Risk in review
Managing risk from the ***front line***

6th Annual Study
April 2017

Table of contents

The heart of the matter 4

Front-line leadership, collaborative success

Who are the Front Liners?

An in-depth discussion 9

Trending: A business-led approach for effectiveness and growth

How Front Liners lead

The financial rewards of front-line leadership

Embedded, collaborative risk management benefits all lines of defence

The importance of strong risk culture

Where risk management has improved—and where it hasn’t

CROs seek more-strategic roles

Cyber risk maturity

Case study
MUFG case study: Global growth brings greater requirements

Risk culture maturity

Measuring risk management maturity

What this means for your business 26

Building an optimised risk management ecosystem

Calls to action

Putting the C-suite to work

Risk in review 2017: Research methodology

For this sixth annual *Risk in review* study, PwC conducted a global survey in the closing months of 2016, netting responses from 1,581 corporate officers across 30 industries and spanning over 80 countries.

Respondents were board members, C-level executives, and their direct reports. Corporate titles most heavily represented were chief risk officer (CRO), chief audit executive (CAE)/ general auditor or direct report, chief financial officer, audit committee chair or member, and CEO or other board member. Participation by C-level executives was up sharply over our 2016 survey, with both CEOs and CROs seeing a 31% spike. (*Note:* Corporate titles account for variants: e.g., CAE/general auditor, CRO/head of risk management, etc.)

To help bring our findings to life, we mined insights from internal PwC leaders, Oxford Economics, and also conducted one-on-one interviews with executives from select companies across industry sectors.

Respondent organisations headquartered in North America made up 34% of our sample universe, followed by organisations based in Europe (33%), Asia Pacific (19%), Latin America (7%), and the Middle East and Africa (7%).

For the purposes of the study, we divided respondents into six broad sector groups: Consumer and Industrial Products and Services (CIPS), representing 40% of respondents; Financial Services (33%); Technology, Information, Communications, and Entertainment and Media (11%); Healthcare (8%); Government and Public Sector (4%); and Education and Not-for-Profit (2%). Respondents in other sectors accounted for 2%.

Thank you to all who contributed to this year's study.

The heart of the matter

Front-line leadership, collaborative success

It’s been almost a decade since the 2008 global financial crisis and its aftermath forced companies into a defensive risk management posture, pulling responsibilities back from the business units to the second line of defence as they fought to weather the storm.

But faced with the new challenges of today’s complex business risk environment, companies are seeing the tide shifting once again. Today a collaborative approach to risk management with risk accountability sitting squarely in the first line of defence can be the key to greater organisational resiliency and growth. That means an engaged first line that makes risk decisions in alignment with strategy. It means a proactive second line that influences decision making through effective challenge and timely consultation and collaboration. And it means a diligent, independent third line focused on its core missions of protecting the organisation and delivering value.

Analysed year on year, our survey data shows a clear trend towards business unit and corporate executives' taking the lead role by aligning ownership of key business risks with ownership of risk decision making.

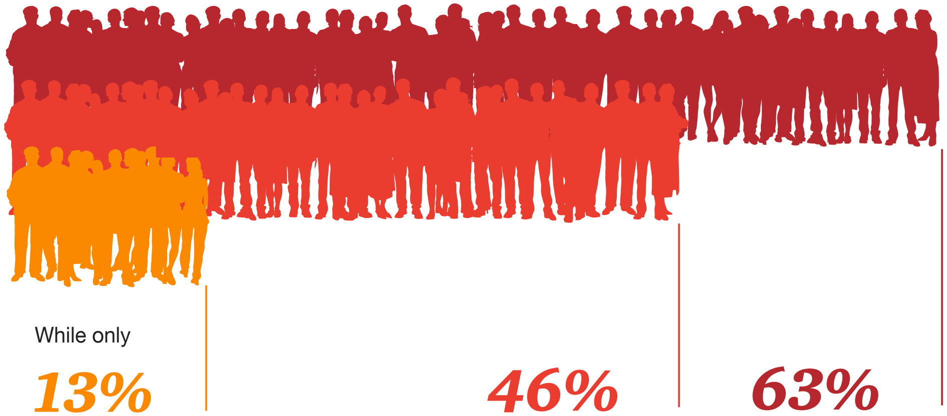
In all, nearly two-thirds (63%) of our respondents said shifting more risk management responsibilities to the first line makes their companies more agile—that is, better at anticipating and mitigating risk events—and 46% have plans to further this shift within the next three years.

But one group of respondents, which we've termed **Front Liners**, is far ahead of the pack.

These companies, which represent about 13% of our survey sample, are significantly more likely to say risk management decisions are owned and managed by the first line of defence. They express confidence that the first line is effective in managing most risk areas, and they back up that confidence with proven methods for effective risk management and formal second and third lines of defence.

These strengths beget strengths: Compared with overall respondents, Front Liners are more likely to expect revenue and profit margin growth in the next two years. And although no less prone to disruption than other companies, Front Liners are quicker to bounce back from adverse risk events and related disruptions. That's because they enable each of their lines of defence to concentrate on their specific areas, thereby enabling them to be more agile and focused during challenging times.

Respondents agree: Front line decision making is ideal



While only

13% currently lead risk decision making and collaboration from the front line ("Front Liners")

46% plan to move more risk management responsibility to the front line within the next 3 years, and

63% agree that moving risk decision making to the front line makes them better at anticipating and mitigating risk

A risk management ecosystem led from the front line, that fosters collaboration and shared accountability across all three lines of defence, positions a company to effectively meet the challenges of today's risk landscape. To get there, a company should:

Set a strong organisational tone focused on risk culture
that starts with the board and CEO and permeates the entire organisation

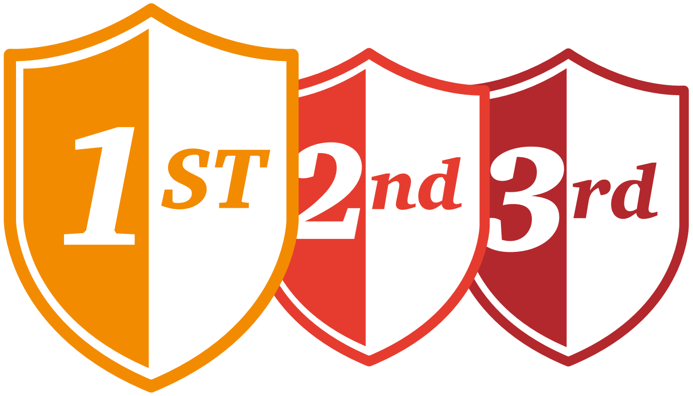
Align risk management with strategy at the point of decision making
so the first line anticipates business risks when setting tactical priorities

Recalibrate the risk management programme across the three lines of defence
with the first line owning business risk decision making, the second line monitoring the first, and the third line providing objective oversight

Implement a clearly defined risk appetite framework
across the organisation

Develop risk reporting
that enables executive management and the board to effectively execute their risk oversight responsibilities

Rather than representing a *threat* to the risk management, compliance, and audit functions, the shift of certain risk management activities to the first line represents an *opportunity*. By aligning all lines of defence within a collaborative, strategic framework, business-led risk management enables the second and third lines to become true partners in creating value for the enterprise.



Senior management and business units

Risk and compliance functions

Internal audit

Who are the Front Liners?

The 13% of surveyed companies that make up our Front Liner group share common strengths, as demonstrated by their responses to our survey. Front Liner respondents:

1. Agreed or strongly agreed that their business units (i.e. the first line of defence) have adequate authority, resources, and executive-level support to manage risks effectively

2. Agreed or strongly agreed that moving certain risk management responsibilities to the first line makes their companies better at anticipating and mitigating negative risk events

3. Currently manage risk decisions at the front line for at least 6 of 12 surveyed risk areas

4. Are more likely than overall respondents to have a defined and well-communicated risk appetite framework and to make key risk management decisions within that framework

5. Are more likely to budget adequately for risk management, utilize technology to aggregate risk across the organisation, create a strong risk culture that embeds risk management in day-to-day operations, and exhibit strong strategic partnership between the three lines of defence

Front Liner CROs are also significantly more likely to say that their companies view the risk management programme as a catalyst for growth rather than an impediment and that their independent risk and compliance functions provide proactive, strategic guidance for their companies' business units.

