FORRESTER®

Constant Disruption Is The New Status Quo

How Early Awareness And Comprehensive Risk Strategies Mitigate Business Disruption And Manage Risk

A FORRESTER CONSULTING THOUGHT LEADERSHIP PAPER COMMISSIONED BY DATAMINR, SEPTEMBER 2022

Table of Contents

Project Team:
Nicholas Phelps,
Principal Market Impact Consultant

Ben Anderson,
Associate Market Impact Consultant

Contributing Research:
Forrester's Security & Risk research group

ABOUT FORRESTER CONSULTING

Forrester provides independent and objective research-based consulting to help leaders deliver key transformation outcomes. Fueled by our customer-obsessed research, Forrester's seasoned consultants partner with leaders to execute on their priorities using a unique engagement model that tailors to diverse needs and ensures lasting impact. For more information, visit forrester.com/consulting.

Executive Summary

Risk professionals must be ambidextrous to protect their business from risks to and from the enterprise, their ecosystem, and systemic risks, as well understand the impact of their decisions on customer experience (CX) and employee experience (EX), partners, and the brand's reputation. In response, many are developing comprehensive enterprise risk management (ERM) programs that help them better navigate risk and steer their businesses through a fast-changing world.

Dataminr commissioned Forrester Consulting to evaluate the state of ERM at enterprises in the US, EU, and APAC. Forrester conducted an online survey with 500 risk leaders at midsize to large enterprises across industries to explore this topic. We found that respondents' organizations encounter significant organizational, strategic, and technological barriers on their way to implementing effective ERM strategies. It's critical that organizations refine their ability to detect known and unknown risks, and decide which risks are worth taking in pursuit of strategic goals and objectives.

Key Findings

Many risk leaders are taking too narrow a view of the systemic risks their organizations face. Business risk will become more — not less — complicated to manage in the future, yet fewer than a third of risk leaders completely agreed that risks to their business can come from anywhere. However, so-called discrete risks represent systemic threats to firms with the potential to disrupt operations, CX, EX, and revenue recognition.

Risk strategies have made significant advancement during the past few years, but still have a long way to go. Just 36% of respondents' organizations have a C-suite champion leading risk management today. Progress towards shoring up risk exposure is hampered by a lack of participation and alignment with other business groups, poorly integrated technologies, and confusion around aligning risk monitoring with response effectiveness.

Cybersecurity and real-time alerting capabilities will be a major area of focus going forward. Respondents were most likely to cite cyber risk tools and real-time alerting capabilities as the most critical features their organization's next risk management platform must include.

Successful ERM implementations are driven by aligned leadership, vision, and technology. It's critical that firms empower leaders to work across the enterprise and better understand and avert the impacts of systemic risk on the business. As they do so, these leaders will require powerful, integrated technology that can improve program effectiveness and response times.

Business Resilience Requires Understanding The Dynamics Of Risk

The events of the past three years have wreaked havoc on even the best-laid business plans. These times have brought into focus how inadequate our collective ability to discover and manage major risk events can be in the face of rapid change. While global enterprises are adjusting to constant upheaval in business operations, the face of risk to businesses will continue to be defined by its dynamic, pervasive nature.[1]

Unfortunately, many risk management professionals take too narrow a view of the risks to their business. For example, just 31% of surveyed risk leaders completely agree that risks to their business can come from anywhere, yet the rise of digital business only opens up more opportunities for incidents to occur as more employees and third-party partners access critical business systems virtually, as climate risk increases the intensity and frequency of natural disasters, as cloud adoption grows, and as customer experience and customer expectations can make or break a brand.

Furthermore, 59% of respondents reported being concerned or highly concerned about 10 or more types of business risks today, while on average, they actively track or monitor just six categories.

RISK LEADERS MUST TACKLE PERVASIVE, SYSTEMIC RISK WITH COMPREHENSIVE STRATEGIES

As businesses become more digitally interconnected and globally dispersed, risks both diversify and deepen their potential for systemic disruption. These physical and virtual interconnections between the complex networks of partners, suppliers, employees, and customers mean the impact of seemingly isolated events like adverse weather, natural disasters, or ransomware attacks against a service provider isn't limited or contained at operational risk. Rather, they threaten systemic repercussions across all elements of the enterprise, including CX, brand reputation, regulatory penalties, and lost revenue.[2]

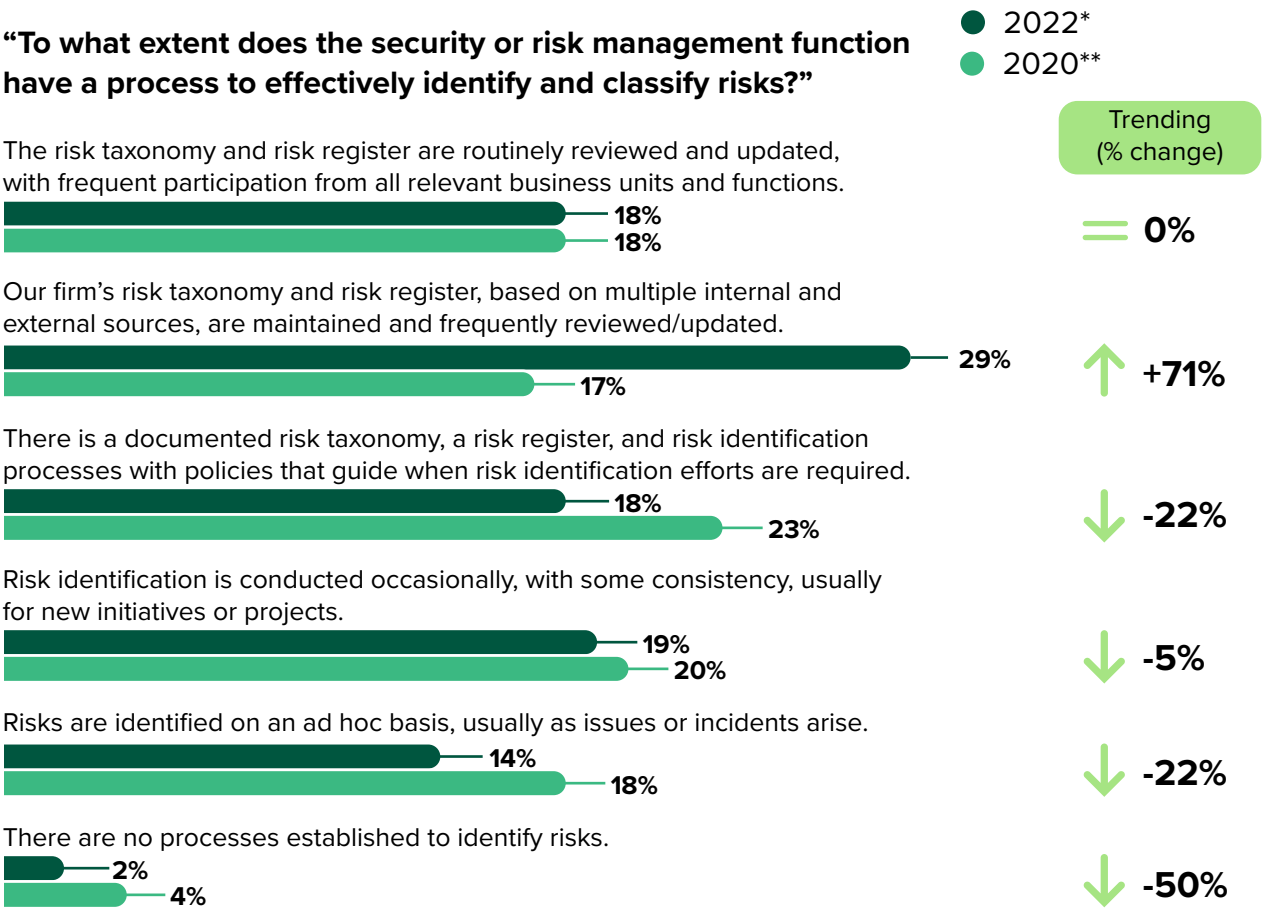
In short, there is no such thing as discrete risk. However, the leaders in our study struggle to respond to this reality with comprehensive strategies that recruit, engage, and empower stakeholders across the organization. Take for

