reputational risk. Leading ICM programs facilitate operational readiness and organizational responses to rapidly changing market conditions, new regulatory requirements, and shifting investor behavior. Excellence in these risk management areas reflects the industry's commitment to invest client assets in accordance with their investment objectives and guidelines, adhere to regulatory requirements, and pursue operational excellence for shareholders and other stakeholders. Yet, in a difficult cost environment, investment in ICM infrastructure may not be prioritized when compared to other infrastructure investments.

Pressures in the industry are likely to continue to evolve, particularly competition for new clients in light of evolving regulations and changing investor behavior. Focusing on the strategic importance of ICM by enhancing current capabilities can provide

organizations with direct and indirect benefits to address those pressures.

Some important considerations for investment management executives to enhance the efficiency, effectiveness, and extensibility of their ICM processes include:

- Assessing the current-state operating model and organizational design of the ICM function in recognition of client agreements, regulatory requirements, and organizational objectives to identify enhancement opportunities
- Categorizing and calculating the costs of ICM and its impact on product and client profitability
- Understanding the impact that the current organizational design and state of infrastructure has on resource capacity
- Identifying ICM process inefficiencies that drive instances of user rejection and control deficiencies
- Addressing data quality and system capabilities to effectuate new regulatory requirements and increasingly complex client guidelines
- Exploring outsourcing opportunities to manage costs, gain access to subject matter knowledge, and enhance operational efficiency

Making ICM a strategic priority not only assists investment managers in living up to its customer and regulatory commitments, but can also position investment managers to be more competitive and profitable.

Despite the recent focus on cybersecurity and liquidity risk, relatively few respondents rated them as among the risks that will pose the greatest challenges to their firm's investment management business. Only 28 percent of respondents cited *cybersecurity* and 22 percent named *liquidity* as one of the three risks posing the greatest challenges over the next two years.

Oversight of investment risk

Respondents reported that their firm assigned a wide range of responsibilities to the individual or

individuals responsible for oversight of investment risk with the most common responsibilities being *monitor compliance with investment guidelines related to investment risk* (86 percent); *develop and implement the investment risk management framework, methodologies, standards, policies, and limits* (78 percent); *manage stress-testing process, including governance, methodology, and reporting* (72 percent); and *meet regularly with governance committees responsible for overseeing investment risk management* (72 percent).

Firms were least likely to give the individual responsible for investment risk management other responsibilities such as *conduct back-testing of risk and related models* (58 percent), *use of independent risk technologies to generate risk analytics independent of the portfolio management function* (56 percent), and *provide input to the day-to-day investment decisions that impact the risk profile* (44 percent).

Managing liquidity risk in investment management

Managing liquidity risk has become a greater focus for regulators in all financial sectors, including investment management. For example, in the United States, SEC rule changes will require open-ended mutual funds to establish a formal liquidity risk management program, designate a liquidity risk management program administrator, categorize their assets based on how many days it would take to convert them into cash without impacting the net asset value (NAV), and require additional regulatory reporting and shareholder disclosures.⁶³ In December 2015, the IOSCO published a report on the tools available to investment management firms globally to manage liquidity risk and has indicated that it is considering developing additional guidance beyond its 2013 liquidity risk management principles.⁶⁴

However, relatively few respondents believed that liquidity risk management related to investment risk presented significant challenges for their institution. The item that was rated most often as extremely or very challenging with respect to liquidity risk

management related to investment risk was *classification of fund asset liquidity, including determining the assumptions used when bucketing holdings into business/calendar day categories and multiple liquidity levels of the same position* (31 percent). Several other items were considered to be extremely or very challenging by one-quarter fewer of respondents: *deploying system/technology compatibilities necessary to facilitate liquidity calculations and ongoing monitoring* (25 percent), *memorializing liquidity risk management practices used to develop, monitor, and periodically assess portfolio liquidity* (22 percent), and *complying with requirements for regulatory reporting on liquidity* (22 percent).

Operational risk management for investment management

When asked to select the three risks that will pose the greatest challenges for their firm over the next two years, 56 percent of respondents named operational risk, making it the risk cited third most often. When asked about specific components of operational risk management, 50 percent of respondents at institutions providing investment management services said that *responding to rising threat of cybersecurity risk and its impact on the confidentiality, availability, and integrity of data and information system* was extremely or very challenging, making it the highest rated issue (See the section “Cybersecurity risk.”)

While operational risk exists in all businesses, the tough call for investment management firms is right-sizing operational risk management. When operational risks are identified prior to causing problems, they can be managed effectively. The problem for management is that identifying operational risks proactively is difficult, and when risks are mitigated before they are visible, the positive impact is hard to quantify. Accordingly, 33 percent of respondents said that *securing the appropriate resources to address risks with the highest priority* is extremely or very challenging for their firm in operational risk management, while 86 percent considered it to be at least somewhat challenging. If sufficient budget authority is difficult to achieve, this suggests that

many investment management firms may have an issue with their commitment to risk management. One obstacle may be that it is often difficult to make a business case that quantifies the benefits of increased investment in risk management.

Obtaining quality data is another difficult task, and 33 percent of respondents said *maintaining reliable data to quantify operational risk and drive risk-based decisions* was extremely or very challenging, with 89 percent considering it at least somewhat challenging.

One approach to managing operational risk is through a steady pace of operational transformation. When people, processes, and technology are refreshed, they effectively reset the clock on operational risk, and during the refresh process, implementation or project risk takes its place. Alternatively, firms that maintain long-tenured systems should execute a disciplined review of their people, processes, and technologies to achieve similar operational risk mitigation.

The difficulty in mitigating operational risk through review is especially true for firms that maintain more complicated best-of-breed enterprise systems architectures. Best-of-breed architectures present additional operational risk due to the tendency toward uncoordinated update schedules of the many applications, and the unique fingerprint of interfaces that can occur in these approaches.

Proactively managing operational risk has its benefits beyond the obvious. Following the old cliché, “If it ain’t broke, don’t fix it,” can lead firms to miss the benefits of proactive operational risk management. Firms should not wait to experience a breakdown in operations resulting in customer, operational, or financial impact before starting to invest in managing operational risk.

Additional benefits can also accrue to firms that effectively manage operational risk. Addressing the potential operational risk in people, processes, and technology can lead to greater efficiency if the review leads to fine-tuning. Training personnel can mitigate operational risk, while also improving morale, retention, and innovation. Process reviews that mitigate operational risk also have the potential to improve timing and throughput. When

applications and interfaces are reviewed for operational risk, the process can uncover a wide range of areas for improvement, from hardware improvements to maintenance plan adjustments.

A final operational risk issue that was rated by many respondents as extremely or very challenging for their investment management business was *understanding and managing operational risk associated with new business initiatives* (33 percent). One of the risks that is especially prominent when a firm enters a new business is client onboarding, which begins in the sales process, both from the perspective of the customer experience and an operational perspective. Customer first impressions are formed at this stage, and operational expertise is part of that first impression. Having the right experts in the onboarding process not only provides the prospect with clear and concise responses, but also sets the stage for operational excellence from day one. Alternatively, when client onboarding falters, it exposes the investment management firm to possible risks including incorrect portfolio management guidelines, incorrect documentation, and inefficient operations.

Leading practices to manage this operational risk include:

- Formal policies and procedures for documentation, review, and approval
- Investment compliance procedure development and impact assessment with operational sign-off
- Portfolio management guideline testing before funds acceptance or trading
- Workflow management tools to control and track the onboarding process

With leading practices in place at this early stage in their operational value chain, investment managers can avoid compounding errors, which can happen when initial stages of a process go poorly, and can demonstrate operational excellence to potential customers at the beginning stages of the customer relationship.

With the increased attention by regulatory authorities on culture and conduct, investment management firms are also working to reduce potential

conflicts of interest. Conflicts of interest manifest differently across the spectrum of investment firms. For investment managers with products for retail segments, sales practices, fees, and commissions to intermediaries are a focus of regulatory attention. For investment managers serving sophisticated investors, such as private equity (PE) firms, conflicts of interest can be much less straightforward. One of the top tensions in PE is the assignment of expenses to the fund (impacting investment performance) or to the general partner (impacting the PE firm's profitability).