Companies in the Consumer and Industrial Products and Services represent 41% of total respondents and 40% of our Front Liner Group. Financial Services respondents represent 29% of total respondents and 33% of our Front Liner Group, so comparatively are more likely to be Front Liners.

While it may be expected that Financial Services companies represent many of our Front Liners, Consumer and Industrial Products and Services companies may not be quite as expected, yet there are reasons they may be inching up the risk management maturing curve:

They are shifting more responsibility for risk management to the first line of defence today

Consumer and Industrial Products and Services companies are more likely to manage operational risk from the first line

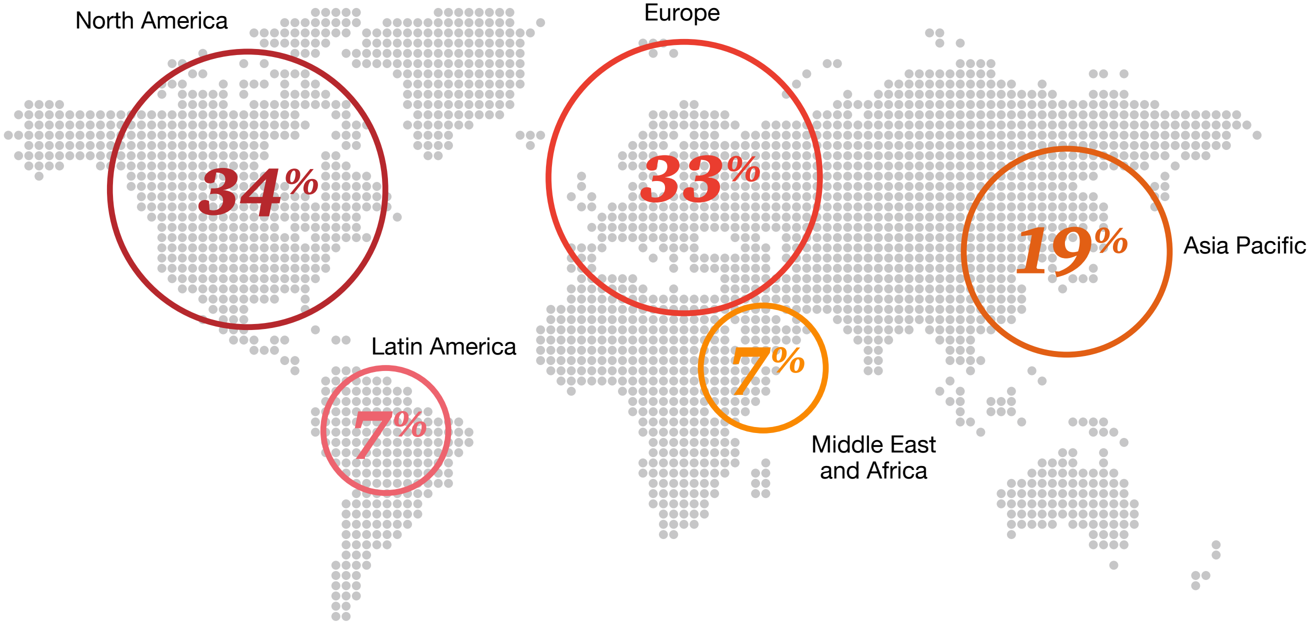
And, of Consumer and Industrial Products and Services companies that have experienced an operational disruption, 53% say they dealt with it effectively, vs. 46% of total

Front Liners by industry and region

By industry:

40%	33%	11%	8%	4%	2%
Consumer and Industrial Products and Services	Financial Services	Technology, Information, Communications, and Entertainment and Media	Healthcare	Government	Education

By region:



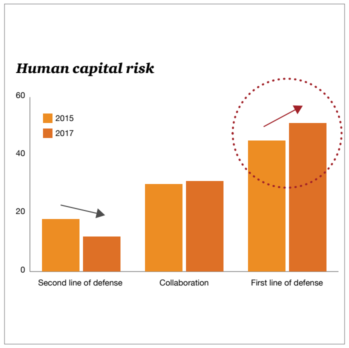
An in-depth discussion

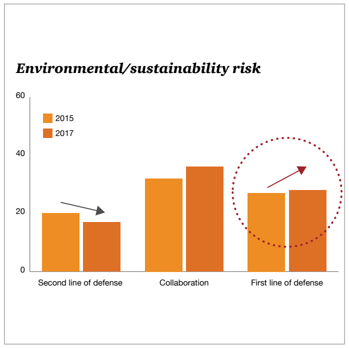
Trending: A business-led approach for effectiveness and growth

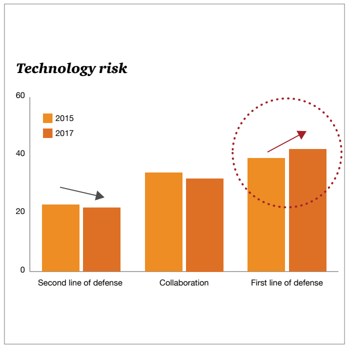
When the first line is in the driver's seat for risk decision making, companies report a more rigorous approach to determining risk appetite and tolerance, along with better overall risk management effectiveness—and they're more likely to expect revenue and profit growth.

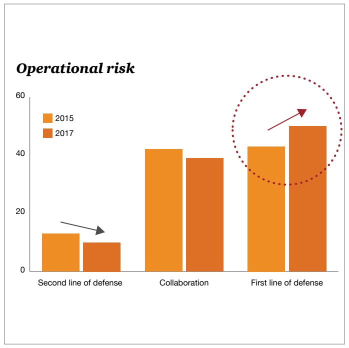
The trend towards first-line ownership of risk decision making is already well established, with all of our respondents reporting that their various risks are owned and managed either solely by the first-line business units or collaboratively between the business units and the second-line risk and compliance functions.

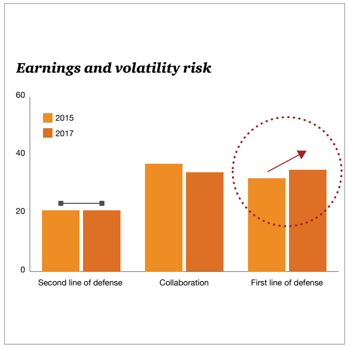
Statistical history shows the move: In comparing *Risk in review* survey results from 2017 and 2015, we see ownership and management of risk by the second line of defence either flat or trending downward across 8 of the 11 risk areas we surveyed in both years. Meanwhile, ownership and management of risk by the first line trended upward in 5 of 11 areas.

