NAVEX®

2023

State of Risk & Compliance Report

NAVEX®

NAVEX is the recognized leader in risk and compliance management software and services, empowering thousands of customers around the world to manage and mitigate risks with confidence. NAVEX's mission is to help customers promote ethical, inclusive workplace cultures, protect their brands and preserve the environment through sustainable business practices.

For more information, visit NAVEX.com and our blog. Follow us on Twitter and LinkedIn.

Contents

Prepared by:

Carrie Penman
Chief Risk and Compliance Officer
NAVEX

Introduction

NAVEX has been collecting and delivering leading-edge market benchmark reports to the risk and compliance (R&C) industry since 2010. In 2019, we published our first-ever "Definitive Corporate Compliance Benchmark Report," a comprehensive review of R&C programs that offered key findings, analysis and insight to help organizations measure, evaluate and advance their programs.

This year, NAVEX partnered again with independent research firm The Harris Poll to survey R&C professionals from a wide range of industries about the design, priorities and performance of their R&C programs. The results of the survey represent over 1,300 respondents globally who influence or manage their organization's risk and compliance programs. In addition, this report includes detailed responses from those who actively manage or influence their program's incident management, policy and procedure management, ethics and compliance training, third-party risk management, integrated risk management, and/or environmental, social and governance (ESG) functions. Insights and analysis addressed in the new 2023 report include:

- How are R&C professionals assessing their own program maturity?
- What are mature programs more likely to have in common?
- How do program trends differ across certain countries?
- What differences exist across organizational size?
- Which program elements are most common across organizations?
- What is the nature of leadership's engagement with R&C?
- How has remote and hybrid work impacted culture?
- What role does data play in today's R&C programs?

How to use this report

The data and insights in this report help chief compliance officers and other R&C professionals make informed program decisions. The report also outlines practical ways to improve R&C programs of all maturity levels and organizational sizes.

- Benchmark your organization's program against peers, industry standards and best practices.
- Assess your program maturity.
- Identify specific steps to improve performance.
- Review and compare program priorities and effectiveness measures.
- Determine whether your approach to organizational risk is aligned with market trends and best practices.
- Review how your organization is protected or exposed to risk through your approach to incident management; policy and procedure management; ethics and compliance training; third-party risk management; and environmental, social and governance practices.
- Leverage reports and recommendations to get organizational buy-in, budget and understanding of the ROI of a comprehensive risk and compliance program.

Survey methodology

The 2023 report research was conducted online by The Harris Poll on behalf of NAVEX among 1,315 adults 18+ who are nonacademic professionals (management/non-management or higher) and knowledgeable about risk and compliance in the United States (n=738), United Kingdom (n=177), France (n=157), Germany (n=151), Canada (n=50), and other countries (n=42). The survey was conducted between January 30 – March 10, 2023.

Raw data were not weighted and are therefore only representative of the individuals who completed the survey.

Respondents for this survey were from NAVEX's list of customers or prospects or selected from among those who have agreed to participate in online surveys. The sampling precision of Harris online polls is measured by using a Bayesian credible interval. For this study, the sample data is accurate to within +/- 2.7 percentage points using a 95% confidence level. This credible interval will be wider among subsets of the surveyed population of interest.

The 2022 report was conducted in Spring 2022 among 1,105 R&C professionals, all of whom were current or prospective NAVEX customers. The research primarily included U.S. R&C professionals (n=774) but did include some participants from at least 18 other countries (n=331).

> When comparing results between 2023 and 2022, it is important to note the differences in the sample size and composition. The 2023 research includes more total responses than in previous years (1,315) and a greater concentration of responses from the EU. Additionally, the 2023 research utilized online research panels. Year-over-year comparisons should be considered with this in mind.

All sample surveys and polls, whether or not they use probability sampling, are subject to other multiple sources of error which are most often not possible to quantify or estimate, including, but not limited to coverage error, error associated with nonresponse, error associated with question wording and response options, and post-survey weighting and adjustments. All charts show data rounded to the nearest whole percent. The values of some percentages are too small to be shown in the charts. Please refer to the appendix for additional data.

Key definitions

POLICY MANAGEMENT includes controlling the organization's policies and procedures throughout the policy lifecycle: drafting, editing, approving, updating, distributing, storing and documenting attestations. Policy management software (or a policy management system) refers to the technology that enables more efficient management and execution of those practices.

ETHICS AND COMPLIANCE (E&C) TRAINING includes regulatory compliance, conduct, employment law and information security training from a behavioral perspective. This definition includes all forms of training on ethics and compliance topics: online, in-person, virtual and blended training approaches. Educational and awareness approaches are also within this scope of training.

INCIDENT MANAGEMENT typically consists of telephone, web, mobile and other whistleblower channels where employees and other stakeholders can make reports. Incident management systems receive, record and encourage responses to questions, reports and incidents received, and offer executive reporting tools and the ability to track and manage resolution.

THIRD-PARTY RISK MANAGEMENT is an umbrella term that refers to all risk-management activities related to third parties: onboarding, screening, monitoring and in-depth risk analysis; as well as associated processes to identify, stratify, prioritize and mitigate third-party risks. Third-party due diligence refers to the studied assessment of third parties before, during and after an engagement. Internal business justifications, external preliminary risk assessments, establishing business rules and authorizations, processing documentation and policies, database analysis and reputational reporting are all third-party due diligence. It also includes active monitoring of third-party engagements for new "red flags" and real-time changes to the third party's risk profile.

INTEGRATED RISK MANAGEMENT is a process that improves decision making and enhances business value by integrating risk intelligence into activities across the enterprise, such as strategic planning and strategy execution, investment decision making, project portfolio management, enterprise performance management, third-party performance management and information governance.

