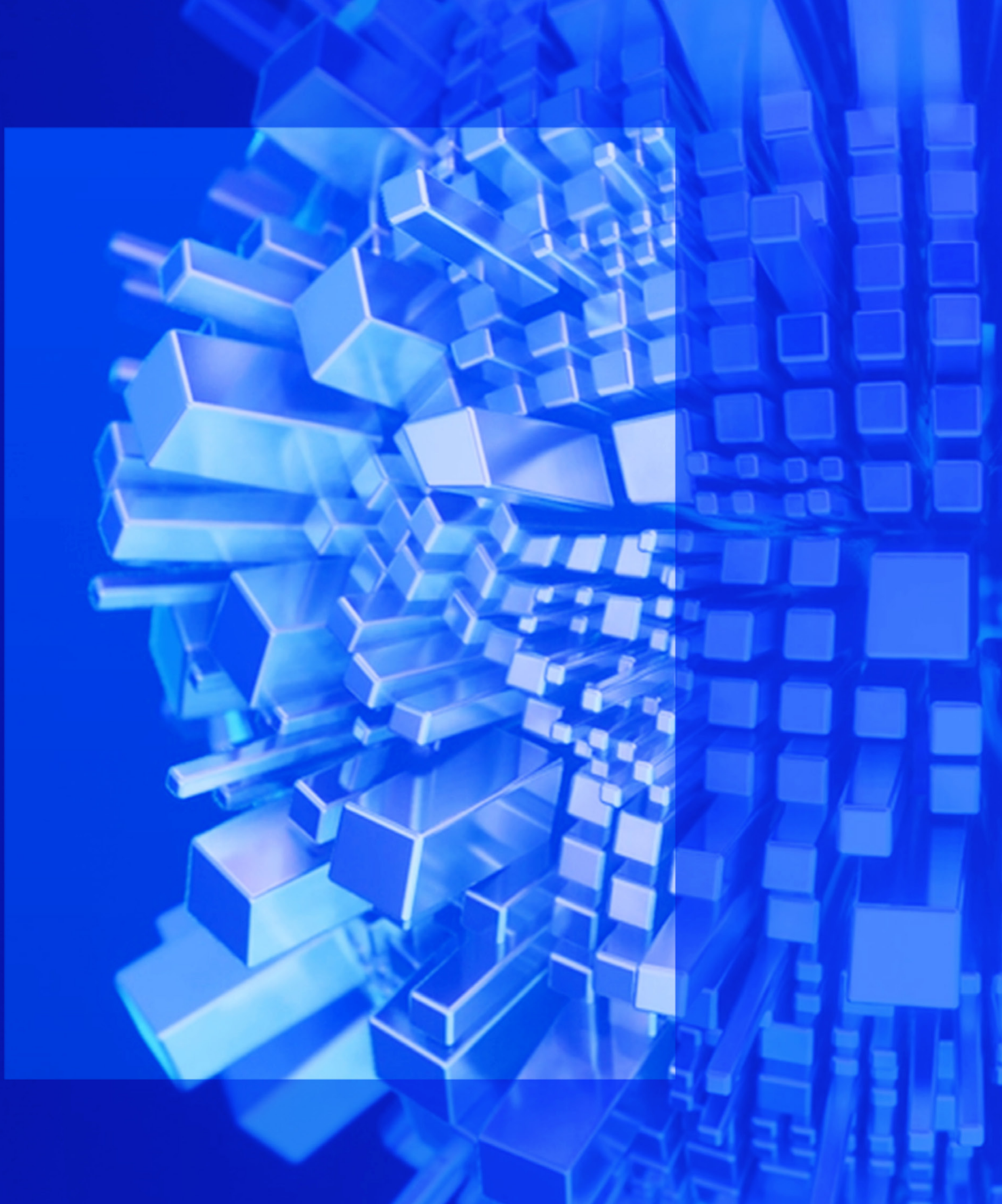
KPMG

Chief Risk Officer Survey

Industry perspective:
Financial Services



read.kpmg.us/CROSurvey

01

Introduction

Chief Risk Officers (CROs) at Financial Services (FS) companies are facing an increasingly complex risk landscape. Cyber-attacks, business resiliency, and regulatory compliance are among the key threats. At the same time, CROs are under pressure to increase efficiencies, while adopting innovative technologies. And as the link between business stability and growth becomes clearer, the momentum around risk transformation will only intensify.

Consequently, FS companies are looking to strengthen risk reporting and insights, enhance data analytics capabilities, and upskill employees to manage risks. Many are also looking to artificial intelligence (AI), machine learning (ML), and cloud-based solutions to accelerate and improve risk-management processes. Perhaps most significant, risk functions are no longer solely focused on compliance but are expected to align risk strategy with the growth strategy of the organization.

To gain better insights into the risk-management issues facing businesses today, KPMG LLP (KPMG) conducted its 2023 Chief Risk Officer Survey. The survey results show how companies are addressing current and future risk challenges, opportunities, and priorities across five intersecting drivers of risk transformation: de-risking, growth or strategic change, compliance risk, effectiveness and efficiency, and cost takeout. This report examines our overall survey to identify the challenges specifically facing the FS sector, reflecting data from 139 U.S. FS risk executives who responded and analysis and perspectives of KPMG Risk Advisory partners. In this paper, we also dig into our data to reveal issues related to key FS subsectors, including banking and capital markets (B&CM), asset management (AM), and insurance (INS).