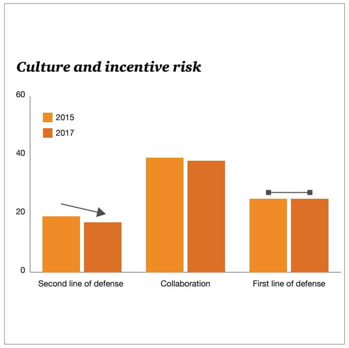

Human capital risk

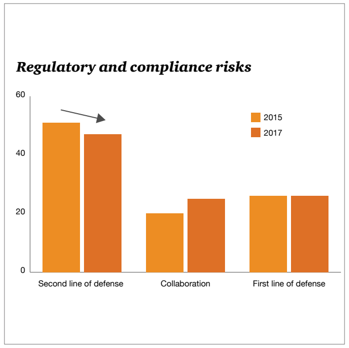

Environmental/sustainability risk

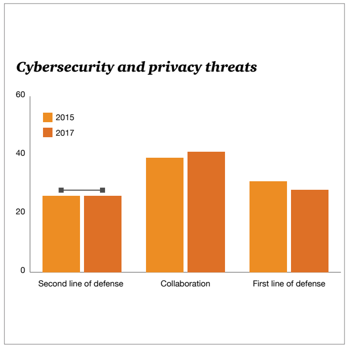

Technology risk

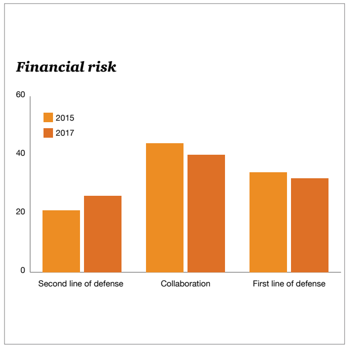

Operational risk

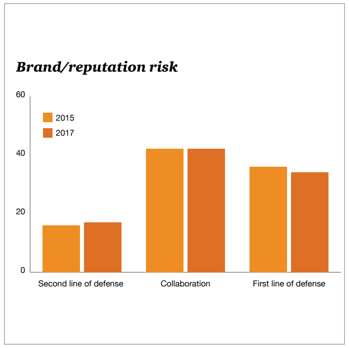

Earnings and volatility risk

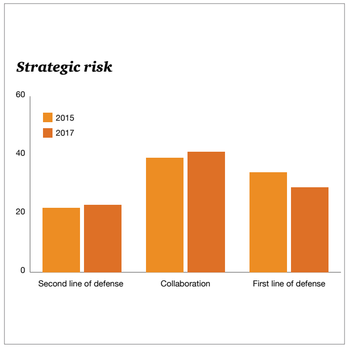

Culture and incentive risk


Regulatory and compliance risks


Cybersecurity and privacy threats


Financial risk


Brand/reputation risk


Strategic risk

This shift is timely. For more than a decade, many companies' risk management efforts functioned primarily as compliance exercises aligned with the requirements of the Sarbanes–Oxley (SOX) and Dodd–Frank acts. Those efforts naturally elevated the positions of chief risk and compliance officers and audit leaders in the overall risk management hierarchy. But after more than nearly 15 years of SOX experience and with the financial crisis of 2007–09 receding further in the rearview mirror, companies are evolving their risk efforts to meet the needs of their current environments.

In PwC's recent, 20th Annual Global CEO Survey, respondent chief executives from across industries named uncertain economic growth, overregulation, availability of key skills, geopolitical uncertainty, and speed of technological change as the top threats their businesses face. Add the clear and present danger of cyberattacks, changing customer behaviours, and social instability, and you have a landscape in which the first-line owners of risk must also take the lead in managing that risk.

> Melissa Lea, SAP AG chief global compliance officer, says that at her organisation, that direct connection is paramount. "We're very first-line heavy. The more we can get risk responsibility out into the field—first into management's hands and then to employees to make sure they're armed with the right expectations to make the right decisions—the more successful we'll be. We try to get people—either on the ground, in-country, or with the best lines of sight into how a particular risk might materialise—to really own that mitigation approach."

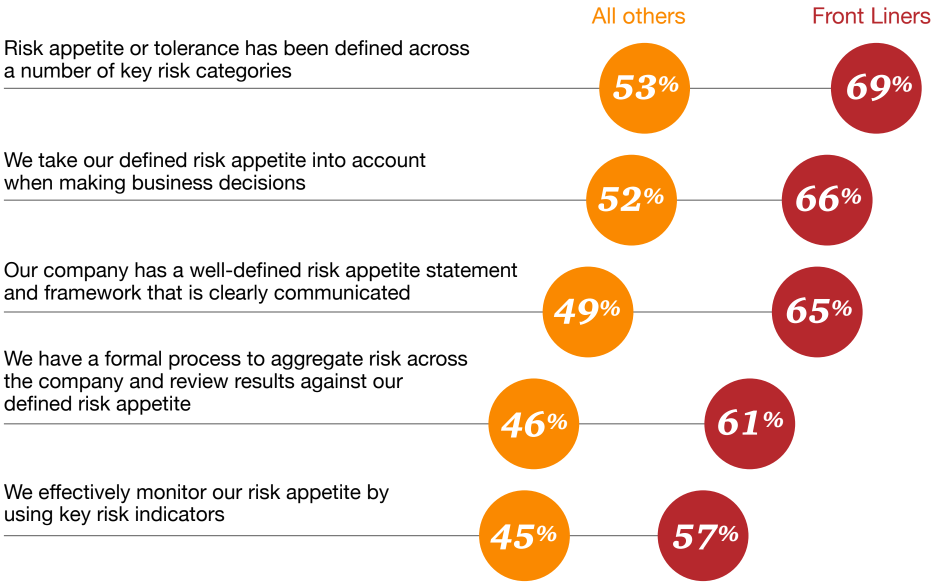
Effective risk management execution requires buy-in across the organisation, with the first line ensuring that risk management aligns with strategy and that the second and third lines of defence get the resources they need to support risk management throughout the company. Survey results from our leading Front Liner companies indicate that type of business-led approach supports more-effective risk management and more-robust revenue and profit margin growth.

How Front Liners lead

Our Front Liner companies are more likely than respondents overall to take a rigorous approach to risk management by leveraging a clearly defined risk appetite and leading practices.

Across five different types of risk management best practices, Front Liners lead other respondents by at least 12 percentage points.

Front Liners take a more rigorous approach to risk management



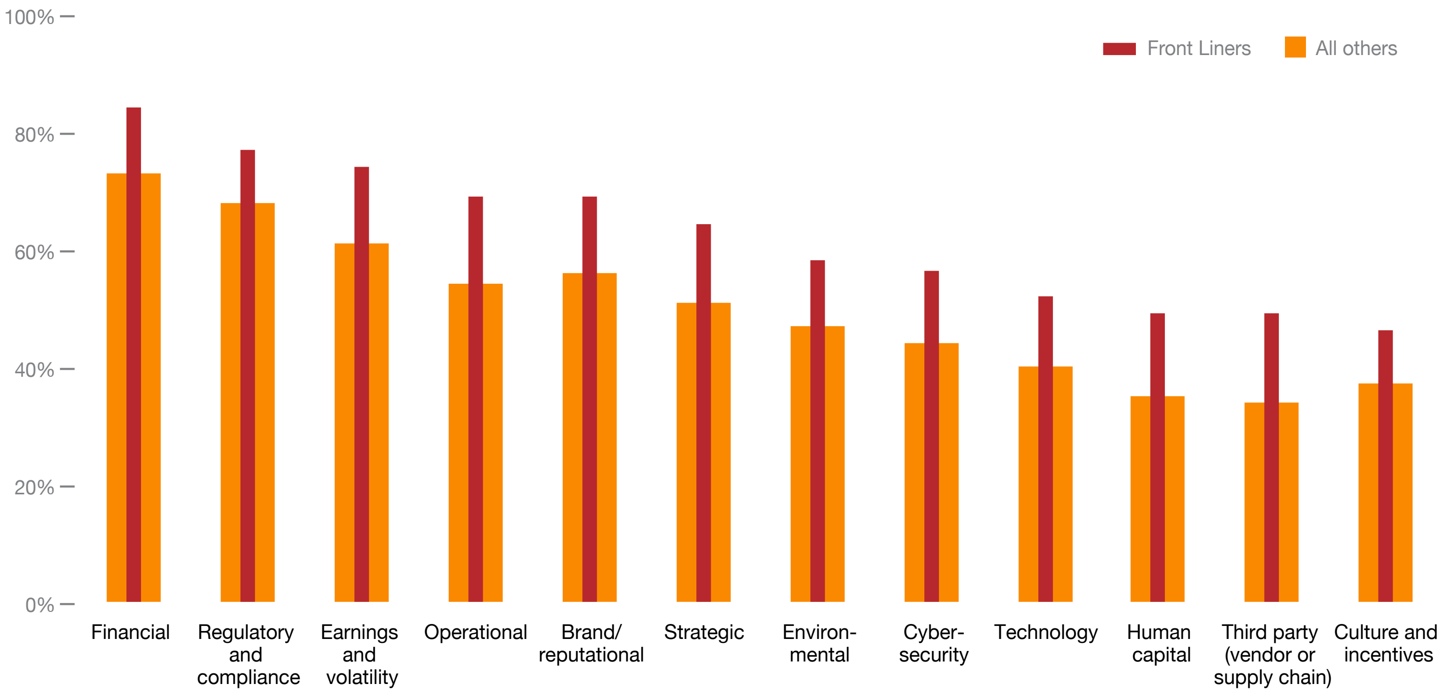
> “The first line represents our risk takers,” says Steve Gruppo, senior executive vice president and chief risk officer at TIAA. “They own the risk and understand our risk appetite. The second line then advises and challenges our business partners and helps them implement our risk programmes, managing both enterprise risks and business unit-specific risks to that appetite.”

As a group, Front Liners are also more likely than other respondents to say they manage effectively across all 12 areas of risk that we surveyed. In some risk areas, the differences are stark.