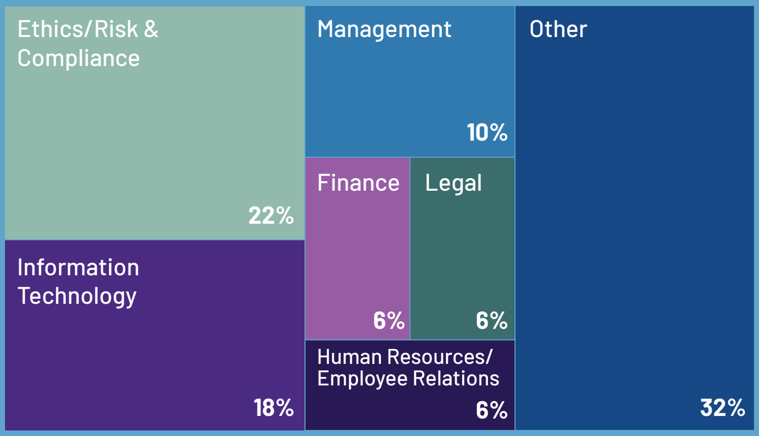
ENVIRONMENTAL, SOCIAL AND GOVERNANCE (ESG) is a subset of non-financial performance indicators which include environmental, social, ethical and corporate governance issues such as managing a company's carbon footprint and ensuring there are systems in place to ensure accountability.

PROGRAM MATURITY is a measure of the size and sophistication of a company's existing risk and compliance program. For the purposes of the 2023 study, maturity designations were self-reported based on the criteria of the High-Quality Ethics & Compliance Program (HQP) Assessment from the Ethics & Compliance Initiative (ECI).[1] We utilize program maturity as an indicator of current proficiency and performance.

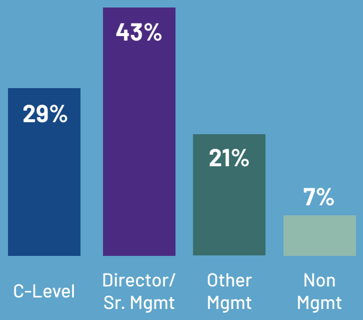
[1] https://www.ethics.org/wp-content/uploads/2018/09/ECI-Framework-Final.pdf

A SNAPSHOT OF OUR SURVEY PARTICIPANTS

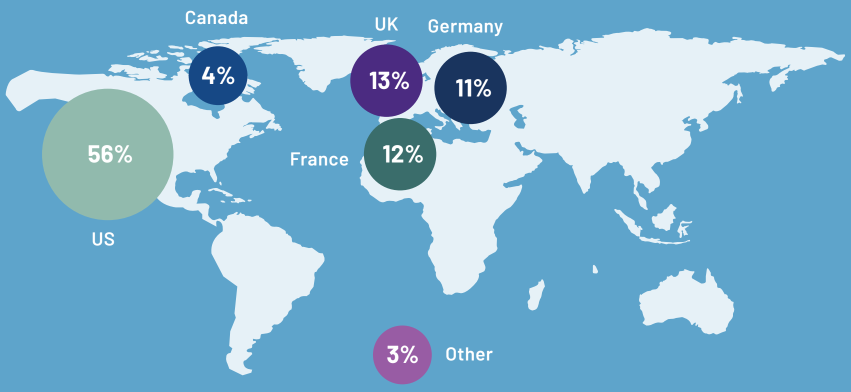
Job function



Job level



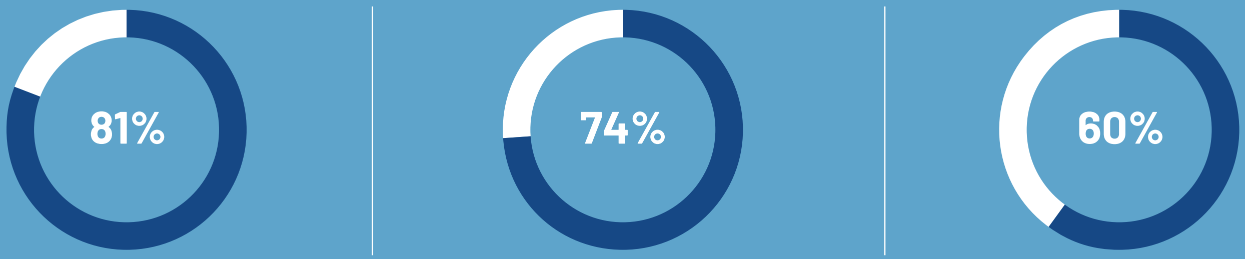
Country of residence



Company headquarters

North America	56%
Europe	39%
Central America	1%
Asia Pacific - Japan	1%
Asia Pacific - Other Country	1%
South America	1%
Other	1%