One of the primary risk challenges identified by the FS sector is the increasing threat of cybersecurity and data breaches, suggesting an urgent need for investment in technology-based solutions and employee training to develop robust cybersecurity measures. Regulatory changes and compliance issues also pose a significant challenge for the FS sector, particularly for larger institutions facing new regulatory demands and increased scrutiny from regulators.

Generally, our survey shows that organizations feel they are adequately equipped to address most of their key risk challenges. However, there are other areas where companies feel less prepared, like market risks and reputational damage, possibly due to concerns about issues including the overall stability of banks, and their ability to govern and manage capital requirements, interest rates, and liquidity.

FS risk executives acknowledge receiving a high level of support from their C-suite, but they still desire greater collaboration around integrating risk management with business strategy. On the other hand, risk management budgets are increasing, with information technology infrastructure and technology-driven risk management as top spending priorities to increase efficiencies. Similarly, AI and ML are increasingly becoming essential elements of risk management processes, with a majority of respondents recognizing their critical role.

Overall, this survey report provides valuable insights into the risk management efforts within the FS sector, highlighting the challenges, strategies, and priorities for risk management in the coming years.

Exhibit 1. Five intersecting drivers

De-risking: Organizations' effort to reduce risk exposure and hedge against expected market conditions

Growth or strategic change: Organizations' organic or inorganic growth; change in products, services, delivery channels; and/or other large-scale strategic initiatives

Compliance risk: New or emerging regulatory requirements, non-compliances with existing requirements, or need to enhance the relationship with oversight authorities

Effectiveness and efficiency: Increase the quality, consistency, extensibility, and confidence in risk management requirements and outputs

Cost takeout: Reduce the overall costs associated with the governance, maintenance, oversight, and execution of risk requirements and practices

© 2024 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

02

De-risking

Organizations' efforts to reduce risk exposure and hedge against expected market conditions

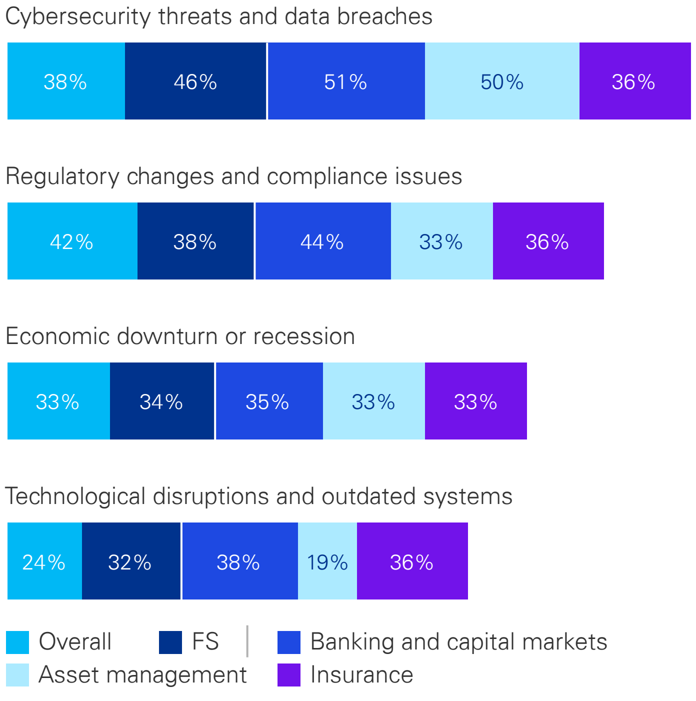
Key findings

Recognizing the major risks facing an organization is the first step to minimizing risk exposure. In the FS sector, cybersecurity threats and data breaches were seen as the top risk challenges facing FS businesses in the next two to five years, cited by 46 percent of respondents (Exhibit 2). This result is not surprising since the sector has faced an uptick in cyber-threat activity, particularly those that are geopolitically driven, and suggests an imminent need to invest in robust cybersecurity measures. This concern around cybersecurity was even higher in the B&CM (51 percent) and AM (50 percent) subsectors, which suggests these companies have a greater vulnerability to malicious hackers. Regulatory changes and compliance issues are also a concern, with larger institutions facing a complex regulatory landscape, both domestic and global, a continual stream of new and more stringent regulatory demands, and increased scrutiny from regulators. In particular, regulators are looking more intensely at FS companies' data management and data governance practices over risk management data, from aggregation capabilities to internal risk reporting practices.

De-risking also requires a plan that enables the organization to be prepared to deal with any adverse event caused by its risk exposure. Respondents saw their organization as having some level of preparedness for nearly all of the top challenges they cited. For example, 79 percent of FS respondents are well or very well prepared for challenges associated with financial risks. Among subsectors, B&CM has a slightly higher level of confidence (84 percent) when it comes to managing financial risks, whereas the AM subsector has the least confidence (66 percent). On the downside, more than half of the respondents said they were least prepared to manage market risks (e.g., competitor disruption, changes in consumer needs or market trends) and reputational damage or negative public perception.