In retail investment management, regulators are stepping in to protect the consumer. Less so in the institutional space, such as PE, where limited partners are exercising their buying power individually or through organizations such as the Institutional Limited Partners Association (ILPA). In both cases, conflicts of interest represent risk to investment managers, even though the conflicts are of a very different nature.

Extended enterprise risk

More than three-quarters of respondents at investment management firms considered *risk transparency and oversight over third-party service providers* as challenging, including 25 percent who rated it as extremely or very challenging, compared to 41 percent who rated it highly as a challenge in 2014. Thirty-one percent of investment management respondents considered third-party risk to be one of the top three challenges over the next two years for their institution's investment management business.

Investment managers employ a spectrum of operational models, ranging from largely insourced to almost fully outsourced. Even firms that have primarily insourced operations rely on third-party vendors for a variety of services. These vendors often subcontract to additional vendors, and so on down the line. If a risk event at any one of these distant

parties causes a failure, the investment manager still holds responsibility. Boards, investors, and regulators increasingly focus on extended enterprise risks facing investment managers including:

- Business disruption
- Theft or inadvertent dissemination of personally identifiable information
- Dissemination of intellectual property
- Regulatory breach (investment compliance, anti-money laundering, or disclosures)
- Counterparty credit risk
- Service failure

One element of an effective risk mitigation strategy is to have backup providers for important services. In the extended enterprise risk model, it is critical to ensure these alternative suppliers have different risk profiles. Having a backup in the same geographic location or one that uses the same critical service providers is much less effective than having diversity in supplier characteristics.

Managing third-party risk also requires an ongoing monitoring program to review the risks from the institution's third-party relationships. For some types of third-party relationships in the investment management business, respondents reported that they monitor these vendors/service providers either continuously or three or more times a year. The types of third-party vendors that investment management respondents said were most likely to receive monitoring either continuously or three or more times a year, were *pricing vendors* (56 percent) and *custodians* (54 percent). The types of vendors that were least likely to receive this frequency of monitoring were *reference data providers* (27 percent) and *contingent workforce* (35 percent). These third parties often received monitoring one to two times a year—35 percent for *contingent workforce* and 27 percent for *reference data providers*.

Management of key risks

When asked to assess how effective their institution is overall in managing risk, 69 percent of respondents felt it was extremely or very effective. Respondents in the United States/Canada were more likely to rate their risk management program as extremely or very effective (89 percent) compared to those in Europe (65 percent), Asia Pacific (65 percent), and Latin America (63 percent).

Respondents most often rated their institution as extremely or very effective in managing traditional risks including *liquidity* (84 percent), *underwriting/reserving* (83 percent), *credit* (83 percent), *asset and liability* (82 percent), *investment* (80 percent), and *market* (79 percent). These risks have been the focus of regulatory attention for many years, and institutions have experience in complying with regulatory requirements. The risk management programs for these risks are more mature with better methodologies and analytics, and with relevant data available.

Although financial institutions have managed operational risk for some time, fewer respondents (51 percent) felt that their institution was extremely or very effective at managing *operational risk*. Beyond the challenges associated with models, risk assessments, and controls for operational risk, many institutions are focusing on assessing the value that is being produced by their operational risk management programs.

Newer risk types are even more difficult to manage, with regulatory expectations less well-defined, and institutions have less advanced methodologies, analytics, and systems, as well as less relevant data available. In addition, many of these risk types are inherently difficult to manage. With cybersecurity risk, for example, institutions often don't know when their systems have been compromised and only learn much later, if at all.

Respondents considered their institution to be less effective at managing new risk types such as

cybersecurity (42 percent), *model* (40 percent), *third party* (37 percent), *data integrity* (32 percent), and *geopolitical* (28 percent).

It is somewhat surprising that only 40 percent of respondents considered their institution to be extremely or very effective in managing *model risk* since this risk type has received significant attention in the last several years. In the United States, regulatory expectations are well-defined, for example, in the 2011 Federal Reserve guidance SR 11-7 and the prior OCC 2000-16 guidance. In other jurisdictions, regulatory expectations are less well-defined but the expectations of regulators have increased in this area. Managing model risk requires hiring professionals that possess both high-level mathematical skills as well as experience in how financial models work in banks and other financial institutions. This has proven difficult since the competition has been intense to hire professionals with these skill sets.

Respondents at banks were more likely to consider their institution to be extremely or very effective in managing *cybersecurity risk* (49 percent), compared to those in investment management firms (41 percent) and insurance companies (38 percent). Cybersecurity has received increased attention by the banking regulators.

Respondents were asked to look ahead to identify the three risks that they believed would increase the most in importance for their business over the next two years. The risk most often ranked among the top three was *cybersecurity* (41 percent). The percentage of respondents who ranked *cybersecurity* among the top three risks that would increase in importance was similar to 2014, but 18 percent ranked it as the No. 1 risk that would increase in importance, compared to 12 percent in 2014.

Regulatory/compliance risk was the risk second most often ranked among the top three (36 percent), with 9 percent ranking it as No. 1. These figures are down from 2014, when 51 percent named it among

the top three risks to increase in importance and 20 percent ranked it as No. 1. This may reflect the fact that there had been a wave of fundamental regulatory reform in the years since the global financial crisis, but that the pace appears to be slowing, or is potentially at an inflection point.

As in 2014, the third and fourth highest-rated risks were *credit* (32 percent in the top three, 16 percent as the No. 1 risk) and *strategic* (32 percent in the top three, 17 percent as the No. 1 risk). Strategic risk may be increasing due to more uncertainty over the outlook for regulation, the political uncertainty in many developed countries, and competition from new fintech firms. Institutions are especially considering the impact of regulations on capital requirements, which can impact the businesses an institution chooses to compete in. Going forward, institutions may need to review their identification of strategic risks more frequently and devote more management attention to the potential for disruption.

Respondents in the United States/Canada were least likely to rank *credit risk* among the top three that would grow in importance (11 percent), while those in Europe (23 percent), Asia Pacific (48 percent), and Latin America (50 percent) were much more likely to expect more focus on credit risk in the future. These responses may also reflect the relative strength of the United States and Canadian economies compared to other regions.

Geopolitical uncertainty

The survey was conducted at a time when political developments in a number of countries had increased uncertainty over the future of globalization and trade, including the Brexit vote in the United Kingdom and the US presidential election. These developments make it even more difficult than usual to measure and anticipate geopolitical risk. This may explain why the percentage of respondents who considered their institution to be extremely or very effective in managing geopolitical risk dropped from 47 percent in 2014 to only 28 percent in 2016.

“Rather than trying to predict geopolitical change, we’re just trying to make sure we’re able to adapt to whatever the ultimate outcome is.”

— **Senior risk executive,
large diversified financial services company**

Respondents were asked about the likely impact on the risks facing their institution of the proposals in some countries to renegotiate trade agreements. Respondents were divided, with 48 percent expecting that the risks facing their institution would increase (although only 6 percent expected risks to increase significantly), while 49 percent thought these proposals would have no impact. Executives in Europe were most likely to expect increased risk: 68 percent expected that risks would increase, including 16 percent who thought they would increase significantly. In the United States/Canada, however, 89 percent of respondents thought these proposals would have no impact on risk, and only 11 percent expected increased risk.

Credit risk

With relatively weak economic conditions in many markets around the world, managing credit risk is a significant challenge for financial institutions. When asked how challenging it would be to manage credit risk over the next two years, the areas most often considered to be extremely or very challenging were *collateral valuation* (38 percent), *commercial real estate* (33 percent), *unsecured credit* (33 percent), and *mortgages/home equity lines of credit* (30 percent). The issues presented by collateral valuation and commercial real estate are connected, with regulators discussing potential challenges in commercial real estate, depending on the property type.

Commercial real estate was more often considered to be extremely or very challenging for institutions to manage credit risk in the United States/Canada

(67 percent) than those in Europe (38 percent), Asia Pacific (24 percent), or Latin America (29 percent). On the other hand, respondents were more likely to see *mortgages/home equity lines of credit* to be extremely or very challenging in Europe (53 percent) than in the United States/Canada (33 percent), Asia Pacific (12 percent), or Latin America (29 percent). Also, *unsecured credit* was more often rated as extremely or very challenging in Europe (44 percent) than in the United States/Canada (17 percent), Asia Pacific (24 percent), or Latin America (29 percent). With regard to asset size, respondents at large institutions (53 percent) were more likely to consider *commercial real estate* as extremely or very challenging than were those at mid-size (15 percent) or at smaller institutions (38 percent).