Front Liners' responses on the topic of past risk events suggest their confidence is based on records of success: A significantly larger percentage of Front Liners reported having addressed negative risk events. This held true across all 12 causes of business disruption that we surveyed.

Among companies that suffered disruptions caused by changes in business models or strategy, 66% of Front Liners reported recovering effectively versus 48% of other respondents. Among companies disrupted by operational risk, 63% of Front Liners reported effective recovery compared with 46% of non–Front Liners. And among companies that suffered business disruptions caused by geopolitical upheaval, 56% of Front Liners said their companies recovered effectively versus 39% of other respondents.

Front Liners manage risks more effectively



The financial rewards of front-line leadership

The connection between effective, strategically aligned risk management and better financial performance has been evident in the results of our past *Risk in review* surveys, so it is not surprising that this year's results suggest that managing risk from the first line of defence translates to improved performance metrics.

Through its alignment of strategy, risk ownership, and decision making, a risk management programme led by the first line automatically becomes more strategic and proactive rather than protective and reactive, thereby contributing to strong revenue and profit growth, expanding market share, lower employee turnover, and greater ability to withstand disruption.

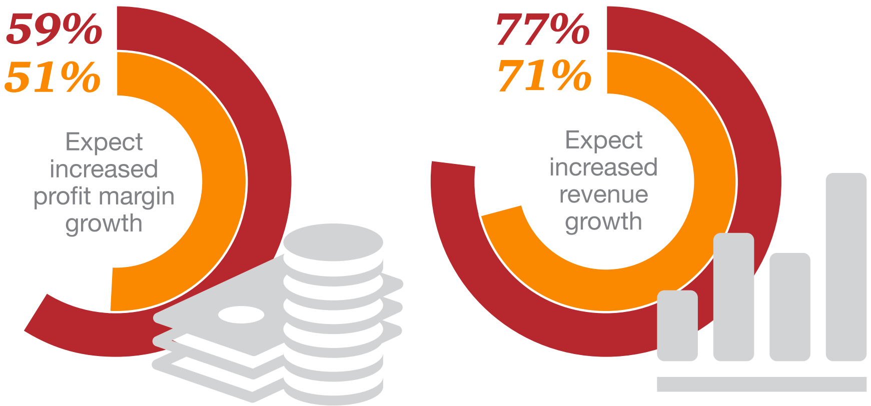
The bottom line: Front Liners are more likely than other survey respondents to expect growth in their revenues and profit margins during the next two years.

"We don't want to stop the risk-taking; we want smart, informed risk-taking that's done with eyes wide open, and within the overall risk appetite of the company. I use the racing car analogy, where the brakes are what actually give you the confidence to go faster. You accelerate on the straights and use the brakes when you're cornering, to stay in control. The net impact is a very high average speed compared to what you'd have if you had no brakes on the car at all."

—Nick Hirons, SVP for global ethics and compliance, GlaxoSmithKline

Front Liners report better performance metrics

In the next 2 years:



Embedded, collaborative risk management benefits all lines of defence

Effective first-line leadership of risk management does not mean minimisation of the role and impact of second-line risk management and compliance functions. Instead, it is a natural consequence of the drive to mainline risk awareness and responsibility throughout company culture and create an optimally effective risk ecosystem. Rather than managing risks in a vacuum, Front Liners push a collaborative approach that brings together all three lines of defence to execute risk management strategically and effectively.

Front Liners focus on developing a strong, organisation-wide risk culture that is led by example from the C-suite, board, and business unit leadership and is aligned with business strategy to enable faster, more-effective response to risk and disruption. In this type of structure:

First-line decision makers anticipate business risks, embed risk management in both strategic planning and tactical execution, and assign the right risks to be managed in the right places.

Second-line risk and compliance functions work collaboratively with the first line, providing checks and balances to optimise the risk management process.

Third-line internal audit provides objectively tests controls, and provides independent assurance, assessing first and second line risk activities.

"It's all about facilitation and partnering," says the general auditor and chief risk officer at a major U.S. corporation. "I am not a decision maker as it relates to enterprise risk management and risk acceptance; I'm a coordinator and a communicator, and my folks are dialed into the business. We identify concerns and validate those concerns. But at the end of the day, when I sit down to report to our CEO and senior risk committee, they're the ones making the decisions about risk acceptance. "You might not always agree in the first two, three, or four rounds, but ultimately, the question is, What's best for the organisation and the shareholders, and how does it affect our goals and objectives?"

The importance of strong risk culture

A mature risk culture operates on a commonly understood taxonomy for aggregating, tracking, and predicting risks, leveraging data analytics and other technologies for optimal coverage. Effective communication from the three lines of defence disseminates a broad baseline understanding of the organisation's risk appetite and tolerances, reinforced by continuous monitoring and a system of risk-related performance incentives.

> "We have a structured process for developing and communicating our risk appetite, which includes board engagement and board approval of risk appetite statements—both at the Enterprise level and one for each of our three major lines of business," says TIAA's Steve Gruppo. "At a high level, that includes a qualitative statement focused on attitudes towards risk, as well as a quantitative set of metrics."

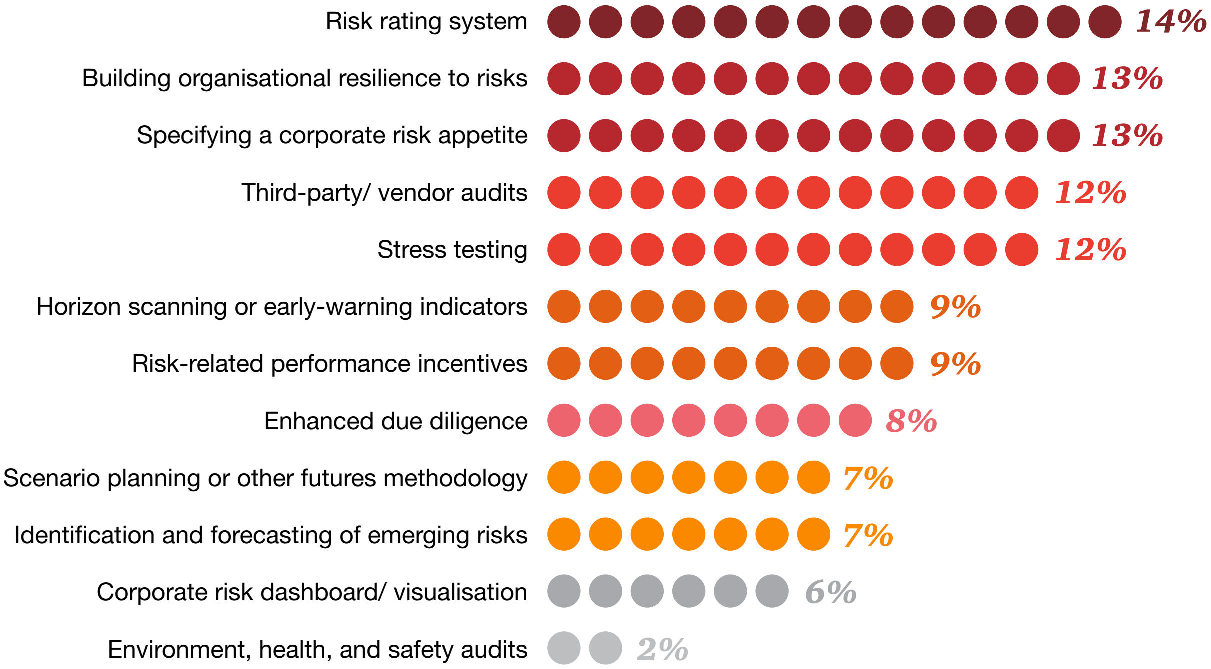
Front Liners lead other companies on measures that define a strong, organisation-wide risk culture by:

- Communicating proactively with external stakeholders following a negative risk event (49% vs. 37%)
- Making ethics and compliance training mandatory for all employees (80% vs. 71%)
- Having one or more board-level risk committees that ensure top-down and bottom-up approaches to risk management (64% vs. 54%)
- Encouraging a culture in which the second line of defence can effectively challenge and enable the first line (55% vs. 45%)

The acquisition and use of leading risk management tools and techniques are also key to maintaining a sound risk culture, and on that measure, Front Liners outpace other respondents by wide margins.