Exhibit 2. Top challenges your organization will face within the next 2–5 years

Q. What do you think are the biggest challenges your organization will face within the next 2–5 years?



"Overall" includes all industries; "FS" combines B&CM, AM and INS

© 2024 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

01
02
03
04
05
06
07
08

Recommendations

- With technology evolving faster than cybersecurity, risk management, and governance, FS companies should thoroughly assess changes to vulnerabilities due to the integration of emerging technologies across the enterprise, including country risk assessments. Invest in technology-based solutions and employee training to enhance cybersecurity measures and protect against data breaches, as well as measure and assess impact and determine a corrective course of action. Align with regulatory changes and ensure compliance by implementing necessary measures and processes.
- Boards and leaders should continue to ask "what if" questions, putting stress on the organization to answer and prepare, including enhancing scenario planning capabilities.
- Strengthen fraud detection, prevention, and response mechanisms to minimize losses due to fraudulent activities; react quickly to emerging threats; and apply the right balance of governance that protects customers and operations.

"Financial services CROs must develop a rigorous and disciplined risk agenda commensurate with operational, business, and strategic plans. This will enable them to proactively address and solve issues from a wide range of stakeholders, including investors, regulators, and customers."

— Anand Desai, Principal, Advisory – Financial Services Line of Business Leader, Risk Services

© 2024 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

03

Growth or strategic change

Organizations' organic or inorganic growth; change in products, services, delivery channels; and other large-scale strategic initiatives

Key findings

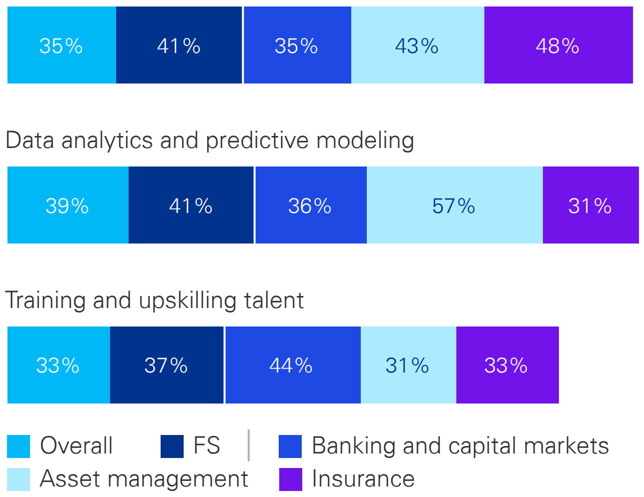
Ideally, risk management should be aligning its activities with the business' goals around products, services, and strategic initiatives. To achieve that alignment, FS respondents cited these three activities as their top strategies: 49 percent said analyzing risk mitigation successes and updating the corporate strategy accordingly, 47 percent indicated providing training and resources for employees on risk management and corporate strategy alignment, while 46 percent said fostering a strong risk and compliance culture as part of enterprise-wide strategy. Among subsectors, B&CM (53 percent) and INS (55 percent) cited providing training and resources to employees on risk management and corporate strategy alignment as a top strategy.

However, our survey also found where risk organizations' alignment with business goals could be improved. Among respondents, 41 percent said that risk reporting and insights was the most critical factor to enhance an organization's risk resiliency in the next few years. In the subsectors, the survey results show that data analytics is the top priority (57 percent) for risk management activity in AM, while the focus for B&CM is on upskilling employees (44 percent) to manage risks (Exhibit 3).

Also critical to aligning risk management to the business is support from the C-suite. Here, the survey results are generally positive, with 82 percent of respondents reporting that they receive a high level of support from their C-suite, while only 17 percent viewed the level of support as only moderate. However, a significant majority—60 percent—of FS respondents said they still desired more significant support from senior management in areas such as ensuring the overall alignment of the risk management with business strategy. In INS, the number was even higher, with 71 percent mentioning they require senior management's attention to support risk management efforts. The apparent disconnect of the results may suggest that while FS risk management executives recognize support from upper management, for some activities, they do not feel they have the authority to impose needed risk protocols on their own.

Exhibit 3. Top risk management activities that will be enhanced in the next two years

Q. Which risk management framework components and activities within your risk organization will be enhanced/strengthened the most over the next two years?



"Overall" includes all industries; "FS" combines B&CM, AM and INS

© 2024 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Recommendations

- Reporting, insights, data analytics, and predictive modeling are closely related, with one driving the other. Invest in data-acquisition processes to drive the most insightful reporting around early warning, emerging risk, notable changes in risk profile and risk levels, and the risk/return trade-off.
- Helping the organization make decisions and investments where there is greater certainty of upside and reduced severity of downside will enhance the risk function's value. As such, the risk framework should be designed to surface and disseminate information that business decision-makers should know but don't know, provide informed perspectives on "what if" scenarios," and tap the brakes when appropriate.
- Strengthen risk reporting and insights, enhance data analytics capabilities, and provide training and resources to employees on risk management and corporate strategy alignment.
- Attract talent with specific risk domain expertise in the first line-of-defense functions to help you more effectively manage evolving risks.