example the programs leaders have built to identify and classify both known and unknown risks, which are critical capabilities for risk management that serve as the foundation for response.

Recently, leaders have shown real but limited progress in how they identify and categorize risk. Compared to two years ago, risk leaders are 71% more likely to describe their approach as centered around dynamic risk taxonomies and registers that leverage multiple internal and external sources to frequently review and update the risks their organization actively looks for. At the same time, the rates at which organizations say there are no processes in place to identify risks has dropped 50%, and approximately 20% fewer respondents say they rely on static or ad hoc processes compared to in 2020 (see Figure 1).

Figure 1

"To what extent does the security or risk management function have a process to effectively identify and classify risks?"



*Base: 500 decision-makers responsible for identifying and managing enterprise risk and responding to crises at their organization
Source: A commissioned study conducted by Forrester Consulting on behalf of Dataminr, April 2022
**Base: 410 risk and compliance decision-makers at organizations with $500M+ annual revenue in the US, UK, or ANZ
Source: A commissioned study conducted by Forrester Consulting on behalf of Dataminr, November 2020

While encouraging on its face, this data also exposes a larger problem with risk strategies: Leaders report that key aspects of their programs have hit a ceiling. During the past two years, it remains just as rare for respondents to say their organizations leverage updated risk taxonomies and registers, which are informed through participation from key business groups. This is the ceiling leaders have hit: They struggle to translate risk taxonomy input from stakeholders into ongoing, cross-functional, and integrated plans for monitoring and responding to the key risks their organizations face. As a result, they limit their organizations' abilities to understand and respond to risks as they occur.

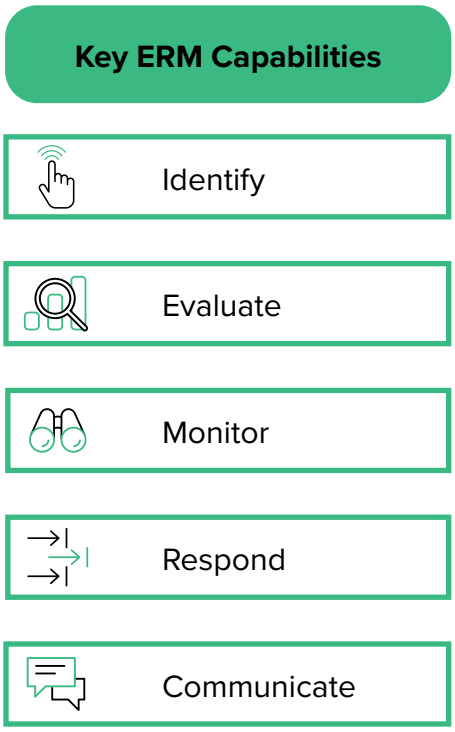
Just 18% of respondents said their organization takes this path today, while 52% agree that organizations with an integrated approach to identifying, evaluating, and responding to incidents will lead to reduced exposure and better outcomes. In other words, respondents are ready to become more comprehensive and effective risk managers, but they are struggling to break through. Forrester has previously discussed the importance of bringing systemic risk into the conversation risk leaders are having with key stakeholders across the enterprise, ideally to get a clearer picture of vulnerabilities and to ensure risk mitigation efforts are aligned to business goals in order to limit strategic risks down the road.[3]

Most Risk Management Strategies Rest On An Unfortified Foundation

To support growth, profitability, and resiliency, all organizations must have a robust risk management process, access to timely information and analysis, and support from the right technologies to help them make better, quicker strategic decisions.[4] Five competencies drive success in this space: the ability to identify, evaluate, monitor, respond, and communicate — and they enable firms to keep pace with the proliferation of business, ecosystem, and systemic risks they face (see Figure 2).

The risk leaders in this study lacked confidence in their current strategies to support their organizations' abilities to manage risk. Just 40% indicated their current strategies are effective or very effective across at least four of five capabilities. Even worse, only 18% reported having strategies that are effective or better across all five. Fundamentally, study data reveals that misalignment is most to blame, and it takes three primary forms: organizational misalignment, misaligned priorities and visibility, and technological misalignment.

Figure 2



Source: A commissioned study conducted by Forrester Consulting on behalf of Dataminr, April 2022

MISALIGNMENT BETWEEN RISK LEADERS AND BUSINESS STAKEHOLDERS HAMPERS PROGRESS

ERM strategies are about more than preparing for the next risk around the corner. Rather, they are designed to help an organization balance its risks in the near- and long-term, and to do so across the organization's business lines, stakeholders, and footprint.[5] This is best accomplished with an empowered executive leading the way, yet just 36%

Just 18% of respondents said their organization is effective or very effective across all five ERM capabilities.

of respondents say their organization has a formal ERM program headed by a CRO or equivalent role today.

Critically, the data also demonstrates that organizations with a formal ERM C-suite leader or equivalent are more likely to be aware of the multiple ways that risk can manifest and impact them. Respondents from organizations with CRO-driven ERM strategies were more likely to be concerned about every category of risk and were considerably more focused on risks posed by emerging technologies, cybervulnerabilities, insider risks, and risks that impact EX or CX, compared to respondents from organizations that lack a C-suite champion overseeing their ERM strategies.

Just more than one-third of respondents' organizations have ERM strategies led by a CRO or equivalent role.

MISALIGNED PRIORITIES MAKES CLEARLY EVALUATING RISK EVEN MORE DIFFICULT

ERM strategies help organizations better understand their appetites and readiness for risk. Avoiding all risk is impossible, and some risks are even desirable. It's critical that both known and unknown risks be identified, mitigated, and remediated wherever possible.[6] However, respondents said their organizations struggle to properly align their concern over risks with an ability to respond effectively.