Front Liners more likely to use risk management tools and techniques

% Front Liners more likely to use versus all others



> “We view all the work we do as a continuous risk assessment process—including regular interactions with the business. If we have to go through a huge separate process, it means we aren’t staying close enough to the business.”
>
> *—Doug Watt, senior vice president and chief audit executive, Fannie Mae*

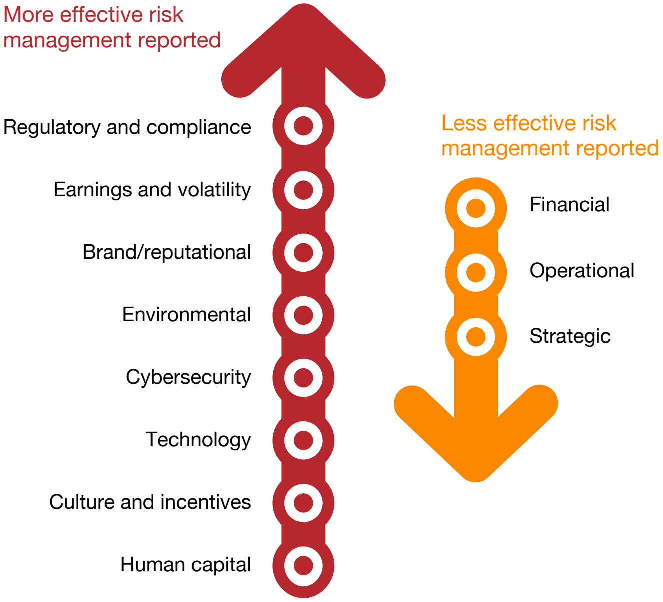
Where risk management has improved—and where it hasn't

A comparison of data from our 2015 and 2017 surveys shows an overall trend towards more-effective management of most business risks as well as towards greater use of strategic risk management practices. However, stats have dropped slightly or remained flat for management of certain risk areas.

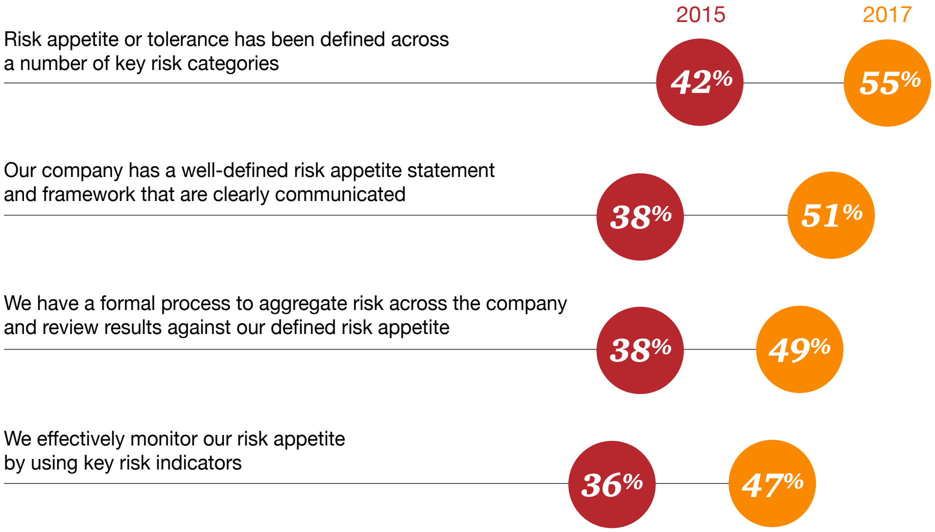
Respondents reported their biggest risk management improvements in the areas of environmental and cybersecurity risk. Meanwhile, respondents reported slight dips in the effectiveness of their responses to financial risk, operational risk, and strategic risk.

The past two years also saw gains across our full sample in the use of certain approaches to risk appetite and tolerance, which supports the strategic shift of risk management towards the first line of defence.

Incremental progress in managing risk effectively, 2017 vs. 2015



Improvement in approaches to risk appetite

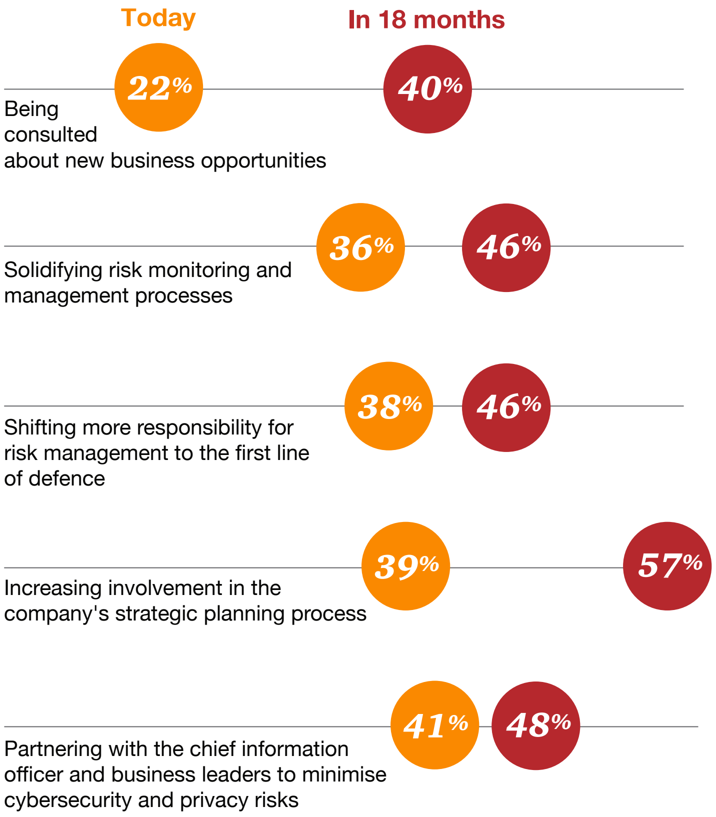


CROs seek more-strategic roles

Even as companies are shifting risk management decision making towards corporate leadership and the business units, chief risk officers (CROs) are aiming to make their roles and functions more strategic. Though only 39% of CROs named increasing their involvement in strategic planning as a current priority, that number jumps to 57% for CROs' priorities for the next 18 months.

In an ecosystem that integrates risk management into first-line decision making, risk and compliance functions have to see the big picture by understanding broad operational processes from strategic, operational, and financial perspectives. By doing so, they amplify their value as key partners in the risk-focused culture.

CROs report progress in managing risks effectively



Also, compared with 2016 results, significantly more CROs say their senior leaders understand the value of strong risk management (72% vs. 58%) and that the second line of defence is seen as a catalyst for growth (43% vs. 36%).

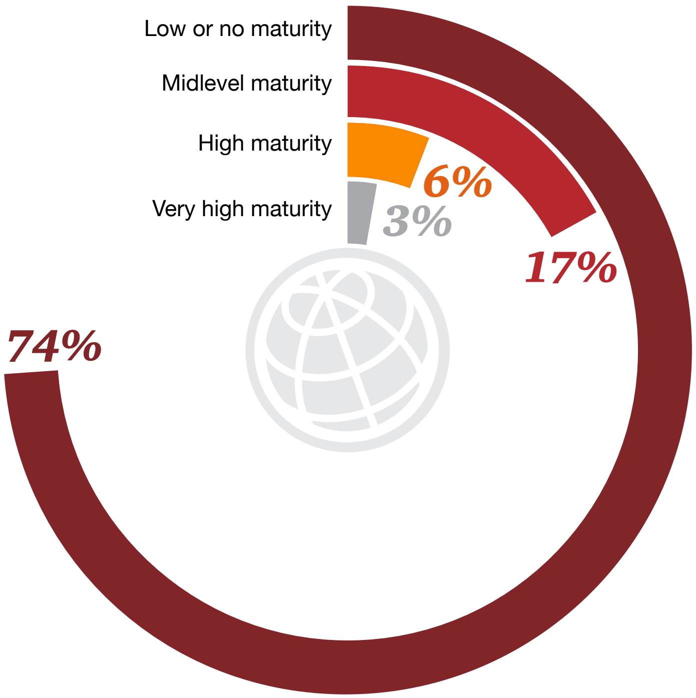
Cyber risk maturity

As digital platforms have become stalking grounds for ever more-cunning cybercriminals, awareness of cyber risk has reached critical mass. In our recent, 20th Annual global CEO survey, more than half of global CEOs (53%) said they expect cybersecurity and data privacy breaches to threaten stakeholder trust in their industries during the next five years. In the United States, 85% of CEO respondents said they're somewhat or extremely concerned about cyber crime's threat to their organisations' growth prospects.