© 2024 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

04

Compliance risk

New or emerging regulatory requirements, noncompliance with existing requirements, or need to enhance the relationship with oversight authorities

Key findings

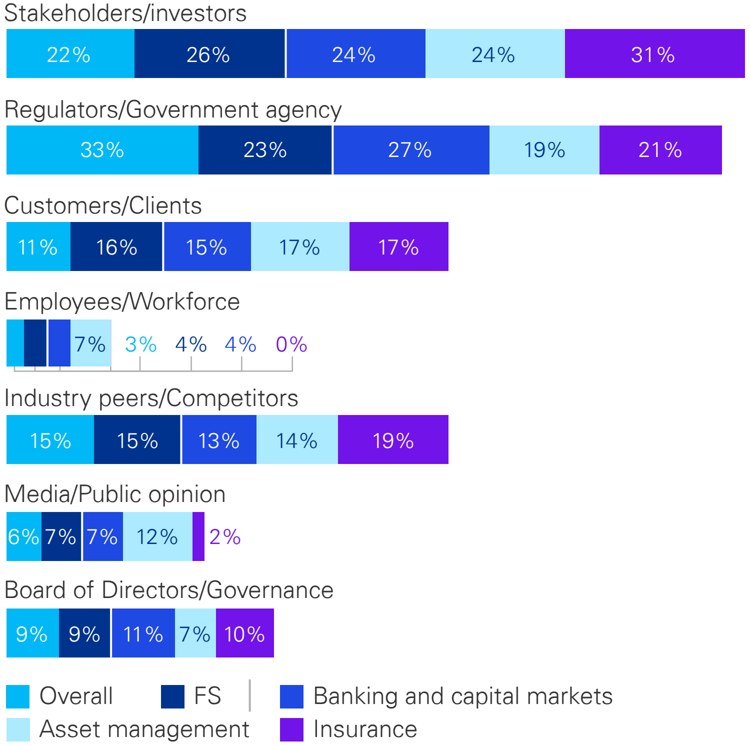
Regulatory activities—both domestic and global—are increasing in pace, scale, and complexity. In our survey, regulatory changes and compliance issues was named as one of the top challenges FS organizations will face in the next two to five years, cited by 38 percent of respondents and coming in just behind cyber threats and data breaches. The result was relatively consistent across subsectors, with B&CM at 44 percent, AM at 33 percent, and INS at 36 percent.

FS is one of the most heavily regulated industries. Not only are FS firms subject to numerous regulations, but those regulations often conflict or overlap. Many of these regulations are an effort to ensure that risk management and related decisions are based on data that is complete and accurate in which the firm has confidence. New rules around liquidity, capital, climate risk, and environmental, social, and governance (ESG), for example, are increasingly stringent in their demands, often imposing heavy fines for failure to comply. These compliance challenges are the primary drivers for investments in risk management, along with a sense among CROs of heightened exposure to new and highly complicated threats, like cyber and state-sponsored criminal activity. Moreover, regulators are demanding continuous improvement, so what is sufficient today may be deficient tomorrow. Consequently, companies can expect an uptick in examinations and investigations, with regulators looking for demonstrable evidence of compliance, as well as proper resourcing and investment.

In addition to industry regulators, investors/shareholders, customers, employees, and the even general public (e.g., through social media) can exert pressures on companies and hold them accountable for their strategies, operations, and compliance activities. In our survey, 26 percent of FS respondents cited stakeholders/investors as the parties from which they receive the most pressure, interest, and/or heightened expectations around risk management, followed by regulators/government agencies at 23 percent, and customers/clients at 16 percent (Exhibit 4).

Exhibit 4. Addressing stakeholder concerns

Q. As it relates to risk management, from which of the following stakeholders are you getting the most pressure, interest, and/or heightened expectations?