While regulators have continued to express concerns about oil and gas lending due to the decline in oil prices in recent years, only 26 percent of respondents felt that *credit exposure to resource-dependent countries and organizations* will be somewhat or very challenging to manage over the next two years.

Respondents reported that their institutions still have substantial work to do to comply with the new impairment measurement approaches being introduced under the US Financial Accounting Standards Board (FASB)'s Current Expected Credit Loss (CECL) model and International Financial Reporting Standards (IFRS) 9.⁶⁵ 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 (ALLL). 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/DFAST) provide some elements that can be potentially leveraged. Only 26 percent of institutions said their existing credit risk management approaches are fully or mostly aligned with the new CECL model, while 41 percent said they were only somewhat aligned and 33 percent said they were mostly not or not at all aligned. The responses concerning IFRS 9 were similar, with 38 percent saying their existing credit risk management approaches were fully or mostly aligned with the new IFRS 9 approach, while 40 percent said they were only somewhat aligned and 23 percent said they were mostly not or not at all aligned.

For both accounting standards, there was a dramatic difference across regions, with institutions in the United States/Canada and Europe being much more likely to report that their existing credit risk management approaches will be aligned with the new impairment models. For example, 50 percent of institutions in the United States/Canada and 69 percent in Europe said their credit risk management approaches will be fully or mostly aligned with IFRS 9 compared to 12 percent in Asia Pacific and 14 percent in Latin America. Additionally, 50 percent of institutions in the United States/Canada expect to be fully or mostly aligned for CECL compared to only 33 percent among European institutions.

FASB's CECL standard applies to all US banks, savings associations, credit unions, and financial institution holding companies. Forecasting expected losses over the remaining contractual life-of-loan and incorporating "reasonable and supportable forecasts" are not only modeling challenges. They require institutions to employ and document the rationale for more judgment and assumptions. Even as financial institutions move beyond implementation, robust governance and reporting processes are essential.

Market risk

Market risk is a traditional risk type where most institutions have more mature risk management methodologies and policies to manage risks in this area. As a result, relatively few respondents considered various aspects of market risk management to

be very challenging. The issues related to managing market risk in the trading book that respondents most often expected would be extremely or very challenging over the next two years were *complying with the Basel Committee's revised Minimum Capital Requirements for Market Risk* (31 percent), followed by *consistently aggregating the results of market risk calculations across portfolios and business areas* (24 percent) and *aligning market risk management with overall ERM program* (23 percent).

The Basel Committee's final framework for Minimum Capital Requirements for Market Risk resulting from the FRTB was released in January 2016, and European banks are further along in their preparations for compliance than are their US and Canadian counterparts. This was reflected in the fact that a larger portion of respondents in the United States/Canada (38 percent) considered *complying with the Basel Committee's revised Minimum Capital Requirements for Market Risk* to be extremely or very challenging than did respondents in Europe (22 percent).

More than half of the respondents at institutions with more than \$100 billion in assets said that compliance with the final Basel market risk framework was extremely or very challenging. This is largely due to the fact that complex trading books at larger institutions increase the complexity of compliance. *Consistently aggregating the results of market risk data calculations across portfolios and business areas* was cited as extremely or very challenging more often by respondents in Asia Pacific (29 percent) and Latin America (29 percent) than by those in the United States/Canada (13 percent) and Europe (14 percent).

Liquidity risk

Since the global financial crisis, regulators and financial institutions have focused significant attention on managing liquidity risk, and financial institutions appear to have made progress in this area. Basel III introduced the NSFR and LCR and the Basel Committee has proposed the TLAC for G-SIBs, and liquidity stress testing has become more common.

Relatively few respondents believed various aspects of liquidity risk management would be extremely or very challenging over the next two years, but in some cases, the percentage increased from 2014. This may indicate that some institutions were in the early stages of examining their liquidity risk management or that they significantly underestimated the difficulty of the effort. The areas that were most often considered to be extremely or very challenging in managing liquidity risk over the next two years were *investment in cash flow forecasting and reporting capabilities* (32 percent, up from 22 percent in 2014), *controlling the consumption of liquidity on a daily basis across the whole organization* (31 percent, up from 23 percent), and *internal allocation of the cost of liquidity buffers across the organization* (31 percent)⁶⁶ (figure 17). In addition, 26 percent of respondents said that *obtaining sufficient, timely, and accurate liquidity risk data* would be extremely or very challenging for their institution over the next two years.

Institutions appear to have put in place procedures to comply with the Basel III liquidity requirements, and these requirements were less likely to be seen as extremely or very challenging than they were in 2014: *investment in operational and other capabilities to comply with the Basel III LCR* (23 percent, down from 31 percent) and *investment in operational and other capabilities to comply with the Basel III NSFR* (23 percent, down from 40 percent).

Asset liability management

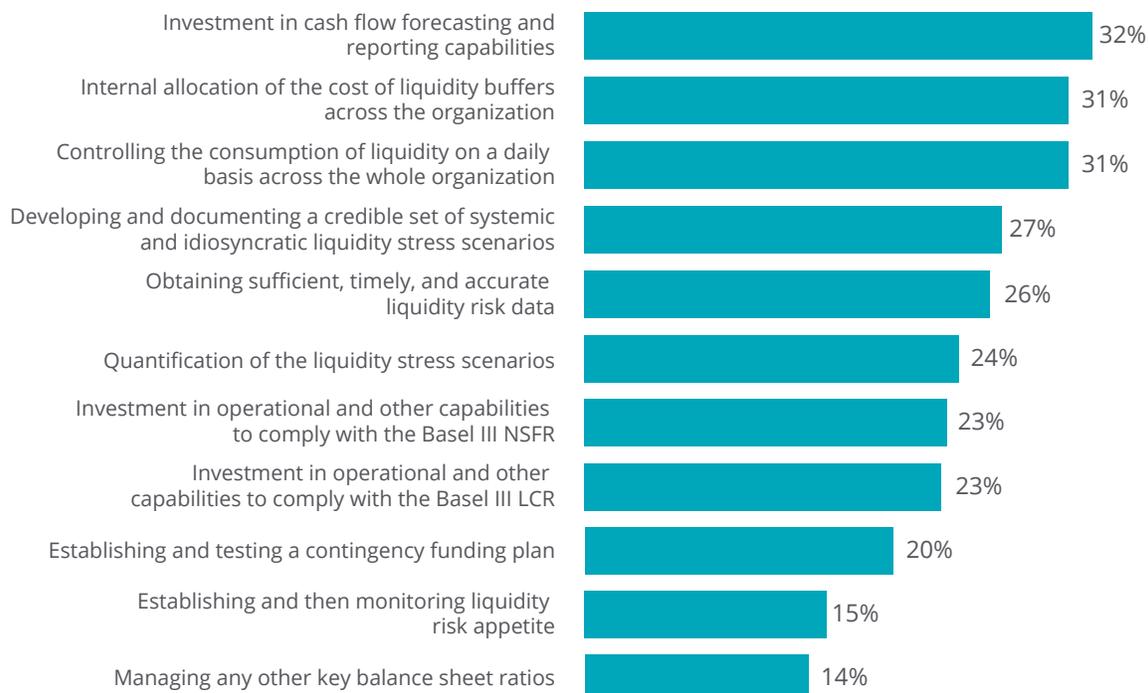
The issues cited most often as being extremely or very challenging in asset liability management were *integrating the modeling of IRRBB and credit risk within the banking book to stress scenarios* (34 percent), *ability to model on a dynamic basis the impact on net interest income of changing interest rates and changing balance sheet* (29 percent), and *obtaining sufficient, timely, and accurate asset and liability data* (28 percent).

Operational risk

The Basel Committee and other regulatory authorities have focused on operational risk for a number of

Figure 17. Over the next two years, how challenging do you expect each of the following will be for your organization when managing liquidity risk?

Percentage of respondents who responded extremely challenging or very challenging



Source: Deloitte analysis.