Respondents indicated they are highly concerned about several categories of risk and simultaneously lack confidence in their organization's ability to respond should these risks incidents materialize. Respondents were most concerned about cybervulnerabilities, data privacy, first-party or internal cyber risks, and risks coming from vendors and technology stacks. Yet 41% lack confidence in their organization's response to cybervulnerabilities, 39% are unsure about their organization's response to data privacy risk, 40% said their organization would have a suboptimal response to first-party cyber risk, and 44% lack confidence in their organization's ability to respond to vendor or technology risks.

Respondents show high levels of concern over critical risk categories, but lower preparedness to respond.

IT'S NOT THE TOOLS, IT'S THE CONNECTIONS: HOW A LACK OF INTEGRATION HURTS ORGANIZATIONS' RISK MANAGEMENT EFFORTS

Finally, respondents indicated that their organizations' technology challenges are less about satisfaction with point solutions and more about their struggles to align technology capabilities into a comprehensive risk mitigation stack. This study asked respondents to rate how effective their organization's risk management tools were at delivering value and found that satisfaction across tools was relatively high. At worst, 70% of respondents said their brand and reputation tools are effective or highly effective while, on the other end of the spectrum, 84% are satisfied with their organization's cyber risk solutions.

So, what exactly is the problem? In a word: integration. Just 20% of respondents indicated that the solutions their organizations use for risk management today are almost totally integrated with other business systems. This contributes to the lack of understanding and alignment across the organization reflected earlier, and it hinders program effectiveness and response times.

While leaders are reasonably satisfied with individual risk management solutions, they struggle to integrate them across the enterprise.

THE CONSEQUENCES OF INEFFECTIVE RISK MANAGEMENT STRATEGIES ARE HIGH AND RISING

As mentioned earlier, the realities of digital business mean that risks are becoming more — not less — likely to manifest for enterprises, and the trend shows every sign of continuing. Indeed, nearly 70% of respondents said their organization experienced at least two separate critical risk events in the past year, while more than 40% said their organization experienced at least three, and nearly 20% said their organization suffered six or more incidents (see Figure 3).

Figure 3

"In your estimation, how many times has your organization experienced discrete critical risk events in the past 12 months?"

- **16%** - None in the past 12 months
- **14%** - Once
- **26%** - Twice
- **24%** - Three to five times
- **13%** - Six to 10 times
- **4%** - 11 to 15 times
- **1%** - 16 to 20 times
- **1%** - More than 20 in the past 12 months

84%

of respondents' organizations have experienced at least one critical risk event in the past 12 months.

Number of incidents	11 or more	Six or more	Three or more	Two or more
% that have experienced	**6%**	**19%**	**43%**	**69%**

Base: 500 decision-makers responsible for identifying and managing enterprise risk and responding to crises at their organization
Note: Percentages may not total 100 because of rounding.
Source: A commissioned study conducted by Forrester Consulting on behalf of Dataminr, April 2022

Risk management is about more than financial and operational risks, yet many risk leaders are overly focused on the impact of critical events on finance and operations, often at the expense of understanding impact to CX, EX, and reputation.[7] Indeed, respondents were most likely to report that incidents had a negative impact on operations and finance, while critical business drivers like EX, reputation, and CX were far less commonly cited. For their part, study respondents who have HR functions as part of their job responsibilities were 25% more likely than cybersecurity respondents and 21% more likely than corporate security respondents to recognize that critical incidents have a negative impact on EX and employee morale. Meanwhile,

corporate communications professionals were 34% more likely to recognize incidents' impacts on CX compared to cybersecurity leaders.

This helps substantiate the issues risk leaders are facing with enterprisewide coordination and visibility today. Operational and financial disruption are traditional areas of measurement for risk leaders, but they lack a connection to CX, customer success, corporate communications, and employee experience teams that are generally quite capable of measuring those elements. This approach leaves firms struggling to form comprehensive strategies to address known and unknown business events, and it complicates building a business case for risk management investment. Why? Because outcomes end up being linked to efficiency gains and cost reductions rather than making a deeper, more relevant case for how programs improve risk visibility, align ERM efforts to business priorities, and deliver forward-looking insights to help firms act quickly and decisively.[8]

Risk Leaders Prioritize Real-Time Alerting And Cybersecurity

As they plan for the next generation of risk management solutions, cyberthreats and early-alerting capabilities will lead risk leaders' technology agendas during the course of the next year.

- **Cyber risk solutions enable stakeholders to track threat actors and their campaigns.** Intelligence from these vendors helps clients build more-resilient security architectures and reduce the frequency and impact of intrusions.[9] Given how concerned respondents are about the various and expanding threats their organizations face, it's highly consistent that cyber risk solutions sit at the top of technologies that risk leaders are looking to onboard and invest in during the near term.
- **Real-time alerting tools power quick and effective incident response.** These tools notify risk leaders about events in the minutes or even seconds after they happen, giving decision-makers context and clarity so they can respond quickly and effectively. Fifty-six percent of respondents indicated their organizations don't have real-time alerting solutions in place today, but 62% said their organization plans to implement or expand its use of these tools, and 54% said their organization plans to increase investment during the next 12 months.

REAL-TIME ALERTING TOOLS HELP MINIMIZE THE IMPACT OF CRITICAL EVENTS

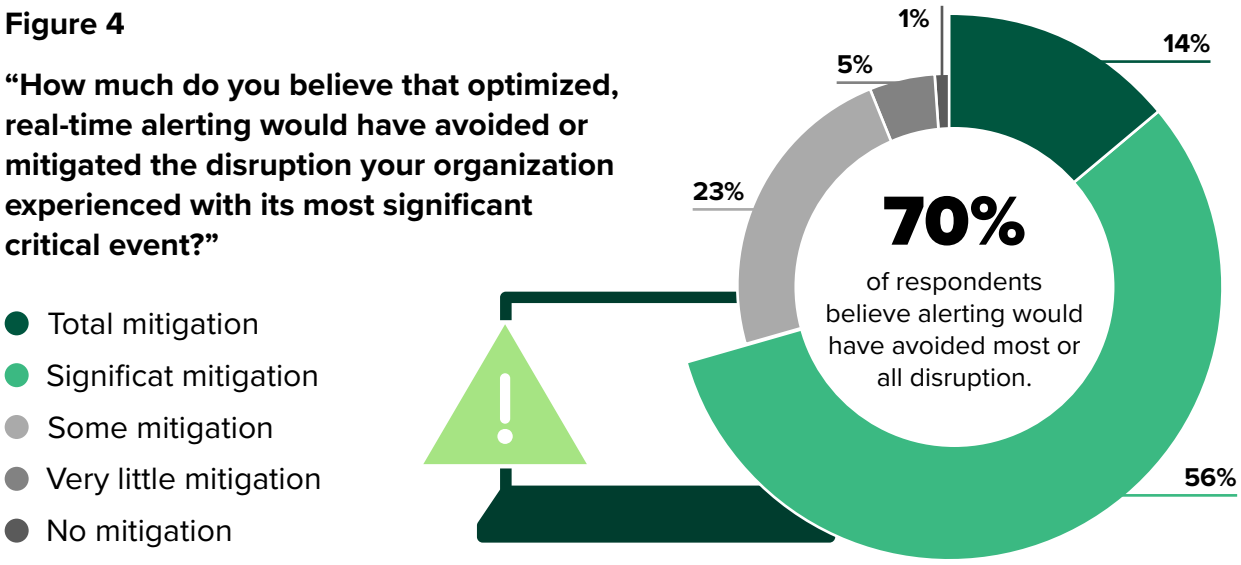
In a highly dynamic risk environment, response speed is not a luxury but a requirement. Real-time alerting gives decision-makers the clarity they need to be proactive and to form, adapt, and manage their responses. Leaders are looking to double down investment and adoption of these tools and capabilities during the next year precisely because they understand the importance of early awareness in mitigating the damage a critical event can cause.