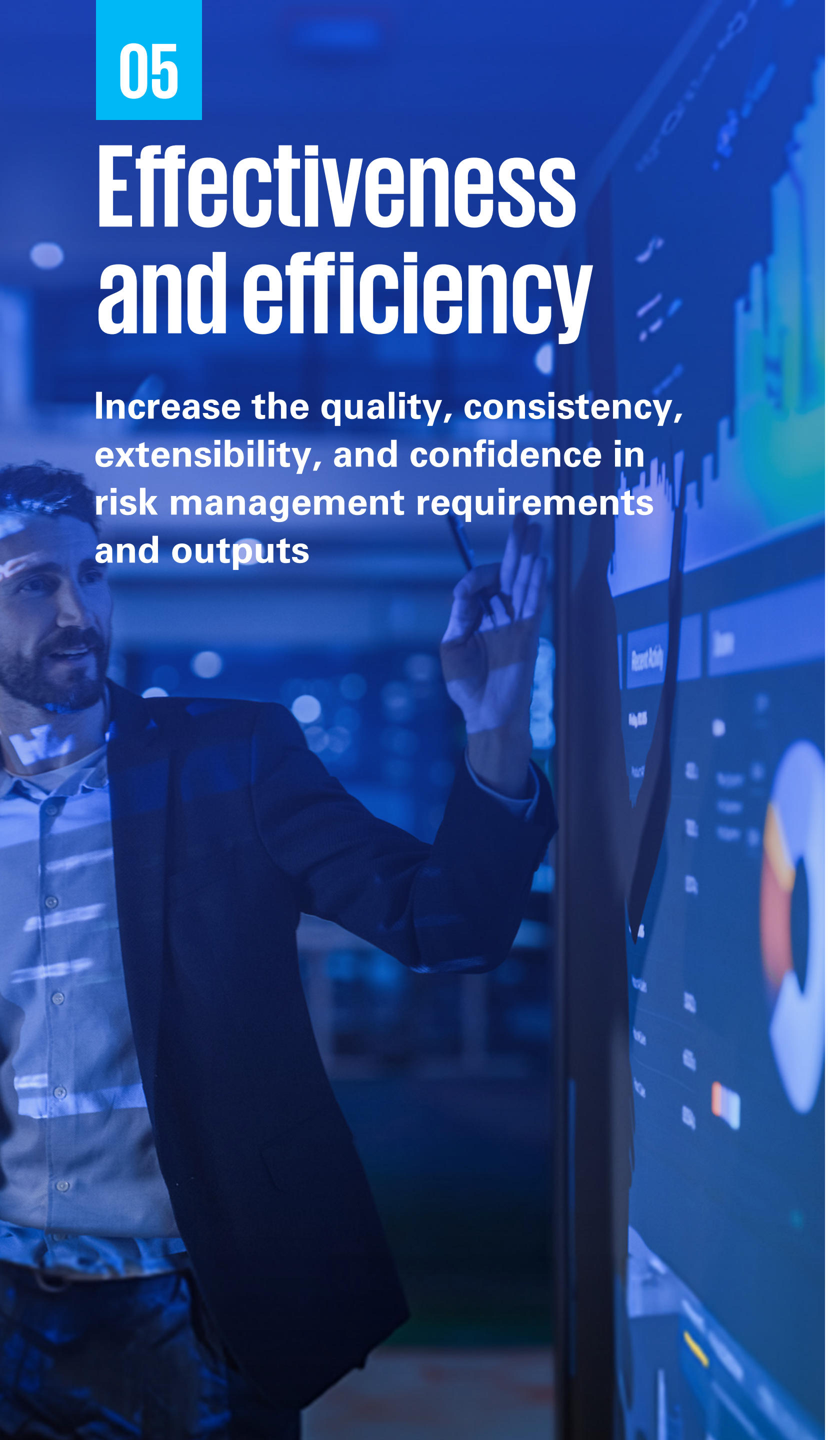
"Overall" includes all industries; "FS" combines B&CM, AM and INS

© 2024 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Recommendations

- Prioritize compliance risks as integral with strategic business priorities and funding. Build compliance assessments and controls upfront and ongoing, as a core element to business strategy. Strive to understand all of the issues that could potentially compromise the organization's risk management posture.
- While it might require significant changes to the risk function, do not shortcut potential issues with regulators or other stakeholders and be sure to appropriately assess potential risk impacts. Invest accordingly to help ensure small problems do not grow into large ones.
- Risk and compliance teams should focus not only on preventing, detecting, and responding to compliance risks, but also on driving trust across the commercial needs of the business.
- Expend effort to understand the principles that regulators are looking to see the organization embrace, in addition to the formal regulatory obligations, and align the risk strategy to meet those objectives.

© 2024 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.



05

Effectiveness and efficiency

Increase the quality, consistency, extensibility, and confidence in risk management requirements and outputs

Key findings

After remaining relatively unchanged for the past year, FS companies are increasing their spending on risk management. Much of that spending is going toward new technology and employee training to keep risk functions effective, efficient, and current. Overall, 56 percent of FS respondents reported that their risk management budget remained the same (-5 percent to +5 percent) in last 12 months, while 38 percent experienced an increase of 5 percent to 10 percent in their budget. However, the next 12 months are expected to be more favorable for risk investments, with 90 percent of the respondents anticipating an increase of more than 5 percent in their risk management budget.