Deloitte University Press | dupress.deloitte.com

years. However, changes may be on the horizon in how regulators require institutions to assess operational risk. In March 2016, the Basel Committee proposed scrapping the internal model-based method for calculating operational risk saying that it “has resulted in excessive variability in risk-weighted assets and insufficient levels of capital for some banks,” and replacing it with a single standardized method.⁶⁷

The regulatory focus on operational risk has led institutions to improve their methodologies in this area. Operational risk is inherently difficult to measure and manage, and it is likely to be a greater focus in the years ahead. Respondents were most likely to report that their institution’s operational risk management methodologies were extremely or very well-developed in *risk assessments* (63 percent), which are a mature methodology that has been around for some time (figure 18).

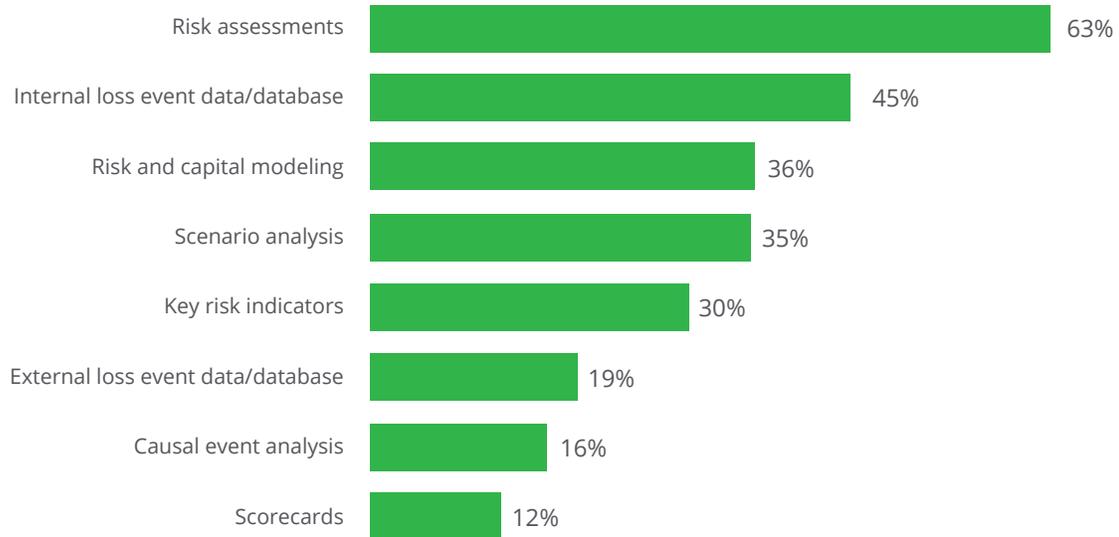
Other methodologies that were rated as extremely or very well-developed by more than one-third of institutions were *internal loss event data/database* (45 percent), *risk and capital modeling* (36 percent), and *scenario analysis* (35 percent).

Key risk indicators (KRIs) are less well-developed than other methods, with 30 percent of respondents saying they are extremely or very well-developed, but more institutions are now putting them in place or enhancing them. These represent a recurring challenge due to the difficulty in finding meaningful KRIs and the lack of consistent data being available.

Several methodologies are still a work in progress such as *external loss event data/database* (19 percent), *causal event analysis* (16 percent), and *scorecards* (12 percent). These types of operational risk analytics remain a challenge for many due to the lack of well-developed and commonly accepted methodologies.

Figure 18. How well-developed is each of the following operational risk management methodologies at your organization?

Percentage of respondents who responded extremely well-developed or very well-developed



Source: Deloitte analysis.

Deloitte University Press | dupress.deloitte.com

When asked to assess the effectiveness of their institution in managing specific types of operational risk, respondents were most likely to say their institution was extremely or very effective in managing more traditional risk types including *regulatory compliance* (64 percent), *legal* (62 percent), *tax* (58 percent) and *fraud* (46 percent). In contrast, respondents were less likely to rate their institution this highly for newer risk types such as *data integrity* (23 percent), *third party* (26 percent), and *cybersecurity* (32 percent).

Third parties present a myriad of risks including contractual nonperformance, violation of laws and unethical behavior, data breaches, loss of intellectual property, and inability to maintain operations in case of a disaster or infrastructure breakdown, among others. Over the last several years, many institutions have outsourced more of their activities to third parties in an effort to reduce costs. Managing these risks presents special challenges since vendors and service providers are not under an institution's direct control. Yet, they present significant risks that can result in financial loss and reputational damage.

Regulators have made it clear that institutions are responsible for managing the risks posed by third parties. For example, in 2013, the OCC issued guidance on managing the risk from third-party relationships, stressing that “a bank’s use of third parties does not diminish the responsibility of its board of directors and senior management to ensure that the activity is performed in a safe and sound manner and in compliance with applicable laws.”⁶⁸

It is notable that a majority of respondents did not consider their institution to be extremely or very effective at managing any of the risk types related to third parties. Respondents most often rated their institution as extremely or very effective in managing third-party risk related to *financial risk* (47 percent), *contractual risk* (46 percent), *performance and operations risk* (41 percent), and *regulatory/compliance risk* (40 percent). There were also some risk types where even fewer respondents considered their institutions to be effective including *reputational* (31 percent), *cybersecurity and data protection* (27 percent), and *resiliency and continuity* (24 percent). (See the section “Cybersecurity risk” below.)

Cybersecurity risk

Cybersecurity risk has been a growing concern for regulators and financial institutions with a number of well-publicized breaches. When asked which risk types would increase the most in importance for their institution over the next two years, respondents most often cited cybersecurity risk, with 41 percent saying it was one of the top three risks, including 18 percent saying it was the No. 1 risk.

Deloitte’s survey results indicate there is much more work to do in this area for most institutions. Only 32 percent of respondents considered their institution to be extremely or very effective in managing cybersecurity risk, and only 27 percent rated their institution this highly when it came to managing cybersecurity risk in its third-party relationships.

As might be expected, when it came to specific cybersecurity threats and risks, relatively few respondents gave their institution high marks. The highest-rated items had no more than roughly half of respondents rating their institution as extremely or very effective in managing *disruptive attacks*

(51 percent), *financial losses or fraud* (51 percent), *cybersecurity risks from customers* (47 percent), and *loss of sensitive data* (46 percent).

Other types of cybersecurity risks had even fewer respondents saying their institution was extremely or very effective, including *insider threats* (38 percent), *cybersecurity risks from third-party partners* (35 percent), *threats from nation state actors* (35 percent), *threats from skilled hackers* (33 percent), and *destructive attacks* (36 percent).

CYBERSECURITY CHALLENGES

Institutions face a number of challenges in managing the threats of cyberattacks. Leading the list of items rated as extremely or very challenging were *staying ahead of changing business needs* (66 percent) and *addressing threats from sophisticated actors* (61 percent) (figure 19).

With the rise of cybersecurity attacks in financial services and other industries, attracting talent has become more difficult, and 58 percent said *hiring or acquiring skilled cybersecurity talent* was

Figure 19. For your organization, how challenging is each of the following in managing cybersecurity risk?

Percentage of respondents who responded extremely challenging or very challenging



Source: Deloitte analysis.

Deloitte University Press | dupress.deloitte.com

“We’ve been working with external parties conducting penetration testing, simulations, vulnerability assessments, and so on. And we’ve also set up a security response center, so that we’re able to monitor on a real-time basis the threat landscape and respond very quickly to any new emerging attack or risk.”

— **Senior risk executive,
large diversified financial services company**

extremely or very challenging. Fifty-seven percent of respondents also gave this rating to *getting actionable, near-real-time threat intelligence*.

On a more positive note, institutions appear to have internal support for their efforts to address cybersecurity. Several items related to organizational support had significantly fewer respondents rating them as extremely or very challenging including *securing ongoing funding/investment* (38 percent), *sharing threat intelligence with peers or industry groups* (34 percent), and *communicating effectively with senior business management and the board* (31 percent). These items all suggest that most institutions are committing adequate resources, are communicating about the issue with senior management and the board of directors, and are ready to work with other firms and with industry groups.

Although support for cyber-related efforts clearly exists, many boards of directors face the challenge of developing sufficient expertise to oversee a technical risk type such as cybersecurity. Some boards are using approaches like engaging outside experts to provide additional technical expertise.

Many respondents said that their institution still struggles with several aspects of implementing an

effective program to manage cybersecurity risk. Roughly half the respondents said the following actions were extremely or very challenging for their institution: *developing actionable metrics that describe the state of the cybersecurity program* (55 percent), *setting an effective multiyear cybersecurity risk strategy approved by the board* (53 percent), and *getting the businesses to understand their role in cybersecurity risk* (47 percent).