Knowledge about



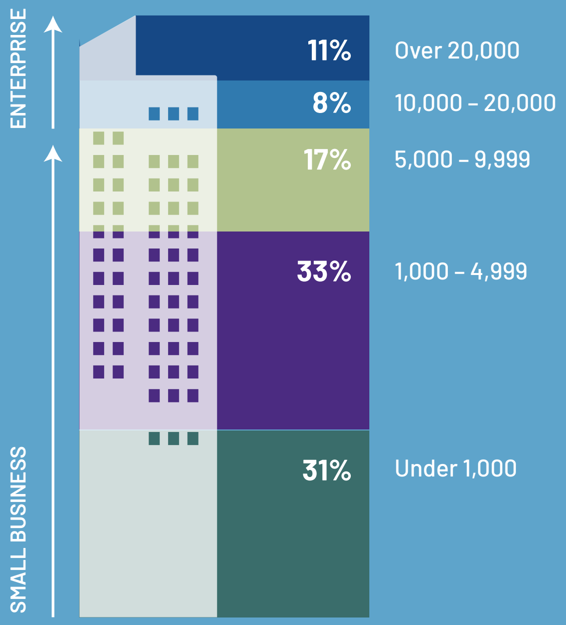
RISK MANAGEMENT

ETHICS & COMPLIANCE

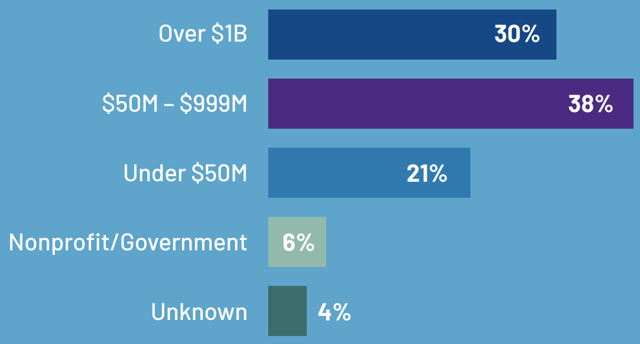
ENVIRONMENTAL, SOCIAL & GOVERNANCE

A SNAPSHOT OF COMPANIES REPRESENTED

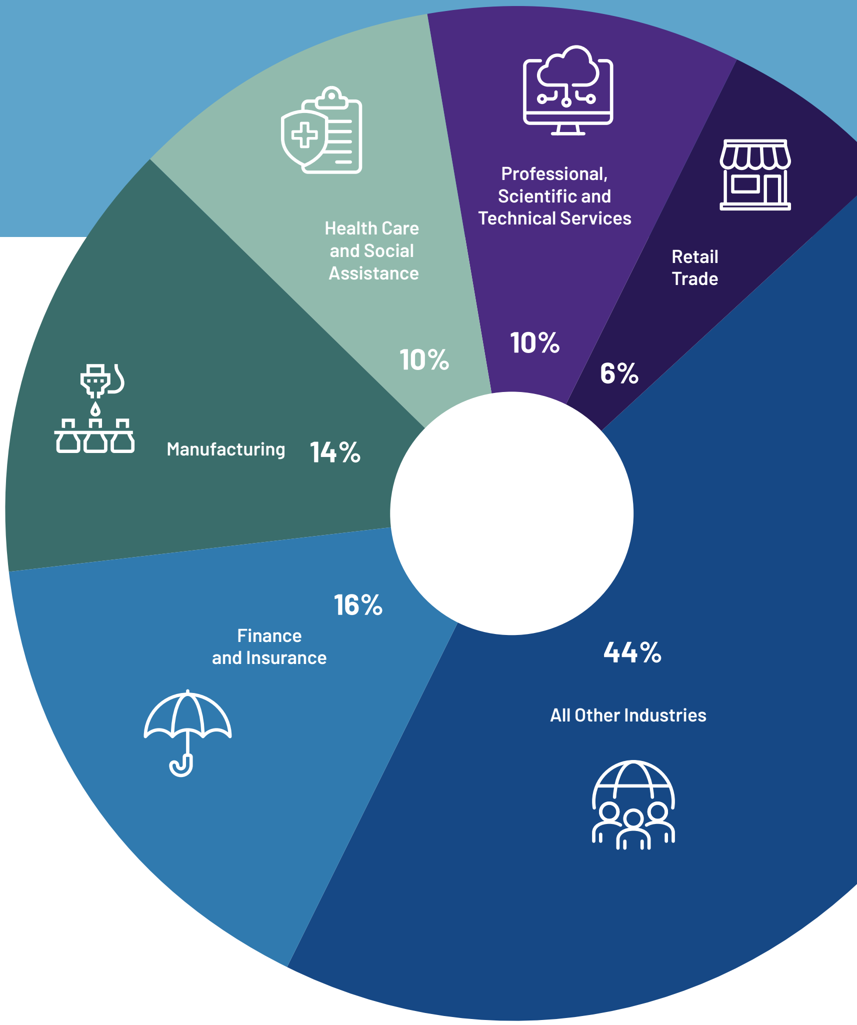
Company size (# of employees)



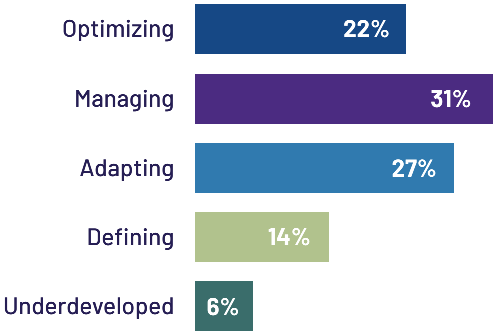
Annual revenue (USD)



Industries



Program maturity



Executive summary

The story of this 2023 State of Risk & Compliance Report is one of progress. Risk and compliance (R&C) professionals are reporting greater program maturity, signaling the growing confidence, stature and sophistication of our professions. Many are also reporting promising collaboration across silos with Information Security (InfoSec), which may indicate more organizations are taking a holistic view of what it takes to successfully manage risk and build ethical cultures. And any fears that workplace culture would suffer as many temporary COVID-19 remote-work arrangements became permanent appear moot – by a wide margin, R&C professionals are reporting positive outcomes from work-from-home models.

However, this publication also depicts a story of challenges. That same InfoSec/Compliance collaboration comes as R&C professionals most commonly reported a *data privacy/cybersecurity breach* as a real-world compliance issue their organization has faced in recent years. Even more than last year, middle management is not always choosing a commitment to compliance over competing interests. And R&C professionals cited anti-retaliation and whistleblowing as a relatively low focus in Europe, where corresponding regulations have intensified.

Drawing on over 1,300 survey responses from R&C professionals around the globe, these findings and more form the basis of NAVEX's 2023 State of Risk & Compliance Report. NAVEX has refined the title of this report to better depict the value it brings to our industry – a barometer of how our profession is self-reporting its successes, obstacles, evolutions, and opportunities to improve.