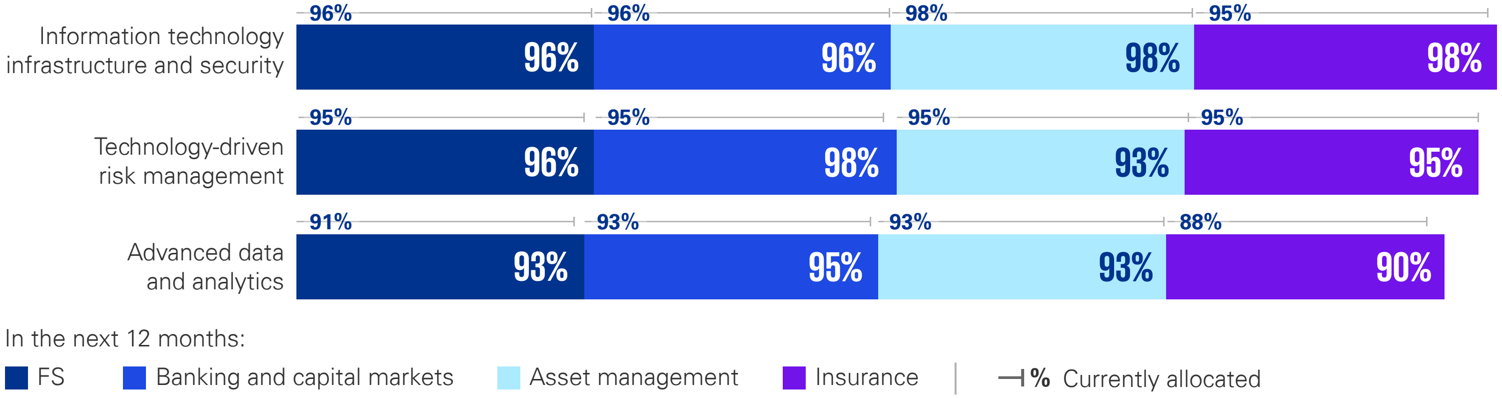
For those organizations planning to increase risk-management budgets to improve risk efficiency and effectiveness, technology remains a key area of investment. Respondents say as their current top three spending priorities information technology infrastructure and security (96 percent), followed by technology-driven risk management (95 percent), and advanced data and analytics (91 percent). The allocation for advanced data and analytics in the banking, capital markets, and insurance sub sectors is expected to experience a modest growth of 2 percent in the next 12 months (Exhibit 5).

When it comes to increasing efficiencies, AI and ML are becoming essential elements of organizations' risk technology landscape. In the survey, a majority of respondents indicated that AI and ML would play a critical role in accelerating risk management processes within their organizations in both the current (56 percent) and future (63 percent) state. Additionally, 50 percent said their organizations use AI and ML to collaborate with industry peers, partners, and experts to gain insights into best practices and risk mitigation strategies when selecting and prioritizing AI and ML use cases. In the INS subsector, 65 percent of the respondents align to the same perception. Among the AM subsector respondents, 59 percent reported using AI and ML to engage cross-functional teams of stakeholders and risk management perspectives in the selection and prioritization of AI and ML use cases.

© 2024 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Exhibit 5. Current and future allocation of risk management budget

Q. How is your risk management budget currently allocated? How do you anticipate allocating your risk management budget for the next 12 months?



Recommendations

- Technology is at the heart of efforts to improve risk efficiency and effectiveness. Allocate budget toward information technology infrastructure and technology-driven risk management. Organizations that use modern technology to improve, update, and enhance their risk function are better able to meet heightened expectations.
- Embrace digital solutions such as AI, ML, cybersecurity, and cloud-based solutions. Ensure digital acceleration of the risk function is in sync with the organization's transformation goals. Integrating strategically selected digital tools and techniques into risk processes can meaningfully propel its transformation. At the same time, be aware of the inherent risks of new technologies, such as AI, and ensure risk-management oversight is applied to their use.
- The skill sets for delivering risk services are changing. To manage the challenges, risk functions will need to acquire or upskill talent, especially in technical areas. Supplementing risk professionals with technical resources, including big data skills and the ability to build and use emerging technologies, will be important to future readiness.
- Implement automation in various processes to improve efficiency and reduce human error. Invest in digital technologies to enhance customer experience, reduce processing times, and lower operational costs.

> **"Help the C-suite make decisions and investments based on greater certainty of upside and reduced severity of downside. That's how risk leaders can drive organizational value."**
>
> — Brian Hart, Principal, Advisory, U.S. Network Leader, Financial Services Risk, Regulatory, and Compliance

© 2024 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

06

Cost takeout

Reduce the overall costs associated with the governance, maintenance, oversight, and execution of risk requirements and practices

Key findings

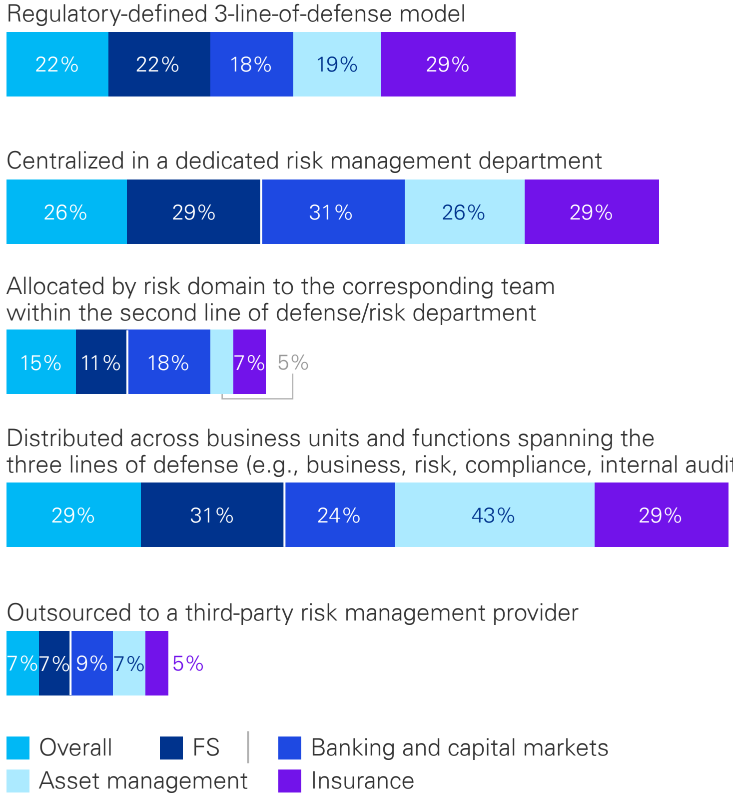
Managing costs while maintaining effective, regulatory-compliant programs is an ongoing challenge for FS risk management executives. Adding to the pressure is overall economic uncertainly and internal cost-cutting mandates, with risk functions increasingly expected to minimize costs and improve efficiencies.