Cybercrime and data privacy risks now have the potential to affect every aspect of a company's operations, and that threat becomes only greater as industries expand their interfaces with the Internet of Things and other emergent technologies. To study organisations that excel at managing cyber risk and to determine how well our survey respondents are positioned for the new cybersecurity reality, we created a cyber risk management maturity curve. Within our full sample population, the highest-maturity respondents reported all four of the following practices:

1. The chief risk officer and chief information officer (CIO)/chief technology officer (CTO) are jointly responsible for overseeing cybersecurity and privacy risk.
2. Cybersecurity and privacy risk are managed by the CIO/CTO.
3. The CIO/CTO works with each individual business unit and function to safeguard data.
4. The company has a cross-functional cybersecurity/information risk committee.

Cyber risk management maturity, all respondents



Across sectors, all of our survey respondents expect cyber risk to cause significantly more corporate disruption in the years ahead. In the face of this new normal, companies with highly developed cyber risk management practices will enjoy a clear competitive advantage.

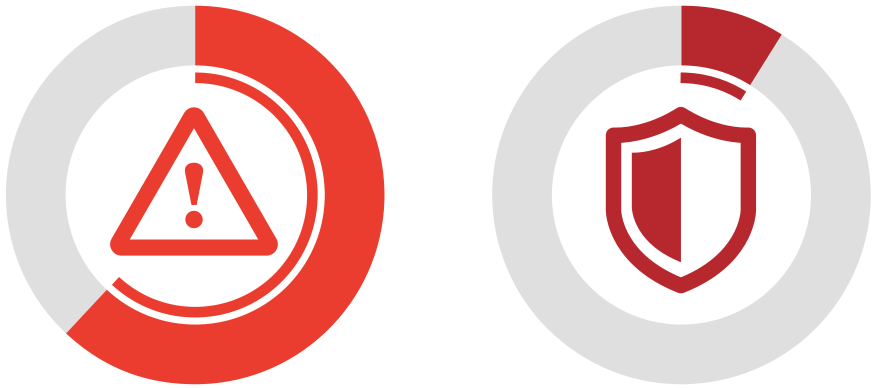
Few companies demonstrate high cyber risk maturity today, even though they expect cyber risk to grow dramatically in the next three years.

Only 3% of our 1,581 respondents scored very high in cyber risk maturity, whereas 6% scored high and 17% scored at the midlevel. Remarkably, two-thirds of respondents (66%) scored in the low-maturity bracket (e.g., satisfying only one of the four maturity criteria), and 8% scored as having no cyber risk management maturity. Yet cybersecurity is one of the risk areas where respondents' claims of response effectiveness indicated the greatest improvement over past survey results. This suggests that even though companies are feeling more confident in their capabilities, they remain on a purely defensive footing against cyber risk and have not adopted leading practices that can help grow their competitive edges vis-à-vis cybersecurity and the market.

Many companies see cyber and privacy as top-growing risks, but few are prepared

62% expect cyber risk to cause disruption in the next 3 years

Yet only **9%** have high or very high cyber risk maturity



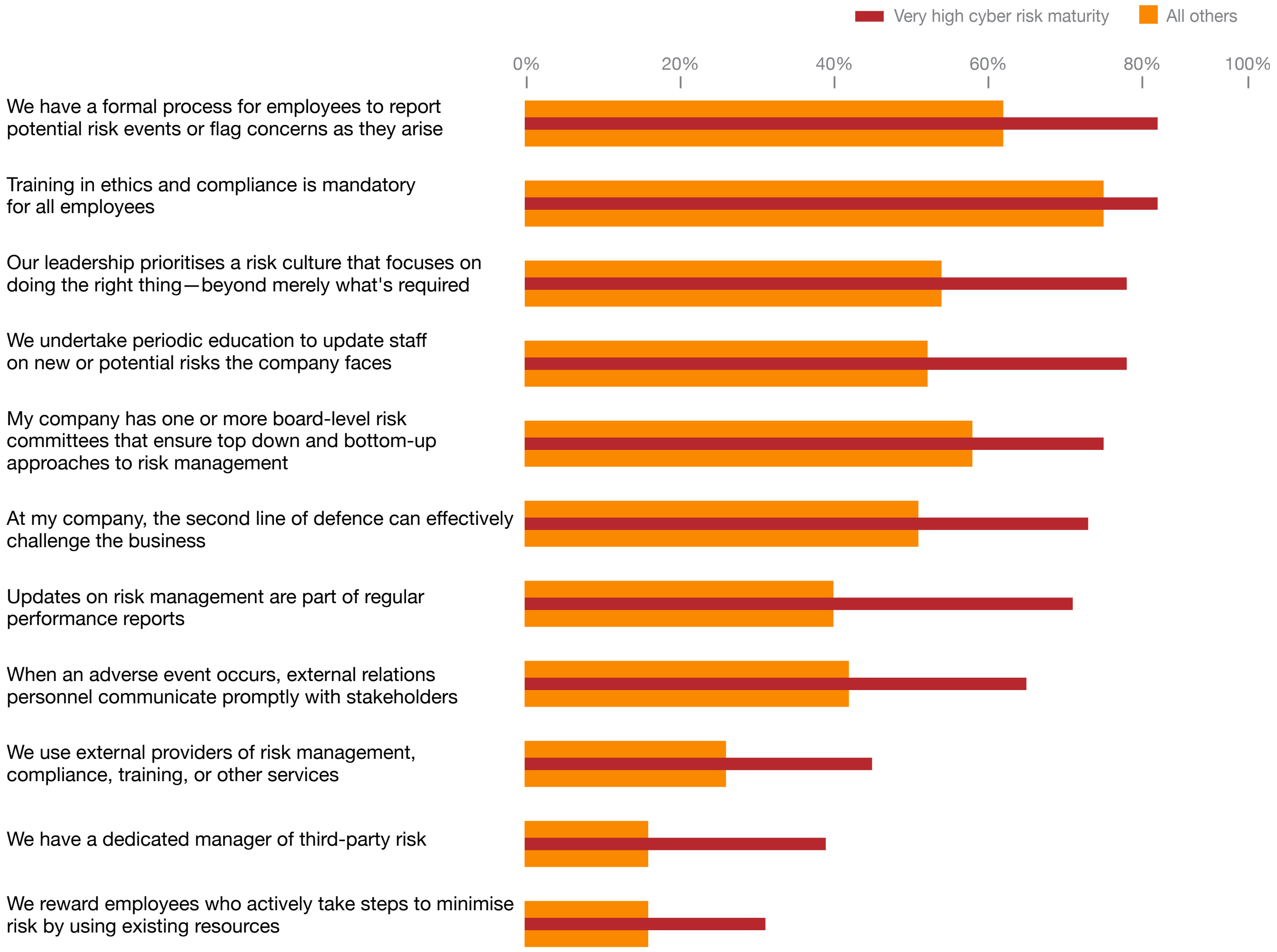
“You can't really address cyber or AML regionally anymore. If you're on a globally connected network, running global systems, the controls you have in place need to be set at the same high bar across shared environments; otherwise you will only be as strong as your weakest link.”

—Lisa Humbert, Managing Director, Chief Information Risk Officer, and Head of Information Risk Management, MUFG Union Bank, N.A.

Improving a company’s cyber risk management maturity appears to have benefits beyond the obvious. Our analysis shows that such maturity is an indicator of advanced risk management capabilities in other areas, with high-scoring companies reporting greater ability to manage strategic, operational, brand, regulatory, financial, and other key risks. On every measure of risk culture, high-scoring companies dramatically outpace respondents overall.

Mirroring our Front Liners’ higher growth expectations, respondents that use all four mature cyber risk management practices show a 63% expectation of profit margin growth during the next two years versus 50% of other respondents. Companies scoring highest on the curve are also somewhat more likely to anticipate revenue growth (75% vs. 71%).