Regulatory risk

In the time since the global financial crisis, many of the regulatory issues that institutions face are starting to look structural rather than cyclical. While regulators are inclined to preserve the reforms of recent years, political uncertainty in major western economies (as demonstrated by the Brexit vote in the United Kingdom and the US presidential election results) has increased the unpredictability of the regulatory environment. Additional proposals from the Basel Committee—as well as some remaining rules implementing the Dodd-Frank Act in the United States and the Capital Requirements Regulation and Directive in the European Union—are still pending.

Regulatory reforms have led to fundamental impacts in such areas as expectations for stronger risk governance frameworks, higher capital and liquidity requirements, restrictions on business activities, enhanced consumer protections, and added regulatory documentation. More recently, regulators have also turned their attention to qualitative issues, such as risk culture/conduct, incentives, and the effectiveness of internal controls.

With the many regulatory requirements that have been introduced since the global financial crisis presenting new and more stringent compliance requirements, most institutions reported that regulatory reform in the major jurisdictions where they operate has resulted in important strategic impacts, especially given the current low-revenue environment. Respondents most often cited *noticing an increased cost of compliance* (79 percent, down from 87 percent in 2014) and *requirements for maintaining higher capital* (71 percent, up from 62 percent in 2014) (figure 20). The cost of compliance has been increasing across the industry, and

Figure 20. Over the next two years, how concerned are you about the potential impact of each of the following on your organization?

Percentage of respondents who responded extremely concerned or very concerned



Source: Deloitte analysis.

Deloitte University Press | dupress.deloitte.com

institutions have increased their efforts to streamline processes and increase efficiency, for example, by using robotics process automation (RPA) to automate routine tasks. The higher capital requirements that have been put in place have had important implications for the lines of business that institutions choose to enter or exit in an effort to minimize their required capital.

The new requirements have important implications across an institution’s strategy including *adjusting certain product lines and/or business activities* (49 percent, down from 60 percent in 2014) and *maintaining higher liquidity* (36 percent, the same as in 2014). Only 5 percent of institutions said that regulatory reform initiatives have had no significant impact on their institution.

Institutions reporting that they are noticing an *increased cost of compliance* were much more likely to be in the United States/Canada (100 percent) and Europe (92 percent) than in Asia Pacific (65 percent) or Latin America (50 percent).

Looking ahead over the next two years, many respondents said that they were extremely or very concerned over the potential impact on their organization from a number of supervisory and regulatory

processes. Leading the list of concerns were *tighter standards or regulations that will raise the cost of doing existing business* (59 percent) and *growing cost of required documentation and evidence of program compliance* (56 percent). The increasing demands of regulatory reporting are a topic of focus at financial institutions, which are looking to control, centralize, and enhance the quality of regulatory data.

Other regulatory items that were cited as significant concerns by many respondents were *increasing inclination of regulators to take formal and informal enforcement actions* (42 percent), *more intrusive and intense examinations* (37 percent), and *new restrictions or prohibitions on profitable activities that will require a significant change in business model or legal structure* (36 percent).

The enhanced level of regulatory scrutiny in the United States/Canada and Europe led respondents to have greater concern over the impacts on their institutions over the next two years. For example, respondents in the United States/Canada (78 percent) and Europe (84 percent) more often said they were extremely or very concerned about *tighter standards or regulations that will raise the cost*

“You look at what we spend on risk management and compliance programs, and over the last seven or eight years, that has gone up quite significantly. So, how we manage the cost of regulatory compliance is one of the biggest challenges.”

— **Senior risk executive,
large diversified financial services company**

of doing existing business than were those in Asia Pacific (26 percent) or Latin America (38 percent). Similarly, *the growing cost of required documentation and evidence of program compliance* was more often a concern among respondents in the United States/Canada (67 percent) and Europe (92 percent) than in Asia Pacific (22 percent) and Latin

America (38 percent). Respondents in the United States/Canada (78 percent) were also much likely to say they were extremely or very concerned about *more intrusive and intense examinations* than were those in Europe (44 percent), Asia Pacific (13 percent), and Latin America (25 percent).

Risk management information systems and technology

Risk data strategy and management have posed significant challenges for many institutions for a number of years, and relatively few respondents considered their institution to be effective in this area. The issues where respondents most often rated their institution as extremely or very effective were *data governance* (26 percent), *data marts/warehouses* (26 percent), and *data standards* (25 percent). Other issues were rated this highly by even fewer respondents including *data sourcing strategy* (16 percent), *data process architecture/workflow logic* (18 percent), and *data controls/checks* (18 percent).

The activity to improve risk data strategy and management has been largely driven by regulatory pressures in specific jurisdictions. The focus in this area in North America and Europe may explain why 44 percent of respondents in the United States/Canada and 33 percent in Europe considered their institution to be extremely or very effective in *data marts/warehouses*, compared to only 17 percent in Asia Pacific and none in Latin America.

Most respondents also had significant concerns when it came to their institution's risk management information technology systems. Given the pace of regulatory change, respondents were most often extremely or very concerned about *risk technology adaptability to changing regulatory requirements* (52 percent). Roughly half of respondents were also extremely or very concerned about several issues related to IT systems including *legacy systems and antiquated architecture or end-of-life systems* (51 percent), *inability to respond to time-sensitive and*

"The need for new and enhanced regulatory reporting was a catalyst for much of the work we've been doing on the data front, but now it's expanding beyond the regulatory space. We've begun focusing on customer level data and aggregation, to better inform pricing and to more clearly understand profitability."

— **Head of enterprise risk governance,
major regional bank**

ad-hoc requests (49 percent), *lack of flexibility to extend the current systems* (48 percent), and *lack of integration among systems* (44 percent). Given the level of concern about these system-related issues, it appears that there is an opportunity for fintech solutions.

Respondents were least likely to have this level of concern with respect to *lack of aggregation of trading and banking books* (13 percent), *lack of product and asset class coverage* (22 percent), and *lack of cross-asset-class risk calculations* (25 percent).

Conclusion

LOOKING ahead, risk management programs face more uncertainty than they have in recent memory. Will the current environment of historically low interest rates persist or is it finally coming to an end? What will be the economic impacts of the growing opposition in many countries to free trade agreements? How will fintech start-ups disrupt traditional business models?

Perhaps the most important uncertainties address the direction of regulation. In the years since the global financial crisis, financial institutions have faced an unprecedented wave of regulatory changes that has broadened the scope of the issues addressed by regulators, as well as made regulatory requirements substantially more stringent. Each year, the trend has been toward greater regulation. The question for risk management programs was whether they had the ability and resources required to comply with escalating regulatory requirements.

But risk management executives are now asking whether we are nearing an inflection point at which the trend toward continually more stringent regulatory requirements comes to an end or is even in some cases reversed, with some regulations being rolled back.

Yet, even if the recent breakneck pace of new regulatory requirements may not continue, financial

institutions may be well-advised to not scale back their risk management programs. Whether regulatory change will slow or requirements will lessen is far from certain. Institutions that reduce their investment in risk management may find that they are unable to easily adjust their capabilities if new requirements are imposed. Many institutions also have found that the new regulatory requirements have created a new normal and a new set of industry expectations, and may not want to change this norm.

In this uncertain landscape, financial institutions are well-advised to remain vigilant in monitoring regulatory developments and building the capabilities to respond quickly to regulatory changes and remain in compliance. They should also consider being actively involved in the debate over the direction of regulation.

With the future direction of risk management more uncertain than it has been for years, perhaps the most important lesson is that many risk management programs should become more nimble. In the coming years, risk management programs should focus not only on being effective and efficient, but equally on acquiring the agility to respond flexibly to a new set of demands on risk management.