Outsourcing of routine risk management activities is one alternative to this challenge. This includes traditional outsourcing as well as "risk as a service"—a form of managed services that leverage technology, talent, and resources from third parties to manage risk business activities.

The survey found that only 7 percent of FS respondents are outsourcing risk management to a third-party provider. That may be changing (Exhibit 6). Overall, 40 percent of FS respondents are considering outsourcing cybersecurity and threat protection services, while at a subsectoral level, INS respondents (43 percent) are more likely to outsource training and capacity building efforts for risk management personnel. Given the concern over cyber-attacks, it follows that organizations would take steps, including outsourcing, to bolster their protection from cyber threats.

Exhibit 6. Risk management organizational models

Q. How are risk management roles, responsibilities, and accountabilities allocated across various business units and functions?



"Overall" includes all industries; "FS" combines B&CM, AM and INS

© 2024 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Recommendations

- Consider optimizing your risk management delivery model, including better geographic representations and offshoring. Outsource low-risk, repeatable activities.
- Weigh outsourcing and co-sourcing decisions against the process changes and additional resources required to maintain the required level of risk control and governance. Remember that core elements of risk management should never be outsourced as the risk is too great, and risk leaders must find a boundary where the organization can maintain quality without inadvertently creating new third-party risk.
- Streamline operations and identify areas where costs can be reduced without compromising service quality or regulatory compliance, including things like redundant services delivered by risk and compliance organizations.
- Use third-party vendors to execute select risk management oversight or execution activities as a key lever not only for cost takeout but also for other long-term outcomes, such as growth, speed, and enhanced reputation. This can be especially important in complicated, high-risk areas with significant stakeholder attention, such as compliance, cybersecurity, and financial crime, where many risk organizations lack methodologies, technology, skills, or scalability

"Modern managed services are very different from traditional outsourcing models based on labor arbitrage for transactional work. Today's leading providers are strategic collaborators. They combine advanced tech, data management, and sector expertise to deliver critical risk processes, such as cybersecurity and regulatory compliance, with outcomes like stakeholder trust, customer retention, and resilience. They can also reduce total cost of operations by as much as 15 to 45 percent, without prohibitive upfront capital investments."

— David Brown, Principal, Advisory, Global Head, Managed Services

© 2024 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

How KPMG can help

KPMG Risk Services brings the strategic vision and technical edge to help you earn the trust of your stakeholders. Our deep FS industry skills concentrated in risk, regulation, cyber, and ESG, and our time-tested change experience, combine to create one powerful capability.

KPMG teams can help you anticipate and balance risk to generate value and a competitive advantage across your enterprise. By incorporating a detailed approach to risk, compliance, cyber, and ESG, we can help you identify new opportunities.

We are obsessively focused on the delivery of your strategy, your priorities, and your agenda. Using tools and solutions that accelerate your modernization journey and balance risk, we then apply deep domain knowledge across the spectrum of risk and regulatory issues, along with our skills in risk, technology, and consulting, to help drive borderless collaboration to convert the opportunities of risk into a sustainable competitive advantage for your organization.

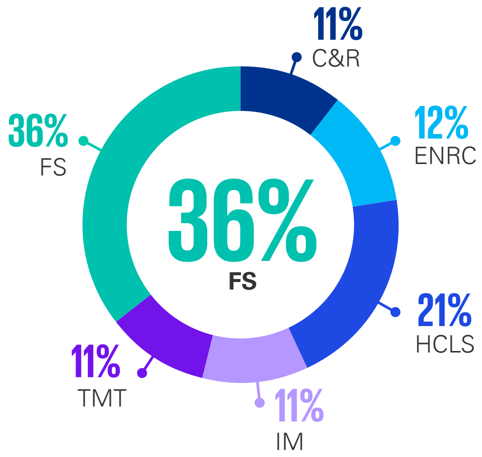
Learn more: visit.kpmg.us/RiskServices

© 2024 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

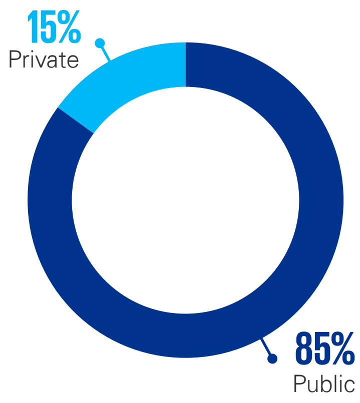
Research methodology

From July to September 2023, KPMG conducted an online survey of 390 enterprise risk officers representing U.S. organizations across six industry sectors with at least $4 billion in annual sales or $25 billion in assets under management (AUM). One-hundred and thirty-nine respondents participated from the FS sectors. Our research is designed to track trends in enterprise risk management and provide an outlook on the future of the enterprise risk function. Survey questions explore risk officer views on current and expected trends in the following areas: Risks and readiness, activities and investments, roles and approaches, and maturity and modernization.