This year's respondent group represents the largest ever in the history of this survey and report, and for the first time, the report includes special analysis for several major European countries and by size of organization.

Our global reach has highlighted some interesting differences between the U.S. and Europe, including, fundamentally, what "Compliance" might mean for organizations in those respective geographies. This is revealed through differences in prioritization of whistleblowing, focus on information security, confidence in leadership, planned training, and much more. Yet despite differences, so often, our guidance settles on some universal truths – that effective R&C programs, ones with cross-functional collaboration, executive buy-in, strong policies, engaging training, robust internal whistleblowing mechanisms and vigilant supplier management, are best poised to navigate the regulatory landscape while fostering a culture of ethics and compliance. Even for the most mature programs, the task of fostering those dynamics is one of continuous improvement.

This year's report should give R&C professionals a better picture than ever before of the ways their programs positively impact their organizations. Our "Key findings" section reflects our take on the narrative that weaves through the hundreds of survey responses we received from around the globe – we hope our audience will consider how those stories and learnings are relevant to their own organizations. Our "Program-specific elements" section provides context for additional survey findings. Finally, our "Key company size comparisons" section showcases relevant findings specific to certain countries and between smaller and enterprise organizations.

We hope this report gives R&C professionals yet another tool to put their program in context with their global peers, and to make informed decisions on ways to improve.

2023

Key Findings

1 Program maturity

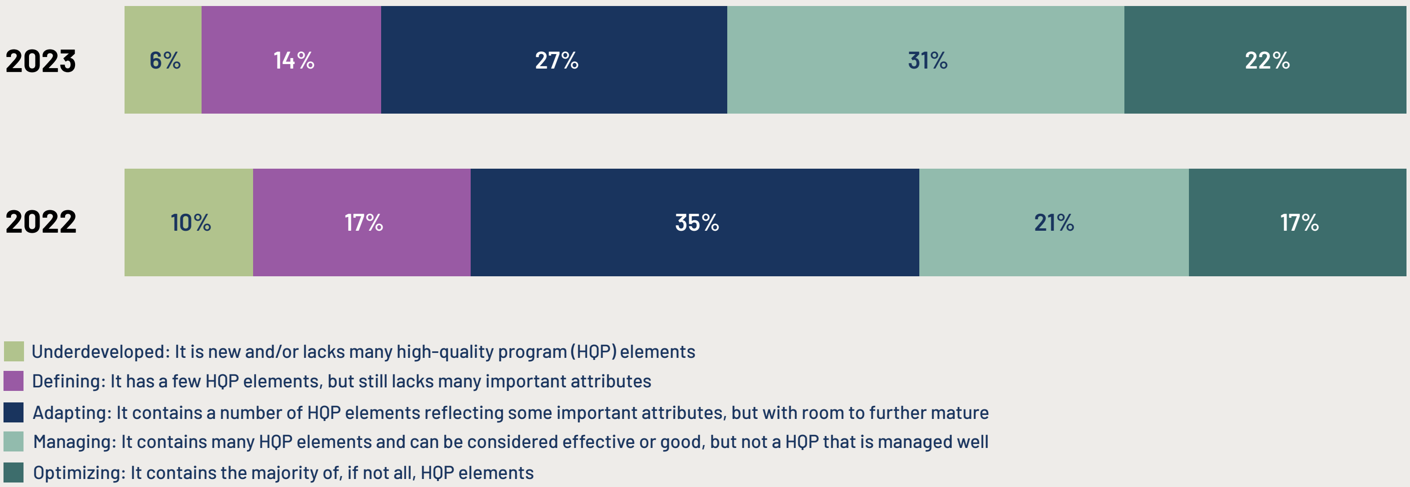
For this year's study, respondents' maturity designations were self-reported based on the High-Quality Ethics & Compliance Program (HQP) Assessment criteria from the Ethics & Compliance Initiative (ECI). This five-point scale begins at the least mature, *underdeveloped*, and builds in maturity from *defining*, *adapting*, *managing* and, at the most mature end, *optimizing*.[2] In assessing findings from this area of the survey, we refer to the two ends of the spectrum in the following way:

> **Mature:** Programs classified as *managing* or *optimizing*

> **Early Stage:** Programs classified as *underdeveloped* or *defining*

A significantly greater share of respondents described their programs as mature – *managing* or *optimizing* – in 2023 than in 2022. More than half (53%) said their organization was on the mature side of the spectrum, compared to 38% in 2022. Only 20% said their program was early stage this year, compared to 27% in 2022. Today's stringent regulatory environment, combined with societal expectations for greater transparency, require more compliance rigor than ever before. Thus, it is a good sign that an increasing share of respondents classified their programs as mature.

R&C program maturity



BASE: ALL QUALIFIED RESPONDENTS (n=1,315)
Which of the following statements best describes your organization's Risk & Compliance program?

[2] https://www.justice.gov/criminal-fraud/page/file/937501/download

Respondents in France (25%) and the United States (23%) were more likely to describe their organizations risk and compliance program as *optimizing* than Germany (16%). Germany-based respondents were more likely than these geographies to describe their program in the middle maturity category of *adapting*.