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 International Monetary Fund, *World Economic Outlook*, October 2016, <http://www.imf.org/external/pubs/ft/weo/2016/02/pdf/text.pdf>.
3. Federal Reserve Bank of St. Louis, “Return on average equity for all US banks,” November 15, 2016, <https://fred.stlouisfed.org/series/USROE>; International Monetary Fund, *Global Financial Stability Report*, October 2016, <http://www.imf.org/external/pubs/ft/gfsr/2016/02/pdf/text.pdf>.
4. Data from the European Central Bank reported in “European banks strain to make a profit,” *Stratfor*, August 2, 2016, <https://www.stratfor.com/image/european-banks-strain-make-profit>.
5. International Monetary Fund, *Global financial stability report*.
6. Ibid.; International Monetary Fund, *World Economic Outlook*.
7. *Economist*, “Basel bust-up,” November 26, 2016, <http://www.economist.com/news/finance-and-economics/21710808-european-banks-fear-proposed-revisions-will-penalise-them-unfairly-showdown>.
8. Ibid.
9. European Commission, “Speech by VP Dombrovskis at the European Banking Federation Conference: Embracing disruption,” September 29, 2016, https://ec.europa.eu/commission/2014-2019/dombrovskis/announcements/speech-vp-dombrovskis-european-banking-federation-conference-embracing-disruption_en.
10. John Glover and Nicholas Comfort, “Banks push back against Basel’s ‘surreal’ plans,” *Bloomberg*, August 8, 2016, <https://www.bloomberg.com/news/articles/2016-08-08/banks-look-to-g20-vow-as-bulwark-against-basel-s-surreal-plans>.
11. Deloitte Center for Regulatory Strategies Americas, *Navigating the year ahead: Insurance regulatory outlook 2017*, December 2016, <https://www2.deloitte.com/us/en/pages/regulatory/articles/insurance-regulatory-outlook.html>.
12. US Department of the Treasury, “Treasury, USTR successfully complete negotiations for a covered agreement with the European Union,” January 13, 2017, <https://www.treasury.gov/press-center/press-releases/Pages/jl0705.aspx>.
13. Carrier Management, “US, EU reach insurance regulation agreement,” Wells Media Group, January 13, 2017, <http://www.carriermanagement.com/news/2017/01/13/163069.htm>.
14. Deloitte Center for Regulatory Strategies Americas, *Navigating the year ahead*.
15. Ibid.
16. Ben Protess and Julie Hirschfeld Davis, “Trump moves to roll back Obama-era financial regulations,” *New York Times*, February 3, 2017, <https://www.nytimes.com/2017/02/03/business/dealbook/trump-congress-financial-regulations.html>.

17. President Donald J. Trump, "Presidential memorandum on fiduciary duty rule," Office of the Press Secretary, The White House, February 3, 2017, <https://www.whitehouse.gov/the-press-office/2017/02/03/presidential-memorandum-fiduciary-duty-rule>.
18. Stephen Castle and Steven Erlanger, "In 'Brexit' speech, Theresa May outlines clean break for UK," *New York Times*, January 17, 2017, <https://www.nytimes.com/2017/01/17/world/europe/brexit-theresa-may-uk-eu.html>.
19. *Economist*, "Lost passports," January 21, 2017, <http://www.economist.com/news/finance-and-economics/21715038-negotiating-bespoke-deal-city-after-brexit-will-not-be-easy-how-city>.
20. International Monetary Fund, *World Economic Outlook*.
21. ThreatMetrix, *Cybercrime report, Q2, 2016*; Maria Korolov, "Banks get attacked four times more than other industries," *CSO*, June 23, 2015, <http://www.csoonline.com/article/2938767/advanced-persistent-threats/report-banks-get-attacked-four-times-more-than-other-industries.html>.
22. Warwick Ashford, "Financial institutions on high alert for major cyber attack," *ComputerWeekly.com*, February 11, 2016, <http://www.computerweekly.com/news/4500272926/Financial-institutions-on-high-alert-for-major-cyber-attack>.
23. New York State Department of Financial Services, "DFS issues updated proposed cybersecurity regulation protecting consumers and financial institutions," December 28, 2016, <http://www.dfs.ny.gov/about/press/pr1612281.htm>.
24. Deloitte Centre for Regulatory Strategy Asia Pacific, *Navigating the year ahead: Financial markets regulatory outlook 2017*, December 2016, <https://www2.deloitte.com/ph/en/pages/financial-services/articles/asia-pacific-regulatory-outlook-2017.html>.
25. *Ibid.*
26. Australian Prudential Regulation Authority, *Risk culture*, October 2016, <http://www.apra.gov.au/CrossIndustry/Documents/161018-Information-Paper-Risk-Culture.pdf>.
27. Hong Kong Securities and Futures Commission, *Circular to licensed corporations regarding measures for augmenting the accountability of senior management*, December 16, 2016, <http://www.sfc.hk/edistributionWeb/gateway/EN/circular/openFile?refNo=16EC68>.
28. Mitchell S. Eitel, "FinTech: New regulatory developments," Harvard Law School Forum on Corporate Governance and Financial Regulation, April 17, 2016, <https://corpgov.law.harvard.edu/2016/04/17/fintech-new-regulatory-developments/>; *Economist*, "The fintech revolution," May 9, 2015, <http://www.economist.com/news/leaders/21650546-wave-startups-changing-finance-for-better-fintech-revolution>.
29. Deloitte Centre for Regulatory Strategy EMEA, *Navigating the year ahead: Financial markets regulatory outlook 2017*, December 2016, <https://www2.deloitte.com/nl/nl/pages/financial-services/articles/financial-markets-regulatory-outlook-2017.html>.
30. Roberto Viola, "European Commission sets up and internal task force on financial technology," European Commission, November 14, 2016, <https://ec.europa.eu/digital-single-market/en/blog/european-commission-sets-internal-task-force-financial-technology>.
31. Deloitte Centre for Regulatory Strategy EMEA, *Navigating the year ahead*.
32. "Singapore's fintech journey: Where we are, what is next," speech by Ravi Menon, managing director, Monetary Authority of Singapore, November 16, 2016, <http://www.mas.gov.sg/News-and-Publications/Speeches-and-Monetary-Policy-Statements/Speeches/2016/Singapore-FinTech-Journey.aspx>.

33. Australian Securities and Investments Commission, "16-440MR ASIC releases world-first licensing exemption for fintech businesses," December 15, 2016, <http://www.asic.gov.au/about-asic/media-centre/find-a-media-release/2016-releases/16-440mr-asic-releases-world-first-licensing-exemption-for-fintech-businesses/>.
34. *Economist*, "Banking and fintech: Love and war," December 5, 2016, <http://www.economist.com/news/finance-and-economics/21679478-unlikely-romance-blossoms-love-and-war>.
35. Percentages total more than 100 percent since some institutions provide more than one type of service. In the 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" or "insurers" (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).
36. Basel Committee on Banking Supervision, *Guidelines: Corporate governance principles for banks*, July 2015, <http://www.bis.org/bcbs/publ/d328.pdf>.
37. Deloitte Center for Regulatory Strategies, *Final look: A practical guide to the Federal Reserve's enhanced prudential standards for domestic banks, 2014*.
38. Ibid.
39. National Association of Insurance Commissioners, "NAIC committee adopts corporate governance models," August 18, 2014, http://www.naic.org/cipr_topics/topic_corporate_governance.htm.
40. Australian Prudential Regulation Authority, "Prudential standard CPS 220: Risk management," January 2015, <http://www.apra.gov.au/CrossIndustry/Documents/Prudential-Standard-CPS-220-Risk-Management-January-2015.pdf>.
41. Basel Committee on Banking Supervision, *Principles for enhancing corporate governance*, October 2010, <http://www.bis.org/publ/bcbs176.pdf>; Basel Committee on Banking Supervision, *Guidelines: Corporate governance principles for banks*, July 2015.
42. Official journal of the European Union, "Directive 2013/36/EU of the European Parliament and of the Council, Article 76," June 26, 2013, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:176:0338:0436:EN:PDF>.
43. Basel Committee on Banking Supervision, *Principles for enhancing corporate governance*.
44. Financial Stability Board, *Principles for an effective risk appetite framework*, November 2013, http://www.financialstabilityboard.org/wp-content/uploads/r_131118.pdf.
45. Basel Committee on Banking Supervision, *Guidelines: Corporate governance principles for banks*.
46. In the ninth edition of the survey, respondents were asked about the expected change in risk management spending over the next three years.
47. Deloitte Center for Regulatory Strategy Americas, *Navigating the year ahead*.
48. Deloitte Centre for Regulatory Strategy Asia Pacific, *Navigating the year ahead*.
49. Ibid.
50. Japan Financial Services Authority, *Overview of results of ERM assessment based on ORSA reports and ERM hearings*, September 15, 2016, <http://www.fsa.go.jp/en/news/2016/20160915-1.html>.
51. The results in this section regarding the uses and challenges of capital stress testing are based on respondents who reported their institution using capital stress tests.