Companies with high cyber risk maturity have better risk cultures



MUFG case study: Global growth brings greater requirements

In 2014, Mitsubishi UFJ Financial Group, Inc. (MUFG) integrated The Bank of Tokyo–Mitsubishi UFJ's (BTMU) U.S. branch banking operations with Union Bank, N.A. and began operating its combined U.S. banking operations under the new name MUFG Union Bank, N.A. The combined operations serve corporate and investment banking clients, commercial banking, wealth and consumer clients, and is committed to an ambitious growth strategy in the U.S. while staying true to MUFG's global vision to be the world's most trusted financial group.

Like other world-leading financial services firms, MUFG Union Bank, N.A. must comply with enhanced regulatory requirements. "Before we combined operations, we were not classified as a large financial institution," says Lisa Humbert, MUFG Union Bank's Managing Director, Chief Information Risk Officer, and Head of Information Risk Management (IRM). "Now we are, and with that comes greater regulatory focus and scrutiny, including increased attention to compliance with the Federal Reserve Board's Enhanced Prudential Standards, OCC's Heightened Standards, and augmented cyber regulations, to name a few."

Addressing these requirements involves driving change on many levels across the enterprise. As banks grow in size and complexity, they must evolve their risk management strategy and approach. This process involves establishing a formal IRM framework, which includes enhanced governance, a defined list of key information risks, threats, controls, procedures, metrics and reporting. Financial services firms must also establish a solid IRM management foundation, with clear roles and responsibilities, clear components and descriptions of how they function, a consistent taxonomy, and risk assessment methodology. IRM organizations work with enterprise risk governance and operational risk functions to ensure consistency across the different types of risks and threats managed by the bank.

"We knew we had to come out of the gate quickly to meet heightened regulatory requirements and sooner in some risk areas than others" says Humbert.

Global financial services firms like MUFG have had to adopt a Three Lines of Defense model. In this model, each line understands its role in managing risk, collaborating with the other lines to ensure effective, proactive and sustainable risk management. The businesses (Line 1) are responsible for managing risk within their areas and must evaluate risk factors as part of their decision-making process; Risk and Compliance, including IRM (Line 2), defines the enterprise's frameworks and reviews and challenges first line compliance with that framework; and Internal Audit (Line 3) provides independent assurance that processes and controls are being followed and appropriate risk management frameworks are in place.

"It's important that the businesses in Line 1 understand the information risk impacts of the decisions they make or that technology makes on their behalf because ultimately the risk impacts the businesses directly. When we talk about managing risks at MUFG, it is clear that we're all doing this together.

"If you're in the IT space, you have to ask, 'Ok, if there's a vulnerability within a critical environment and technology doesn't fix it, is that risk going to impact the IT department?' If the vulnerability is exploited, it's going to impact the business and potentially the company's reputation and much more. It's the business that is being put at risk. Applying an effective Three Lines of Defense model, we have the insights and the tools to understand this and move swiftly to address the risks we face, in partnership together," Humbert states. "Risk culture and awareness training is also required at all levels, from senior leaders to IT teams and employees across the organization, all of whom play a part in managing information risk," she says.

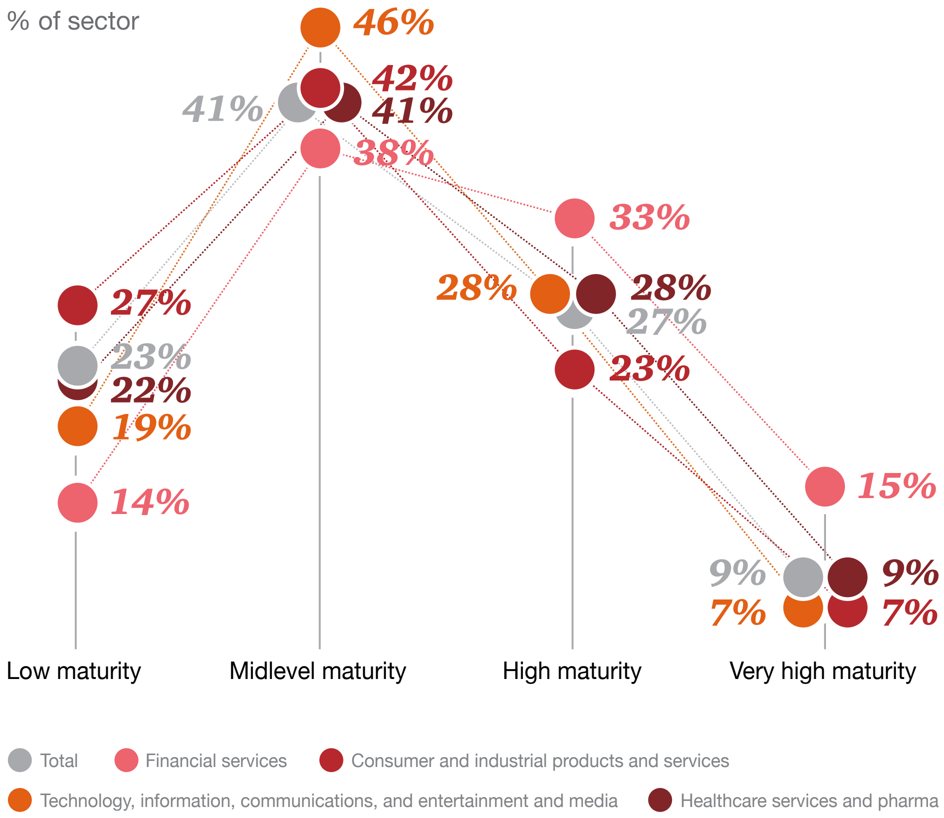
Risk culture maturity

In assessing risk culture maturity, we questioned companies about 11 practices that are hallmarks of highly developed risk cultures. To grade cultural maturity, we awarded respondents one point for each practice their organisation has in place. Low-maturity respondents scored 0–2 points, medium maturity 3–5 points, high maturity 6–8 points, and very high maturity 9–11 points. Financial services and healthcare organisations posted the highest overall scores.

Across most sectors, respondents were most likely to have in place mandatory training in ethics and compliance, with financial services (81%) and healthcare (79%) posting the highest positive-response rates. Other areas showing high buy-in across multiple sectors include having a formal process for employees to flag concerns or report potential risk events (led by financial services with 70% and healthcare with 66%) and having one or more board-level risk committees (led by financial services with 72% and healthcare with 56%).

Areas that lag across sectors include rewarding employees who use existing resources to minimise risk, wherein only one sector (healthcare) posted a positive response rate above 20%. Similarly, only financial services posted a response rate above 20% in having a dedicated manager of third-party risk.