In fact, 70% of respondents believe that optimized, real-time alerting would have helped their organizations significantly or totally reduced the harm of the most significant or disruptive event they faced last year (see Figure 4). When you include those that would have enjoyed some mitigation last

year, that number jumps to 93%. Ultimately, time is the most valuable, least renewable resource of any enterprise, and investments that help optimize early detection and contextualization of critical events rank so highly on risk leaders' agendas because of their role in driving fast, accurate responses and heightened resilience.

Figure 4

"How much do you believe that optimized, real-time alerting would have avoided or mitigated the disruption your organization experienced with its most significant critical event?"



Base: 500 decision-makers responsible for identifying and managing enterprise risk and responding to crises at their organization
Note: Percentages may not total 100 because of rounding.
Source: A commissioned study conducted by Forrester Consulting on behalf of Dataminr, April 2022

93%

of security and risk decision-makers believe that improvements to real-time alerting would have at least somewhat mitigated their most significant critical event from last year. Seventy percent believe it would have led to significant or total harm reduction.

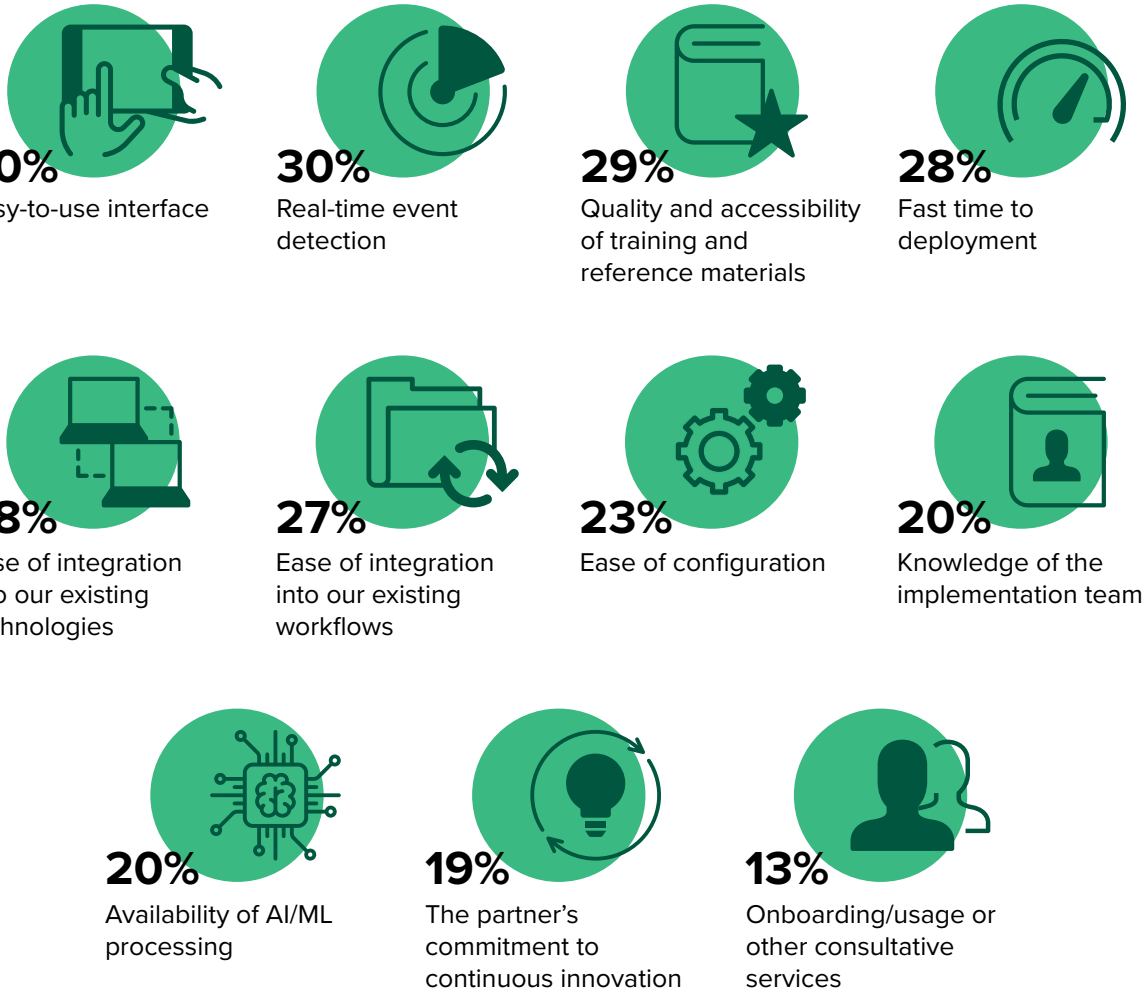
ORGANIZATIONS REQUIRE APPROACHABLE SOLUTIONS THAT BOOST ADOPTION AND ACCESSIBILITY

ERM strategies are aided by taking an integrated approach to identifying, evaluating, and responding to incidents and, ultimately, they will lead to reduced exposure and better outcomes. This requires that risk leaders collaborate with other key stakeholders within the organization, so it follows that leaders prioritize solutions that promote adoption.

Respondents said that ease of use and real-time alerting will be their most important criteria in their organization's next risk management solution. Closely following, risk leaders prefer solutions that have high-quality training and reference materials, that can deploy quickly, and that seamlessly integrate into existing technologies and workflows. In doing so, solutions that enable faster, broader adoption of risk management tools help risk leaders more effectively expand their concept of risk to cover all corners of their enterprise (see Figure 5).

Figure 5

"Which of the following features are most important to you when selecting your next risk management partner or solution?"