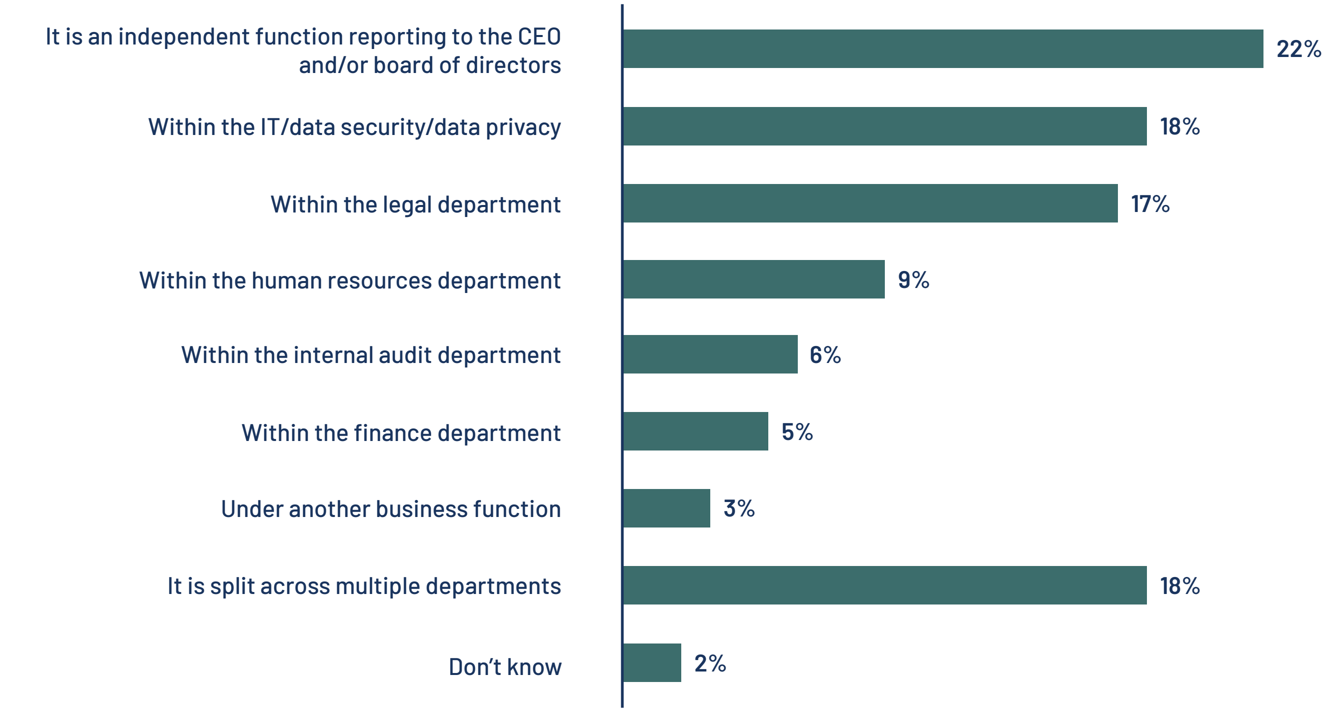
The data also shows that program maturity often aligns with strong board- and executive-level engagement. A deeper analysis of the roughly half of the responses from those who classify their program as mature reveals the following:

- **67%** deliver periodic reports to the board of directors
- **55%** have compliance experience or expertise represented on their board
- **52%** participate in private sessions with a board-level committee
- **25%** indicate that Compliance is an independent function reporting directly to the CEO or board

Among all respondents, a similar number of respondents (22%) reported that Compliance is independent and reports to executive leadership.

Respondents in the U.S. (21%) and the U.K. (22%) were the most likely to say that their compliance functions were housed in multiple departments, compared to 10% of respondents in Germany and 9% of respondents in France.

Department where compliance function resides



BASE: KNOWLEDGEABLE ABOUT ETHICS & COMPLIANCE (n=977)
Where is your organization's compliance function housed?

While it is beyond the scope of this research to determine whether program maturity is a cause or result of executive-level interest, it seems logical that more mature programs would produce data and results with strategic implications worthy of executive attention. It is also quite possible that a sophisticated board might require a more mature compliance program be in place and expect regular reporting on its performance. This is reflected in ECI's model, which specifically identifies board engagement as a factor in moving a program to greater levels of maturity.

2 Interdependence of Compliance, Data Privacy and IT/Information Security

It will come as no surprise to readers of this report that information security (InfoSec) continues to be a major concern for the compliance function.

As organizations of every size become more digitally dependent and connected – both internally and to their suppliers – it is no longer reasonable to consider InfoSec an isolated IT risk. Similarly, the compliance function is embracing the fact that InfoSec is becoming one of their most pressing compliance risks. To fully understand and mitigate these risks requires access to, and influence over, business processes that may have historically lived exclusively within IT.