52. The Financial Stability Board, *Policy recommendations to address structural vulnerabilities from asset management activities*, January 12, 2017, <http://www.fsb.org/wp-content/uploads/FSB-Policy-Recommendations-on-Asset-Management-Structural-Vulnerabilities.pdf>; International Organization of Securities Commissions, "IOSCO publishes report on liquidity management tools in CIS," December 17, 2015, <https://www.iosco.org/news/pdf/IOSCONEWS411.pdf>.
53. The results in this section regarding the uses and challenges of liquidity stress testing are based on respondents who reported their institution using liquidity stress tests.
54. Basel Committee on Banking Supervision, *Minimum capital requirements for market risk*, January 2016, <http://www.bis.org/bcbs/publ/d352.pdf>.
55. Basel Committee on Banking Supervision, *Consultative document: Reducing variation in credit risk-weighted assets – constraints on the use of internal model approaches*, March 2016, <http://www.bis.org/bcbs/publ/d362.pdf>.
56. Basel Committee on Banking Supervision, *Capital floors: The design of a framework based on standardized approaches*, December 2014, <http://www.bis.org/bcbs/publ/d306.pdf>.
57. Basel Committee on Banking Supervision, *Consultative document: Standardised measurement approach for operational risk*, March 2016, <http://www.bis.org/bcbs/publ/d355.pdf>.
58. This question was asked of respondents at institutions that are either subject to Solvency II, subject to similar regulatory capital requirements, or not subject to Solvency II or similar requirements but have adopted them.
59. Deloitte Centre for Regulatory Strategy Asia Pacific, *Navigating the year ahead*.
60. The results in the section are based on questions that were only asked of respondents at institutions that provide insurance services.
61. The survey results in this section are based on questions that were only asked of respondents at institutions that provide investment management services.
62. This item was not included in the 2014 survey.
63. Deloitte Center for Regulatory Strategies Americas, *Navigating the year ahead*.
64. International Organization of Securities Commissions, "IOSCO publishes report on liquidity management tools in CIS."
65. Financial Standards Accounting Board, *Financial instruments—Credit losses; measurement of credit losses on financial instruments*, June 2016, http://www.fasb.org/jsp/FASB/Document_C/DocumentPage?cid=1176168232528&acceptedDisclaimer=true.
66. This item was not included in the ninth edition of the survey.
67. John Glover, "Banks' hands tied as Basel tightens rules on operational risk," Bloomberg Technology, March 4, 2016, <https://www.bloomberg.com/news/articles/2016-03-04/banks-hands-tied-as-basel-tightens-rules-on-operational-risk>.
68. Office of the Comptroller of the Currency, "Third-party relationships: Risk management guidance," October 30, 2013, <https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html>.

CONTACTS

GLOBAL FINANCIAL SERVICES INDUSTRY LEADERSHIP

Bob Contri

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

Anna Celner

Global leader
Banking & securities
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

SURVEY EDITOR

Edward T. Hida II, CFA

Risk & capital management leader

Financial Services

Deloitte & Touche LLP

+1 212 436 4854

ehida@deloitte.com

ABOUT THE EDITOR

Edward Hida leads Deloitte's global risk & capital management group and is an 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.

ACKNOWLEDGEMENTS

This report is a 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:

Michelle Dahl, Deloitte Services LP

Matt Gantz, Deloitte & Touche LLP

Shelly Marie Marshall, Deloitte & Touche LLP

Claire Miller, Deloitte & Touche LLP

CONTRIBUTORS

Katie Bryant

Deloitte Australia
katbryant@deloitte.com.au

Joseph Burdis

Deloitte US
jburdis@deloitte.com

James H. Caldwell

Deloitte US
jacaldwell@deloitte.com

Eric Clapprood

Deloitte US
eclapprood@deloitte.com

Doug Dannemiller

Deloitte US
ddannemiller@deloitte.com

Karl Ehram

Deloitte US
kehrsam@deloitte.com

Christopher Faile

Deloitte US
cfaile@deloitte.com

Michael Fay

Deloitte US
mifay@deloitte.com

Brian Flanagan

Deloitte US
brianflanagan@deloitte.com

Tony Frame

Deloitte US
aframe@deloitte.com

Richard Godfrey

Deloitte US
rgodfrey@deloitte.com

Christopher Hogan

Deloitte US
chhogan@deloitte.com

Elizabeth Jordan

Deloitte US
ejordan@deloitte.com

Dilip Krishna, CFA

Deloitte US
dkrishna@deloitte.com

Alexander LePore

Deloitte US
alepore@deloitte.com

Kevin McGovern

Deloitte US
kmcgovern@deloitte.com

Kevin Nixon

Deloitte Australia
kevinnixon@deloitte.com.au

Brian O'Neill

Deloitte US
brianeoneill@deloitte.com

Monica O'Reilly

Deloitte US
monoreilly@deloitte.com

Jonathan Jules Prejean

Deloitte US
jprejean@deloitte.com

Martin Prince

Deloitte US
maprince@deloitte.com

Christopher Spoth

Deloitte US
cspotth@deloitte.com

David Strachan

Deloitte UK
dastrachan@deloitte.co.uk

David Wright

Deloitte US
davidwright@deloitte.com

GLOBAL RISK & CAPITAL MANAGEMENT CONTACTS

ARGENTINA

Raul Antonio Malvestiti
Deloitte Argentina
rmalvestiti@deloitte.com

Gustavo Fabian Serenelli
Deloitte Argentina
gserenelli@deloitte.com

Jorge Serenelli
Deloitte Argentina
jserenelli@deloitte.com

AUSTRALIA

Steven Cunico
Deloitte Australia
scunico@deloitte.com.au

Peter Matruglio
Deloitte Australia
pmatruglio@deloitte.com.au

Timothy Oldham
Deloitte Australia
toldham@deloitte.com.au

AUSTRIA

Kurt Blecha
Deloitte Austria
kblecha@deloitte.at

Dominik Damm
Deloitte Austria
ddamm@deloitte.at

BELGIUM

Roeland Baeten
Deloitte Belgium
rbaeten@deloitte.com

Arno De Groot
Deloitte Belgium
adegroote@deloitte.com

Yves Dehogne
Deloitte Belgium
ydehogne@deloitte.com

BRAZIL

Anselmo Bonservizzi
Deloitte Brazil
abonservizzi@deloitte.com

Luiz Fernando Ferreira Dias
Deloitte Brazil
luizdias@deloitte.com

Rodrigo Mendes Duarte
Deloitte Brazil
rodrigomendes@deloitte.com

Marcello de Francesco
Deloitte Brazil
mfrancesco@deloitte.com

Gustavo Amaral de Lucena
Deloitte Brazil
gustavolucena@deloitte.com

Elias Zoghbi
Deloitte Brazil
eliaszoghbi@deloitte.com

CANADA

Azer Hann
Deloitte Canada
ahann@deloitte.ca

Victoria Loutsiv
Deloitte Canada
vloutsiv@deloitte.ca

CARIBBEAN

Lise Baril

Deloitte Cayman Islands
lbaril@deloitte.com

Taron Jackman

Deloitte Cayman Islands
tjackman@deloitte.com

CHILE

Christian Duran

Deloitte Chile
chrduran@deloitte.com

Fernando Gaziano

Deloitte Chile
fpgaziano@deloitte.com

Pablo Herrera

Deloitte Chile
paherrera@deloitte.com

CHINA

Eddie Chiu

Deloitte China
eddchiu@deloitte.com.cn

Ye Fang

Deloitte China
yefang@deloitte.com.cn

Tony Wood

Deloitte China
tonywood@deloitte.com.hk

Lynda Wu

Deloitte China
lyndawu@deloitte.com.cn

COLOMBIA

Elsa Mena

Deloitte Colombia
emenacardona@deloitte.com

CYPRUS

Panicos Papamichael

Deloitte Cyprus
ppapamichael@deloitte.com

DENMARK

Hans Van Leeuwen

Deloitte Denmark
hleeuwen@deloitte.dk

FINLAND

Lasse Ingstrom

Deloitte Finland
lasse.ingstrom@deloitte.fi

FRANCE

Marc Van Caeneghem

Deloitte France
mvancaeneghem@deloitte.fr

Michel Guidoux

Deloitte France
mguidoux@deloitte.fr

GERMANY

Michael Cluse

Deloitte Germany
mcluse@deloitte.de

Jörg Engels

Deloitte Germany
jengels@deloitte.de

GREECE

Thanos Papanikolaou

Deloitte Greece
tpapanikolaou@deloitte.gr

ICELAND

Arni Jon Arnason

Deloitte Iceland
arni.jon.arnason@deloitte.is

INDIA

Abhinava Bajpai

Deloitte India
abbajpai@deloitte.com

Abhay Gupte

Deloitte India
agupte@deloitte.com

Aruna Pannala

Deloitte India
apannala@deloitte.com

Muzammil Patel

Deloitte India
muzammilpatel@deloitte.com

INDONESIA

Brian Johannes Indradjaja

Deloitte Indonesia
bindradjaja@deloitte.com

Claudia Lauw

Deloitte Indonesia
clauw@deloitte.com

Richard Ticoalu

Deloitte Indonesia
rticoalu@deloitte.com

IRELAND

John McCarroll

Deloitte Ireland
jmccarroll@deloitte.ie

Colm McDonnell

Deloitte Ireland
cmcdonnell@deloitte.ie

Martin Reilly

Deloitte Ireland
mreilly@deloitte.ie

Sean Smith

Deloitte Ireland
seansmith1@deloitte.ie

ISRAEL

Avi Keisar

Deloitte Israel
akeisar@deloitte.co.il

ITALY

Stefano Appetiti

Deloitte Italy
sappetiti@deloitte.it

Antonio Arfè

Deloitte Italy
aarfe@deloitte.it

Pierluigi Brienza

Deloitte Italy
pbrienza@deloitte.it

Paolo Gianturco

Deloitte Italy
pgianturco@deloitte.it

Lorenzo Manganini

Deloitte Italy
lmanganini@deloitte.it

Luigi Mastrangelo

Deloitte Italy
lmastrangelo@deloitte.it

JAPAN

Daisuke Kuwabara

Deloitte Japan
daisuke.kuwabara@tohatsu.co.jp

Tsuyoshi Oyama

Deloitte Japan
tsuyoshi.oyama@tohatsu.co.jp

Hiroshi Sakui

Deloitte Japan
hiroshi.sakui@tohatsu.co.jp

Kentaro Takaya

Deloitte Japan
kentaro.takaya@tohatsu.co.jp

KENYA

Julie Akinyi Nyangaya
Deloitte Kenya
jnyangaya@deloitte.co.ke

LUXEMBOURG

Laurent Berliner
Deloitte Luxembourg
lberliner@deloitte.lu

Martin Flaunet
Deloitte Luxembourg
mflaunet@deloitte.lu

Marco Lichtfous
Deloitte Luxembourg
mlichtfous@deloitte.lu

Jean Philippe Peters
Deloitte Luxembourg
jppeters@deloitte.lu

Xavier Zaegel
Deloitte Luxembourg
xzaegel@deloitte.lu

MALAYSIA

Fazlin Hanoum Ilhan
Deloitte Malaysia
filhan@deloitte.com

Muzafar Kamal
Deloitte Malaysia
muzafarkamal@deloitte.com

MALTA

Mark Micallef
Deloitte Malta
mmicallef@deloitte.com.mt

MEXICO

Miguel Hernandez
Deloitte Mexico
mihernandez@deloittemx.com

Miguel Angel Garcia Martinez
Deloitte Mexico
miggarcia@deloittemx.com

Carlos Perez
Deloitte Mexico
caperez@deloittemx.com

MIDDLE EAST

Aejaz Ahmed
Deloitte Middle East
aeahmed@deloitte.com

Fadi Sidani
Deloitte Middle East
fsidani@deloitte.com

THE NETHERLANDS

Harold Malaihollo
Deloitte Netherlands
hmalaihollo@deloitte.nl

Evert Van der Steen
Deloitte Netherlands
evandersteen@deloitte.nl

Marco Vet
Deloitte Netherlands
mvet@deloitte.nl

NEW ZEALAND

Rodger Murphy
Deloitte New Zealand
rodgermurphy@deloitte.co.nz

NIGERIA

Joseph Olofinsola
Deloitte Nigeria
jlofinsola@deloitte.com.ng

NORWAY

Sverre Danielsen
Deloitte Norway
sdanielsen@deloitte.no

PHILIPPINES

Simon Lee

Deloitte Philippines
leesimon@deloitte.com

POLAND

Adam Kolaczyk

Deloitte Poland
akolaczyk@deloittece.com

Zbigniew Szczerbetka

Deloitte Poland
zszczerbetka@deloittece.com

Dariusz Szkaradek

Deloitte Poland
dszkaradek@deloittece.com

PORTUGAL

Joao Gomes Ferreira

Deloitte Portugal
joaoferreira@deloitte.pt

Vitor Viana Lopes

Deloitte Portugal
vlopes@deloitte.pt

Miguel Filipe Morais

Deloitte Portugal
mmorais@deloitte.pt

Goncalo Nogueira Simoes

Deloitte Portugal
gsimoes@deloitte.pt

RUSSIA

Julia Brovkovitch

Deloitte Russia
jbrovkovitch@deloitte.ru

SINGAPORE

Frederic Bertholon-Lampiris

Deloitte Singapore
flampiris@deloitte.com

Raghu Mehra

Deloitte Singapore
rmehra@deloitte.com

Tse Gan Thio

Deloitte Singapore
tgthio@deloitte.com

SOUTH AFRICA

Wayne Savage

Deloitte South Africa
dsavage@deloitte.co.za

Catherine Stretton

Deloitte South Africa
cstretton@deloitte.co.za

SOUTH KOREA

Seung Woo Lee

Deloitte South Korea
seungwoolee@deloitte.com

Jung In Lee

Deloitte South Korea
junginlee@deloitte.com

Ki Wan Lee

Deloitte South Korea
kilee@deloitte.com

Jong Won Oh

Deloitte South Korea
jongwonoh@deloitte.com

SPAIN

Rafael Campo Bernad

Deloitte Spain
rcampobernad@deloitte.es

Cesar Gurrea

Deloitte Spain
cgurrea@deloitte.es

SWEDEN

Elisabeth Werneman

Deloitte Sweden
ewerneman@deloitte.se

SWITZERLAND

Leif Boegelein

Deloitte Switzerland
lboegelein@deloitte.ch

Philipp Keller

Deloitte Switzerland
phkeller@deloitte.ch

TAIWAN

Thomas Wan

Deloitte Taiwan
thomaswan@deloitte.com.tw

THAILAND

Somkrit Krishnamra

Deloitte Thailand
somkrishnamra@deloitte.com

TURKEY

Itir Sogancilar

Deloitte Turkey
isogancilar@deloitte.com

UNITED KINGDOM

Zeshan Choudhry

Deloitte UK
zchoudhry@deloitte.co.uk

Hubert Justal

Deloitte UK
hubjustal@deloitte.co.uk

Enrico Messori

Deloitte UK
emessori@deloitte.co.uk

Vishal Vedi

Deloitte UK
vvedi@deloitte.co.uk

David Strachan

Deloitte UK
dastrachan@deloitte.co.uk

UNITED STATES

A. Scott Baret

Deloitte US
sbaret@deloitte.com

Edward T. Hida II, CFA

Deloitte US
ehida@deloitte.com

Robert Maxant

Deloitte US
rmaxant@deloitte.com

Alok Sinha

Deloitte US
asinha@deloitte.com

VIETNAM

Tho Nguyen Thi Anh

Deloitte Vietnam
thonguyen@deloitte.com

Ngoc Tran

Deloitte Vietnam
ntran@deloitte.com

Deloitte. University Press



Follow @DU_Press

Sign up for Deloitte University Press updates at www.dupress.deloitte.com.

About Deloitte University Press

Deloitte University Press 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 University Press is an imprint of Deloitte Development LLC.

About this publication

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

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

About Deloitte

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

Copyright © 2017 Deloitte Development LLC. All rights reserved.
Member of Deloitte Touche Tohmatsu Limited