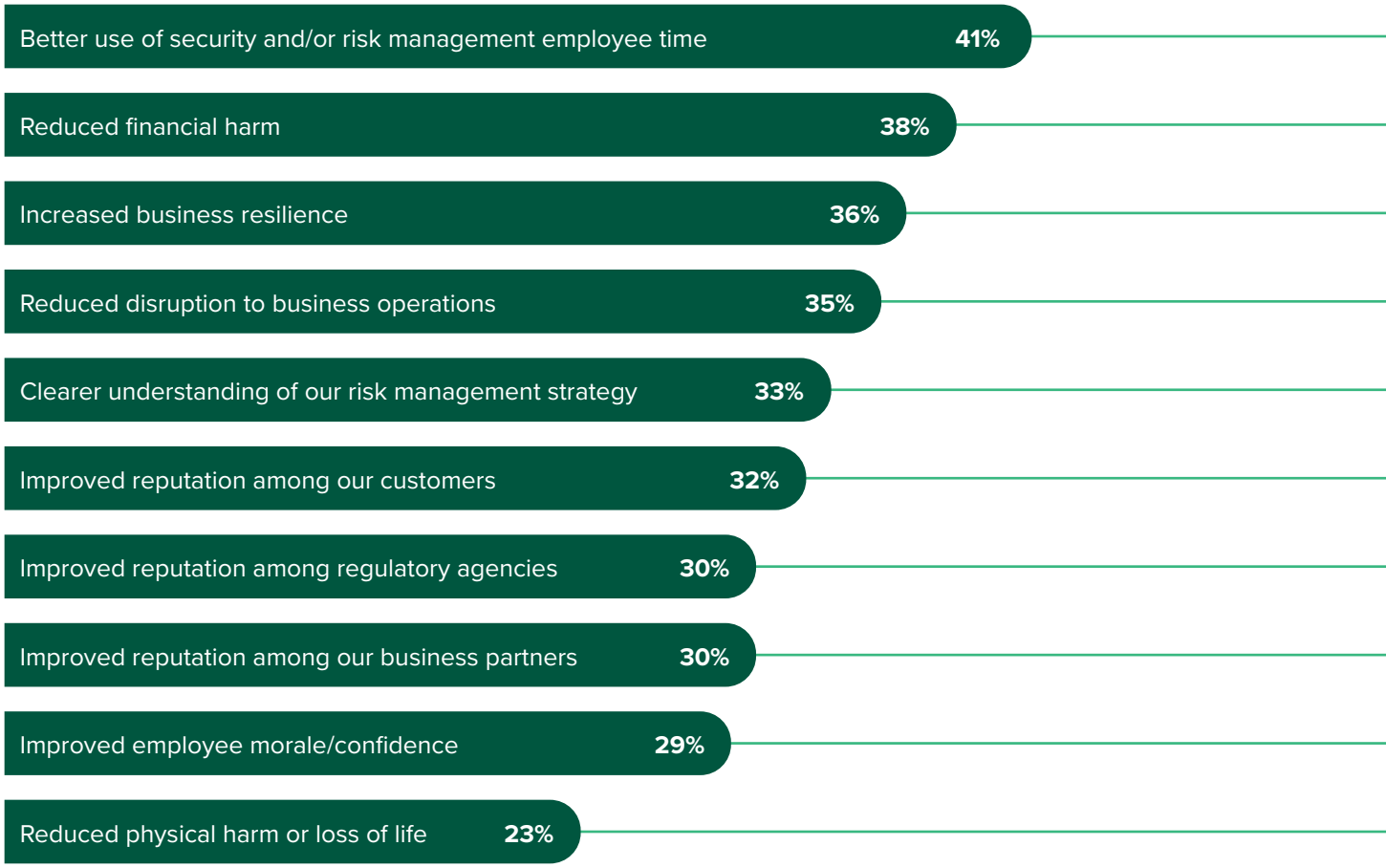


Base: 500 decision-makers responsible for identifying and managing enterprise risk and responding to crises at their organization
Source: A commissioned study conducted by Forrester Consulting on behalf of Dataminr, April 2022

Proper integration of risk management technologies is also seen as a major driver of resilience and efficiency. We asked respondents to outline the benefits that would result from adopting an integrated risk management platform that combines risk identification, evaluation, monitoring, response, and communications. Every respondent said they expect at least one positive outcome from an integrated risk management platform. At the top of the list, risk leaders believe their teams could spend less time on rote tasks and more time on strategically important initiatives. They were nearly as likely to associate integrated platforms with reduced financial harm and greater business resilience (see Figure 6).

Figure 6

"Which of the following benefits would result from adopting an integrated risk management platform that lets you quickly and accurately identify and evaluate risks and execute coordinated response, monitoring, and communications workflows?"



Base: 500 decision-makers responsible for identifying and managing enterprise risk and responding to crises at their organization
Source: A commissioned study conducted by Forrester Consulting on behalf of Dataminr, April 2022

Fortify Your ERM Foundation For A More Resilient Organization

During the next five years, business and technology changes will only accelerate, and the constant shifts in businesses' risk landscapes will increase accordingly. In response, mature firms enable world-class ERM programs to navigate risk and steer their businesses through the changing dynamics and expectations to become a trusted business and a value-aligned brand.[10]

Previously, this study described the five core competencies that drive ERM success: the ability to identify, evaluate, monitor, respond to, and communicate about risk effectively. We also demonstrated that organizations' risk strategies often struggle to achieve mastery, especially across these categories. Doing so certainly requires investment, focus, and the input of stakeholders across the organization. But what lies beneath successful ERM implementations? To address this question, this study identified and compared the 15% of respondents from the organizations with the most sophisticated ERM programs with the 15% from the organizations with the least effective approaches.

SUCCESSFUL ERM PROGRAMS ARE CHAMPIONED BY LEADERS WHO ARE EMPOWERED ACROSS THE ORGANIZATION

One critical barrier to implementing an effective ERM strategy arises in its enterprisewide nature: Organizations can count on a need to identify and overcome organizational silos. Indeed, respondents from organizations with less-effective ERM strategies were 30% more likely to cite organizational complexity as a barrier to implementing more-effective risk management, and those from organizations with less-effective ERM implementations were 38% more likely to need a clearer understanding of their risk management strategies. This indicates that enterprisewide acceptance and understanding is lacking compared to more effective strategies.

Conversely, respondents from organizations with highly effective ERM strategies were 27% more likely to have a C-suite leader for ERM, and 28% more likely to have risk and compliance led by the C-suite, compared to those from lower-maturity organizations. C-suite champions are empowered

to work across organizational silos and to coordinate with other business leaders within the organization. This helps explain why respondents from organizations with effective ERM are also 63% more likely to review and update their risk registers through frequent participation from relevant business units and functions, enabling better visibility across the enterprise's risk footprint and better alignment between risk strategy and business goals.

RESPONDENTS FROM ORGANIZATIONS WITH MORE-EFFECTIVE ERM STRATEGIES ARE MORE AWARE OF RISK CATEGORIES AND REPERCUSSIONS

Respondents from organizations with more-effective ERM strategies are more likely to have every category of risk in the study on their radar, and they showed a heightened understanding of how risk impacts key business considerations like EX, CX, and company reputation. They were also more likely to express confidence in their ability to respond to each risk category (see Figure 7).