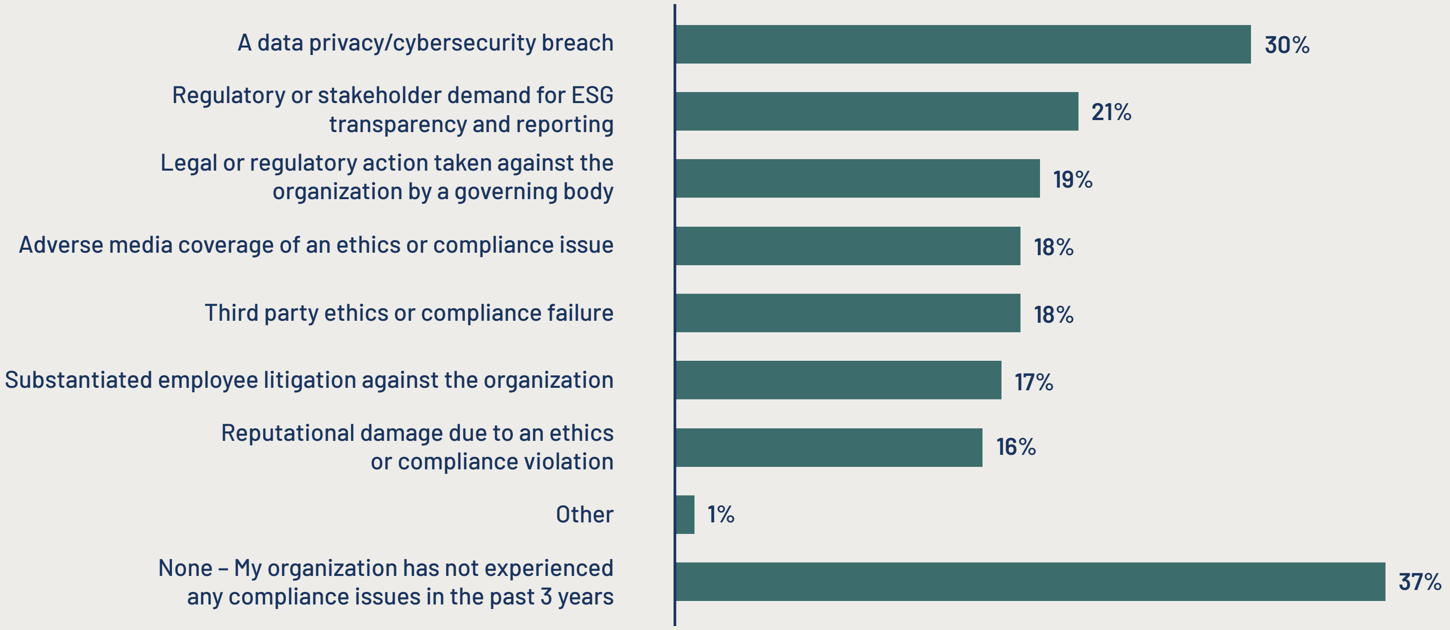
This year's findings demonstrate the importance of collaboration between the two roles, along with a compliance risk landscape that is tilting increasingly toward InfoSec and data privacy concerns. Simply put, the chief compliance officer (CCO) and chief information security officer (CISO) are interdependent, and IT-risk prevention requires them to work together.

Increase in InfoSec issues as well as data privacy concerns

Three in ten (30%) respondents said their organization experienced a data privacy/ cybersecurity breach in the past three years, the most common compliance issue experienced over that period. This is a substantial increase from 2022, when 22% of respondents said their organization had experienced a data privacy/cybersecurity breach over the prior three years.

This increase in self-reported cyberattacks comes as the world of work has shifted dramatically, and permanently, for many organizations. As mentioned in last year's report, there are lingering impacts of the COVID-19 pandemic. One of these is the transition to remote, then hybrid, work models. As noted elsewhere in this report, a striking 93% of respondents said their organization continues to have at least some employees working remotely. This hybrid work model introduces ethical concerns – think quiet-quitting or unauthorized "moonlighting." But it also introduces InfoSec issues that require more or different employee training to mitigate risks. Compliance and IT must be partnered and fully aligned to ensure employees adhere to expected ethical standards and observe data security procedures in the new remote and hybrid-work environment.

Compliance issues in the past three years



BASE: ALL QUALIFIED RESPONDENTS (n=1,315)
Has your organization experienced any of the following compliance issues in the past 3 years? Please select all that apply.

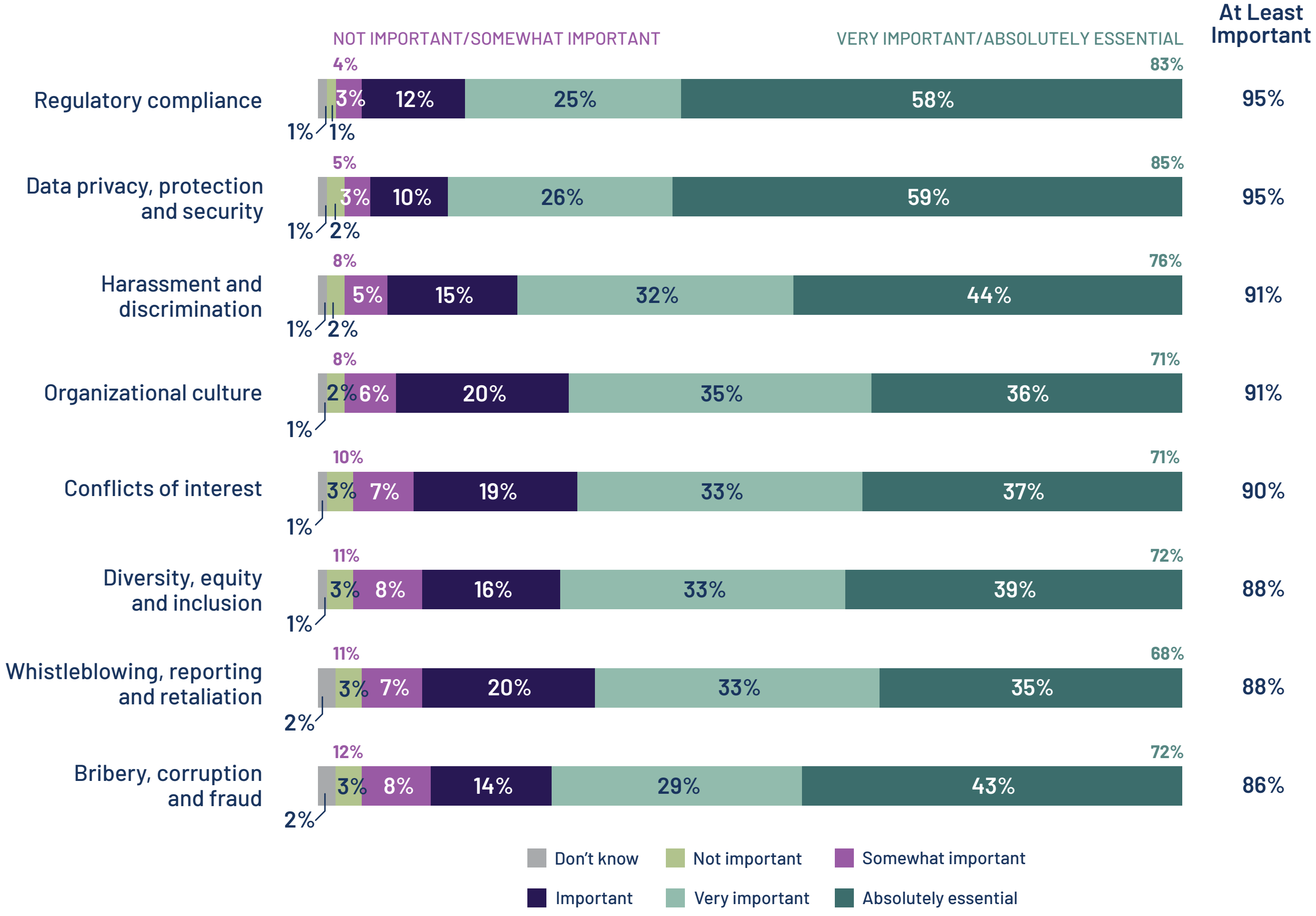
As in years past, respondents rated *Data Privacy, Protection & Security* at effectively the same level of importance as *Regulatory Compliance* in 2023. Specifically, 59% of respondents ranked the data privacy issue at the highest-possible priority level of *absolutely essential* while 58% of respondents ranked *Regulatory Compliance* at the highest priority level.