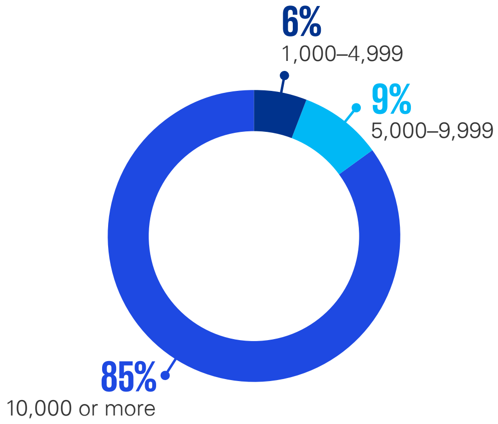
Organizational sector



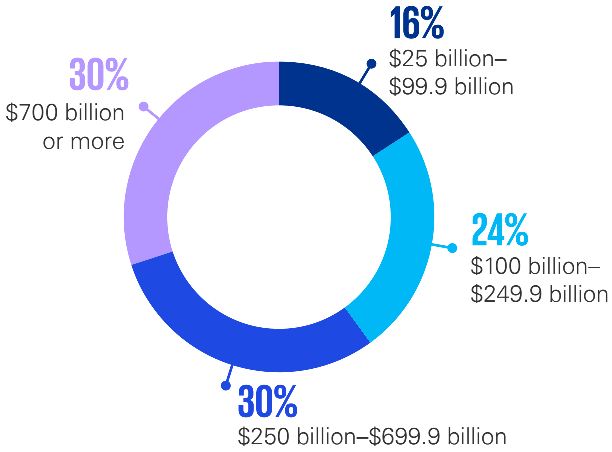
Organization type



Full-time employees in the company (Globally)



Size of company's assets under management
(FS respondents only)



Of the 390 enterprise risk officers responding to the survey, 139 respondents (36%) participated from the FS sectors.

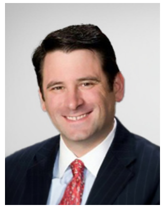
Notes: N=390; Single select; Percentages may not total 100 due to rounding.

© 2024 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

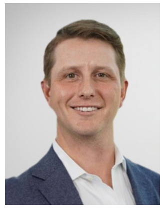
Authors

Anand Desai
Principal, Advisory
Financial Services Line of Business Leader, Risk Services
ananddesai@kpmg.com

Rob Fisher
Partner, Advisory
Consulting Financial Services Line of Business Leader, U.S.
rpfisher@kpmg.com



Brian Hart
Principal, Advisory
U.S. Network Leader, Financial Services Risk, Regulatory, and Compliance
bhart@kpmg.com



Cameron Burke
Principal, Advisory
Financial Services Risk, Regulatory, and Compliance
cburke@kpmg.com

Joey Gyengo
Principal, Advisory, and U.S. Enterprise Risk Management Solution Lead
jgyengo@kpmg.com

KPMG is recognized as a leader in risk consulting

Financial risk

Third party assurance

Client advocacy in risk*

KPMG ranked No. 1 across multiple risk categories in Source's report, *Perceptions of Risk Firms in 2023.*

The Source study, *Perceptions of Risk Firms 2023*, is based on a U.S. client and prospect perception survey about risk consulting firms, led by Source. It reveals what 300 senior users in the U.S. think about the 16 leading risk advisory firms and examines how clients see firms differently as they move from awareness, to shortlisting a firm, to becoming a direct client. The report is intended to help in understanding each firm's positioning in the market and the overall competitive landscape in which they operate. For more information please visit: https://www.sourceglobalresearch.com/

*Advocacy score is based on the percentage of KPMG client respondents that say they would use the firm again and would put their personal reputation on the line for the firm.

visit.kpmg.us/SourceRankings

01
02
03
04
05
06
07
08

© 2024 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

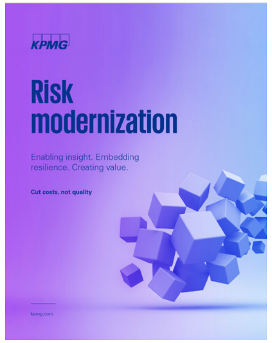
Related thought leadership

Read the full report: read.kpmg.us/CROSurvey

2023 Chief Risk Officer Survey

Ten Key Regulatory Challenges of 2024

Read all four articles: Risk modernization



Cut costs, not quality

Unlocking the potential of digital acceleration in risk management

Implementing a modern technology architecture to accelerate risk transformation

New ways of working in Risk – Modernizing the risk delivery model

Subscribe to receive Risk and Cyber insights

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Please visit us:

kpmg.com | **Subscribe**

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2024 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

DASD-2024-15184