MORE EFFECTIVE ERM STRATEGIES ARE DRIVEN BY POWERFUL, INTEGRATED TECHNOLOGY

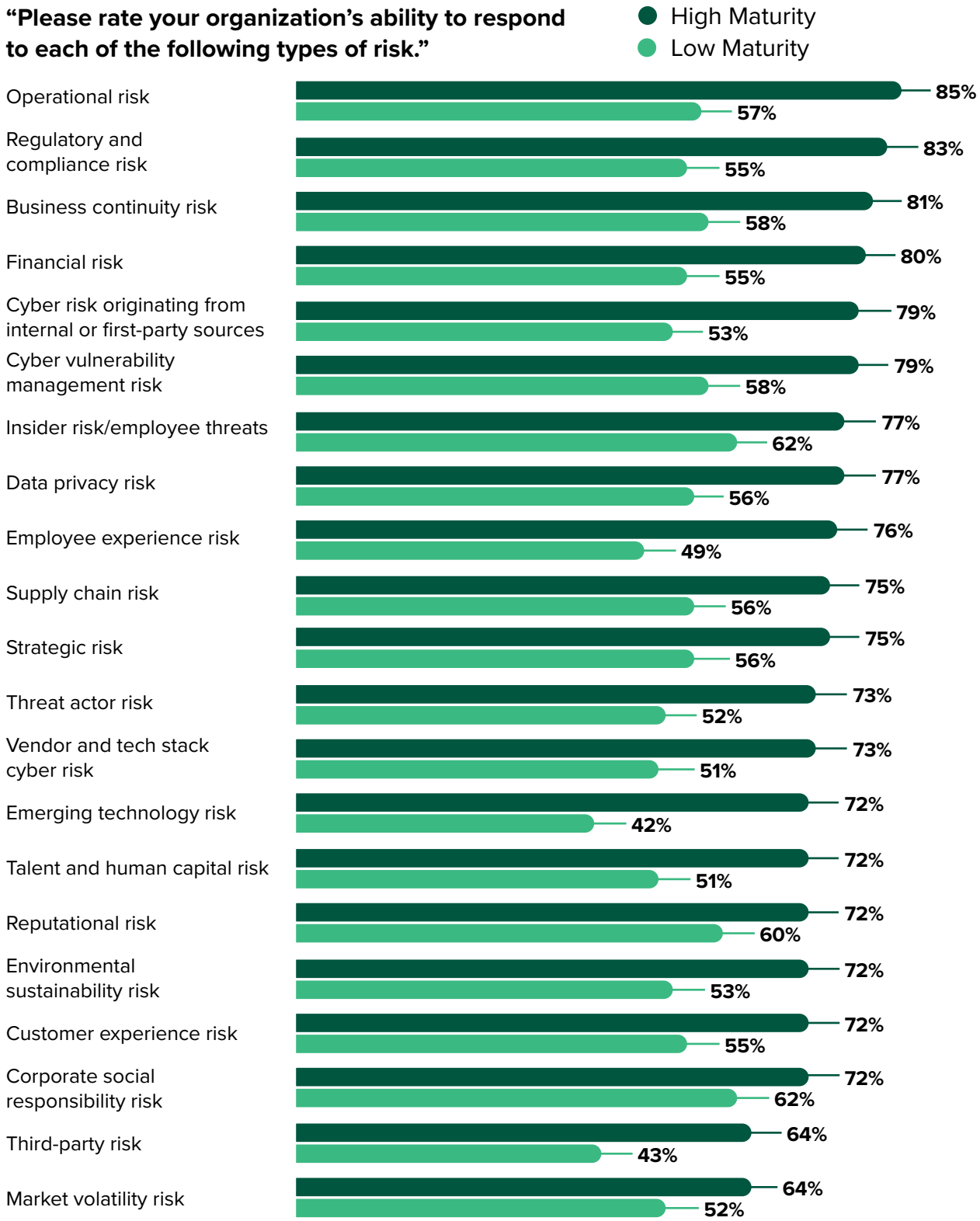
Finally, more-effective ERM strategies tend to be accompanied by fully featured, integrated technology suites. Respondents from more-mature organizations said their organization was 78% more likely to have implemented cyber risk solutions, 39% more likely to have implemented threat or risk assessment tools, 71% more likely to have implemented safety and security mobile applications, 44% more likely to have implemented incident management, and 9% more likely to have implemented real-time alerting tools than respondents from less-mature organizations.

They were also more likely to describe their organization's tools as effective. For example, they were 20% more likely to say their organization's real-time alerting tools are effective or highly effective. Even more tellingly, they were 74% more likely to describe their organization's risk management tools as integrated or fully integrated with one another, which significantly boosts alignment, speed, and accuracy.

Additionally, respondents from organizations with more-effective ERM programs said they were more likely to see a host of benefits from their strategies. They were 95% more likely to cite improved reputation among

Figure 7

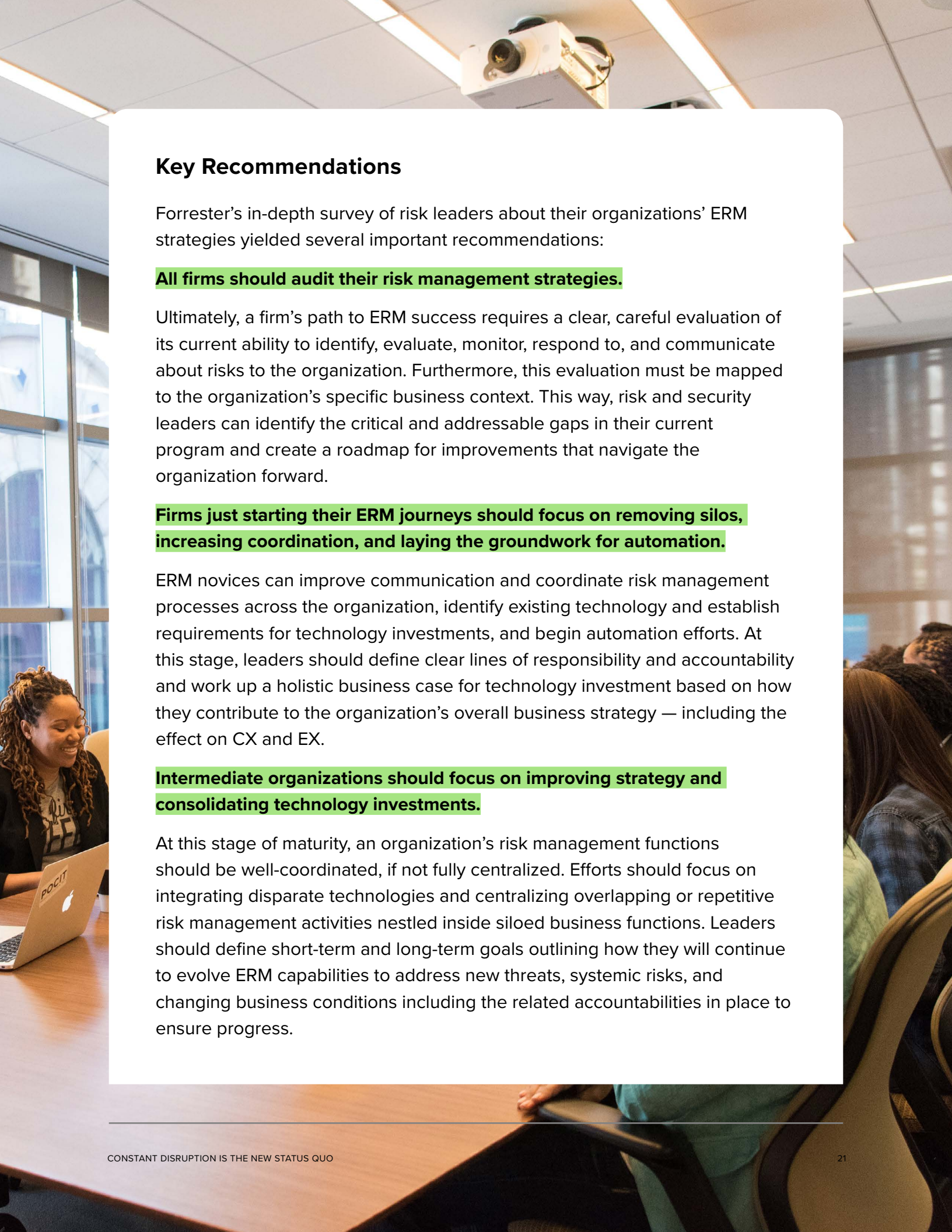
"Please rate your organization's ability to respond to each of the following types of risk."