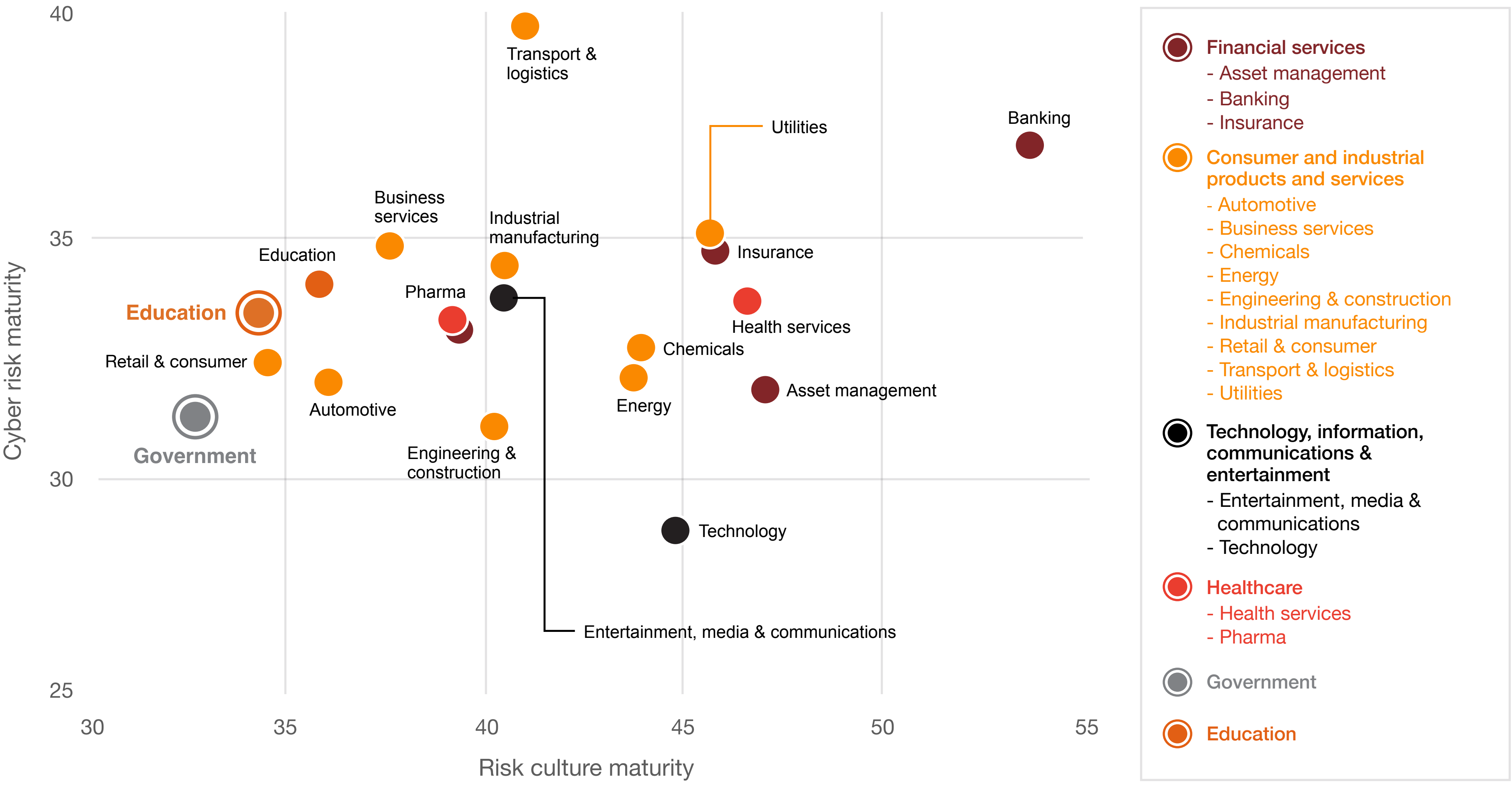
Risk culture maturity, major industry groups



Measuring risk management maturity

In examining industry sectors to determine their comparative risk maturities, we reached the expected result: The most-highly-regulated industries have the most-highly-evolved risk management practices. However, when we plotted the major industry sectors on maturity curves for cyber risk management and risk management culture, we found the relatively low cyber risk maturity across industries resulted in some potentially unexpected results, as shown on the next page.

Industries by risk culture and cyber risk maturity



What this means for your business

Building an optimised risk management ecosystem

First-line risk management leadership is all about engagement: placing responsibility for the various building blocks of an effective risk management programme—strategic alignment, expertise, processes, assurance—with the line of defence best prepared to execute them. Clarifying the function of each line of defence also frees those lines from undertaking tasks that properly rest elsewhere, and close collaboration between the lines promotes a free and welcomed flow of perspectives and ideas.

"Shifting risk responsibility back to the first line and moving the second line into the oversight role takes a great deal of collaboration, but it can be difficult to collaborate and provide effective challenge at the same time," says Kimberly H. Johnson, executive vice president and chief risk officer at Fannie Mae. "Risk management used to be a deep-in-the-numbers function, but now you also need to have emotional intelligence to be an effective risk manager. You need to be able to challenge ideas and assumptions without challenging the person and shutting down the discourse."

Calls to action

Shifting risk management activities to the first line of defence is only one part of moving towards a more proactive, strategically aligned risk management programme. Building a risk management ecosystem optimised for today's challenges requires buy-in across the enterprise. Here are five steps that can set your organisation on the right path.

1. Set a strong organisational tone focused on risk culture.

The CEO and the board should model this tone, which should permeate the organisation and be continually monitored and measured for effectiveness.

- CEOs should ensure performance management and incentives are aligned with their risk culture goals.
- Leadership team communications should foster clear and consistent messaging.
- Risk should be incorporated into routine conversations and decision making.

2. Align risk management with strategy at the point of decision-making.

- Having a clear view into the organisation's strategy gives the first line a common vision on which to align its decisions and behaviours, positioning it to react faster to risks and disruptions.
- Decision makers should embed risk management into both strategic planning and tactical execution.

3. Recalibrate the risk management programme across the three lines of defence.

For optimal performance, the first line owns business risk decision making, the second line monitors the first, and the third provides objective oversight.

- Defining boundaries and natural intersections clearly across the lines of defence enables the coordination of roles and responsibilities with maximum effectiveness.
- Leadership can then better define its risks, assign them to the different lines, and ensure that those risks are managed in the right places.
- Each line of defence must be enabled with the information and resources it needs to be effective.

4. Implement a clearly defined risk appetite and framework across the organisation.

- (a) Define risks the company is in business to take, (b) risks that cannot be tolerated, (c) which risks should be measured and monitored, (d) and which risks are associated with financial performance variances that could impede strategy achievement.
- A commonly understood risk taxonomy should govern the process of aggregating, tracking, and anticipating risks. And the process should leverage technology and data analytics when available.
- The risk appetite and framework must be clearly communicated to decision makers.

5. Develop risk reporting that enables executive management and the board to effectively execute their risk oversight responsibilities.

- Enhance data governance and data collection processes to support risk reporting efforts
- Risk aggregation, tracking, and reporting are critical to keeping business decisions within the agreed risk appetite/tolerance.
- Reporting and monitoring processes should routinely track risks and associated risk management activities.
- Owners should be assigned to top-tier enterprise risks and be required to provide detailed, time-bound risk action plans.

Putting the C-suite to work

When leaders drive risk management, they move beyond support to ownership

The **Chief Executive Officer (CEO)** must set the tone for a constructive risk culture, promote a coherent, organisation-wide risk appetite framework, and align risk management with strategic planning.

The **Chief Financial Officer (CFO)** should support calibration of risk management decision making by allocating resources to the lines of defence and to decision making points.

The **Chief Risk Officer (CRO)** enables effective risk management by promoting active monitoring, leading risk tolerance training, and coordinating with the CIO/CISO to manage cyberrisk organisation wide.

The **Chief Compliance Officer (CCO)** takes a leadership role in helping the organisation aggregate risk. CCOs are more likely than other titles to say they have a formal process for aggregating risk across the company and that they review results against a defined risk appetite (58% vs. 51% for CROs).

The **Chief Information Officer (CIO)**, who owns all the technology risk, equips the lines of defence with the necessary technology for predicting and monitoring risk. The **Chief Information Risk Officer (CIRO)** coordinates with the CRO to monitor cyber and data privacy risk.

The **Chief Audit Executive (CAE)**, as the last and objective line of defence against risk, must continually evaluate the risk management programme overall—including the CRO's effectiveness—"and independently assess first and second line risk activities.

The **Board of Directors** supports the CEO in setting a top-down risk culture and overseeing aggregated risk in the context of the organisation's risk appetite and risk tolerance framework.

pwc.com/riskinreview

To have a deeper conversation about how this subject may affect your business, please contact:

Dean Simone, Partner
Risk Assurance Leader—
US, Asia Pacific, and
Americas Cluster
dean.c.simone@pwc.com
+1 (267) 330 2070

Jason Pett, Partner
Internal Audit, Compliance and Risk
Management Solutions Leader
jason.pett@pwc.com
+1 (410) 659 3380

Scott Greenfield, Partner
Advanced Risk and Compliance
Analytics Solutions Leader
+1 (646) 471 5383

Todd Bialick, Partner
Trust and Transparency
Solutions Leader
todd.bialick@pwc.com
+1 (973) 236 4902

Brian Schwartz, Principal
Internal Audit, Compliance
and Risk Management
Financial Services Leader
brian.schwartz@pwc.com
+1 (202) 729 1627

Grant Waterfall, Partner
Global Cybersecurity and
Privacy Co-Leader
grant.waterfall@pwc.com
+1 (646) 471 7779

Jim Woods, Partner
Global Risk Assurance Leader
jim.woods@hk.pwc.com
+1 (852) 2289 2316

Neelam Sharma, Director
Advanced Risk and Compliance
Analytics Solutions
neelam.sharma@pwc.com
+1 (973) 236 4963