This finding holds true across the geographic areas of focus for this report, with France, Germany, the United Kingdom and the United States all showing alignment with data privacy and regulatory compliance in the top areas of priority for organizations, though those in the U.S. appear to place even greater importance than their European counterparts.

In our opinion, this alignment of priorities tracks with recent cybersecurity predictions by research and advisory firm Gartner® (Gartner Press Release, "Gartner Unveils Top Eight Cybersecurity Predictions for 2023-2024," March 28, 2023. https://www.gartner.com/en/newsroom/press-releases/2023-03-28-gartner-unveils-top-8-cybersecurity-predictions-for-2023-2024): "Organizations are beginning to recognize that a privacy program can enable them to use data more broadly, differentiate from competitors, and build trust with customers, partners, investors, and regulators. Gartner recommends security leaders enforce a comprehensive privacy standard in line with GDPR to differentiate in an increasingly competitive market and grow unhindered."

We think this as an area where Compliance and InfoSec will be working very closely together, with data privacy so high on the list of priorities for Compliance.

Importance of compliance issues to organization



BASE: KNOWLEDGEABLE ABOUT ETHICS & COMPLIANCE (n=977)
How important are the following compliance issues to your organization?

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

InfoSec tops training priorities

In another telling example of InfoSec's priority for Compliance, respondents most commonly indicate that *Cybersecurity* is a planned training topic over the next two-to-three years, narrowly edging out *Ethics and code of conduct training* for the top spot. Interestingly, *Data privacy* was the third-highest planned training, putting it above *Harassment and discrimination*.

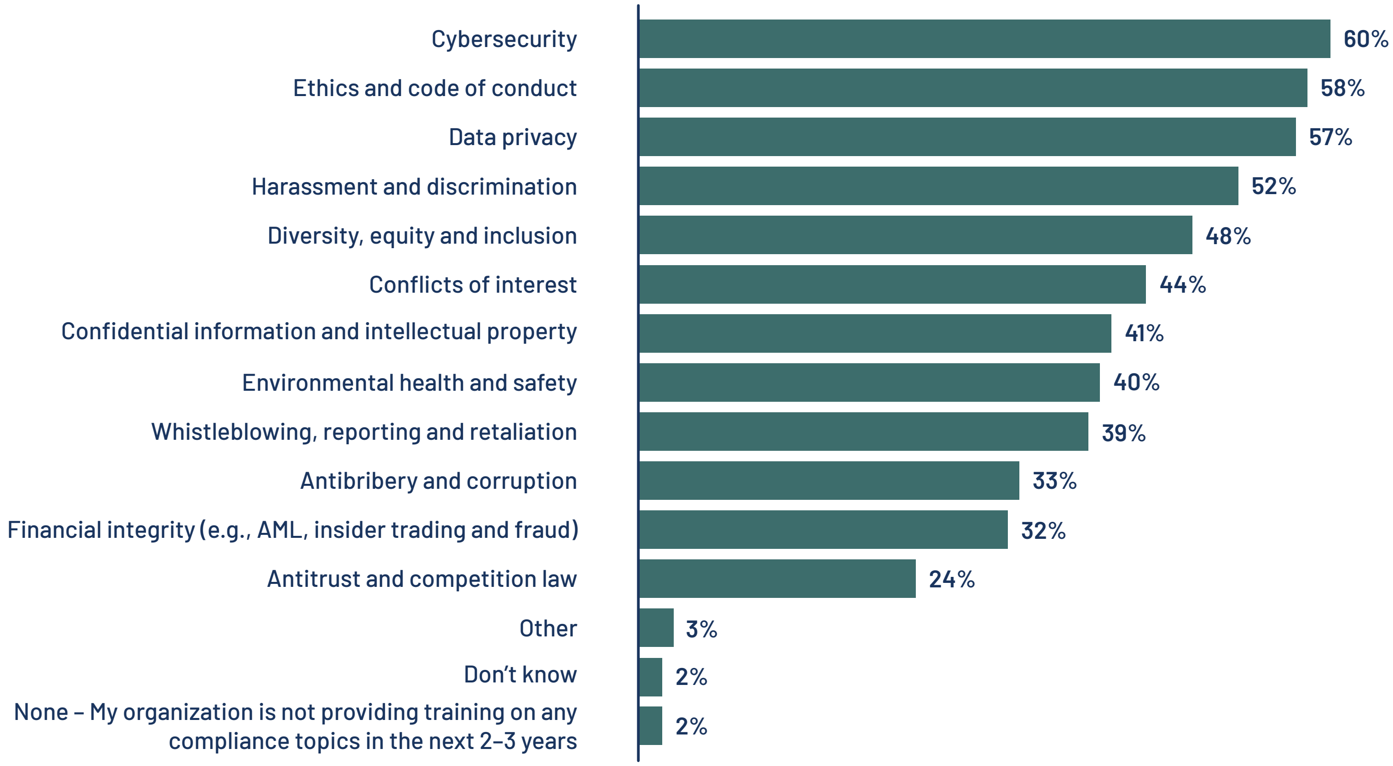
The findings are similar when looking at the breakdown of more granular training subtopics. Forty-nine percent of respondents indicated planned training around *Remote work – cybersecurity*, essentially tied with those saying they planned training around *Sexual harassment* in the next two-to-three years.