Base: 152 decision-makers responsible for identifying and managing enterprise risk and responding to crises at their organization
Source: A commissioned study conducted by Forrester Consulting on behalf of Dataminr, April 2022

business partners as a program benefit, 34% more likely to cite reduced disruption to business operations, 22% more likely to cite improved reputation with regulatory agencies, and 10% more likely to cite better use of security and risk employee time. In short, investment in comprehensive, effective risk management strategies pays off.

Organizations with advanced ERM programs are far more likely to realize the benefits of their risk management strategies.



Key Recommendations

Forrester's in-depth survey of risk leaders about their organizations' ERM strategies yielded several important recommendations:

All firms should audit their risk management strategies.

Ultimately, a firm's path to ERM success requires a clear, careful evaluation of its current ability to identify, evaluate, monitor, respond to, and communicate about risks to the organization. Furthermore, this evaluation must be mapped to the organization's specific business context. This way, risk and security leaders can identify the critical and addressable gaps in their current program and create a roadmap for improvements that navigate the organization forward.

Firms just starting their ERM journeys should focus on removing silos, increasing coordination, and laying the groundwork for automation.

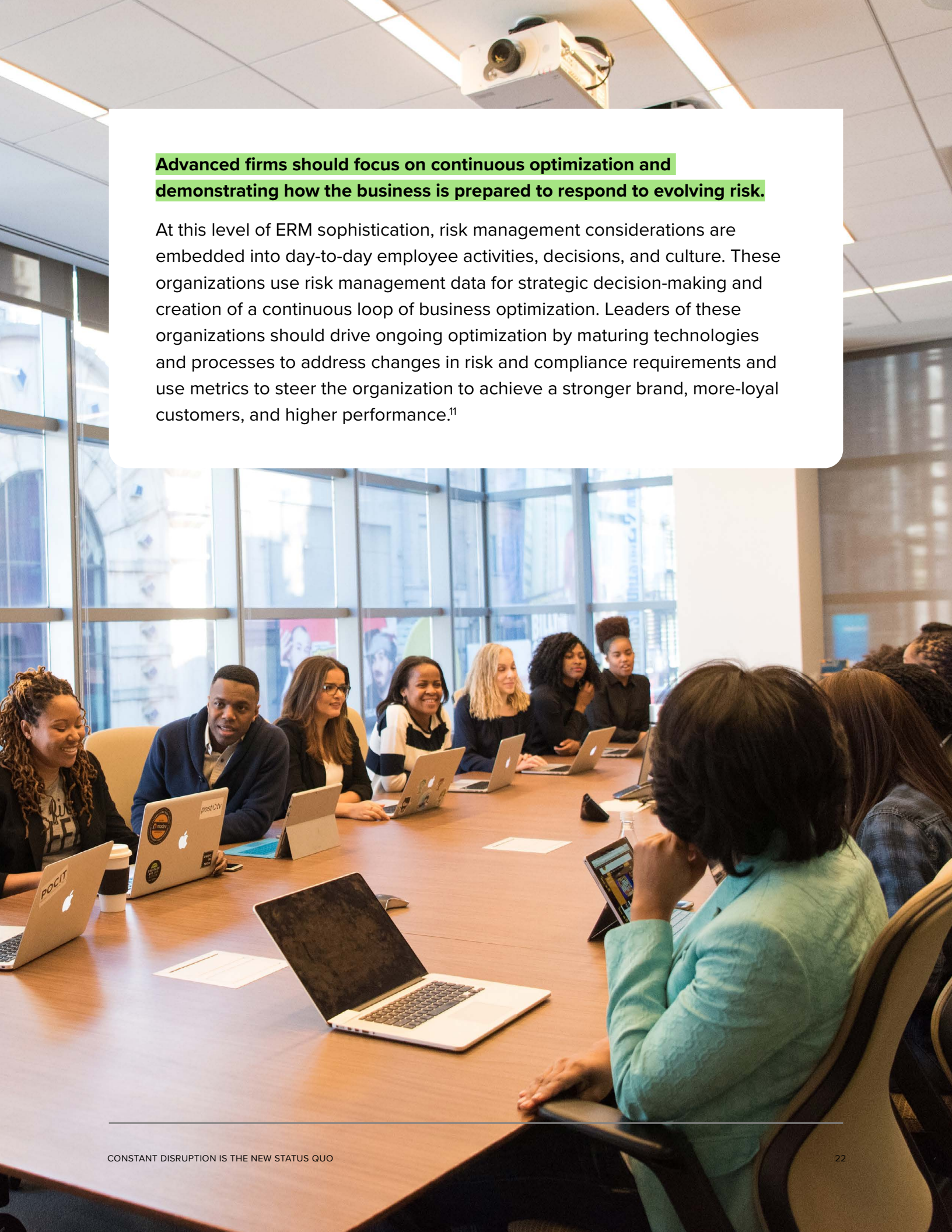
ERM novices can improve communication and coordinate risk management processes across the organization, identify existing technology and establish requirements for technology investments, and begin automation efforts. At this stage, leaders should define clear lines of responsibility and accountability and work up a holistic business case for technology investment based on how they contribute to the organization's overall business strategy — including the effect on CX and EX.

Intermediate organizations should focus on improving strategy and consolidating technology investments.

At this stage of maturity, an organization's risk management functions should be well-coordinated, if not fully centralized. Efforts should focus on integrating disparate technologies and centralizing overlapping or repetitive risk management activities nestled inside siloed business functions. Leaders should define short-term and long-term goals outlining how they will continue to evolve ERM capabilities to address new threats, systemic risks, and changing business conditions including the related accountabilities in place to ensure progress.

Advanced firms should focus on continuous optimization and demonstrating how the business is prepared to respond to evolving risk.

At this level of ERM sophistication, risk management considerations are embedded into day-to-day employee activities, decisions, and culture. These organizations use risk management data for strategic decision-making and creation of a continuous loop of business optimization. Leaders of these organizations should drive ongoing optimization by maturing technologies and processes to address changes in risk and compliance requirements and use metrics to steer the organization to achieve a stronger brand, more-loyal customers, and higher performance.[11]



Appendix A: Methodology

In this study, Forrester conducted an online survey of 500 enterprise risk decision-makers at organizations in North America, Europe, and APAC to evaluate the state of their organizations' risk management strategies. Survey participants included decision-makers in security, EX, corporate communications, and supply chain roles. Questions provided to the participants asked how their organizations navigate risk strategies, technologies, and workflows. Respondents were offered a small incentive as a thank you for time spent on the survey. The study began in December 2021 and was completed in July 2022.

Appendix B: Demographics

GEOGRAPHY	
North America	**45%**
Europe	**30%**
APAC	**26%**

TITLE	
C-level executive	**17%**
Vice president	**24%**
Director	**39%**
Manager	**19%**

SIZE (REVENUE)	
More than $10B	**11%**
$5B to $10B	**16%**
$1B to $ 4.9B	**38%**
$500M to $999M	**36%**

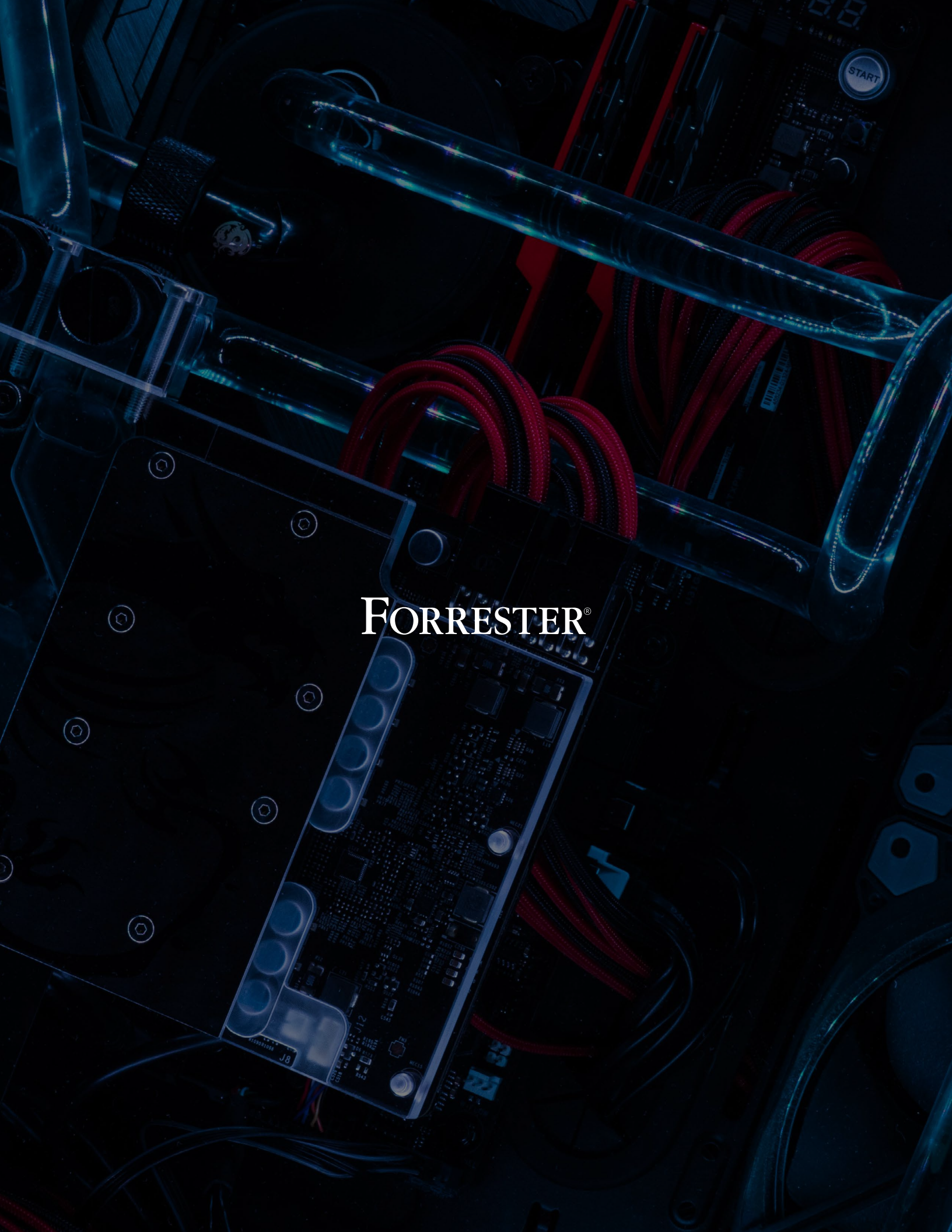
DEPARTMENT	
Cyber/information security	**16%**
HR / EX	**16%**
Corporate comms	**12%**
Security operations	**12%**
Supply chain	**9%**
Sourcing / procurement	**9%**
Business continuity and disaster recovery	**9%**
Physical security	**6%**

RISK RESPONSIBILITY	
Final decision-maker	**51%**
Part of team leading decisions	**33%**
Influences decisions	**16%**
$500M to $999M	**36%**

Note: Percentages may not total 100 because of rounding.

Appendix D: Endnotes

[1] Source: “ERM Vision, 2021 To 2026,” Forrester Research, Inc., August 2, 2021.
[2] Ibid.
[3] Source: “Transition From A Traditional To A Transformational CRO,” Forrester Research, Inc., May 12, 2022.
[4] Source: “Proactively Manage Risk With The Forrester ERM Success Cycle,” Forrester Research, Inc., August 2, 2021.
[5] Source: “ERM Vision, 2021 to 2026,” Forrester Research, Inc., August 2, 2021.
[6] Source: “Proactively Manage Risk With The Forrester ERM Success Cycle,” Forrester Research, Inc., August 2, 2021.
[7] Source: “Build The Business Case For Enterprise Risk Management,” Forrester Research, Inc., August 2, 2021.
[8] Ibid.
[9] Source: “The Forrester Tech Tide™: Threat Intelligence, Q2 2021,” Forrester Research, Inc., April 13, 2021.
[10] Source: “Drive Faster, Better Strategic Decisions With Enterprise Risk Management,” Forrester Research, Inc., August 2, 2021.
[11] Source: “Get Strategic With A Dynamic ERM Roadmap,” Forrester Research, Inc., August 2, 2021.


START
FORRESTER®