Looking at regional data, U.S. respondents were most likely, at 64%, to indicate their organization planned cybersecurity training in the next two-to-three years. Only 47% of respondents in Germany said their organization planned the same, along with 57% from France and 56% from the U.K. Sixty-two percent of U.S. respondents said their organization planned training around data privacy over the same period, compared to 54% in Germany and 46% in the U.K. and France.

This is all fascinating given the fact that Europe has more focus and stringent regulations around data protection than the U.S. from a privacy perspective, but European respondents to this survey seem to indicate less focus on losing the data via breach where data has the highest likelihood of exploitation.

These results reveal a scenario where professionals across different R&C disciplines must collaborate closely to ensure that the training provided is aligned with the organization's specific InfoSec risks.

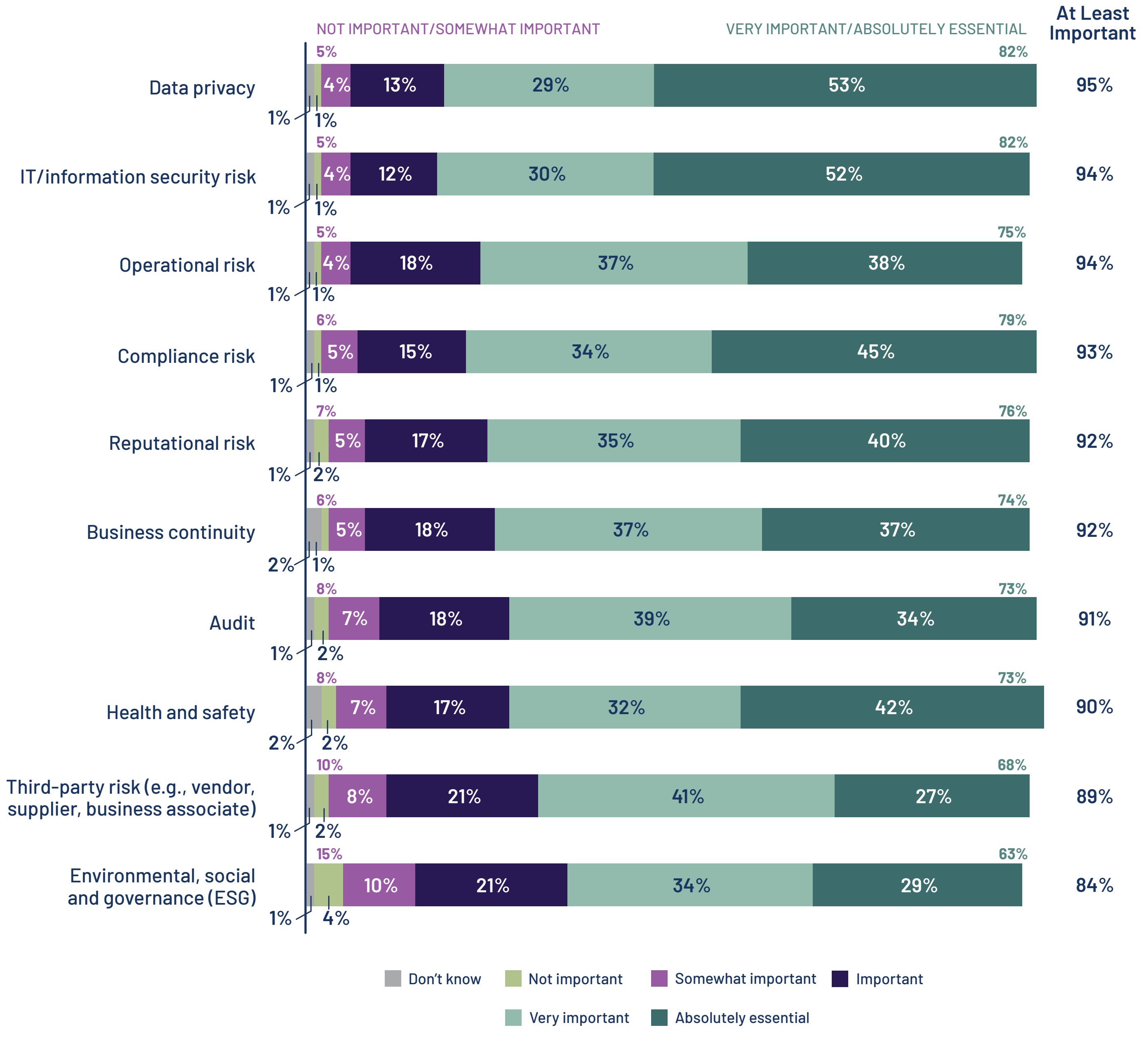
Compliance topics will train on in the next 2-3 years



BASE: KNOWLEDGEABLE ABOUT ETHICS & COMPLIANCE (n=977)
On which of the following compliance topics will your organization provide training in the next 2–3 years? Please select all that apply.

Managing InfoSec risk is essential to business success

Importance of management of risk areas



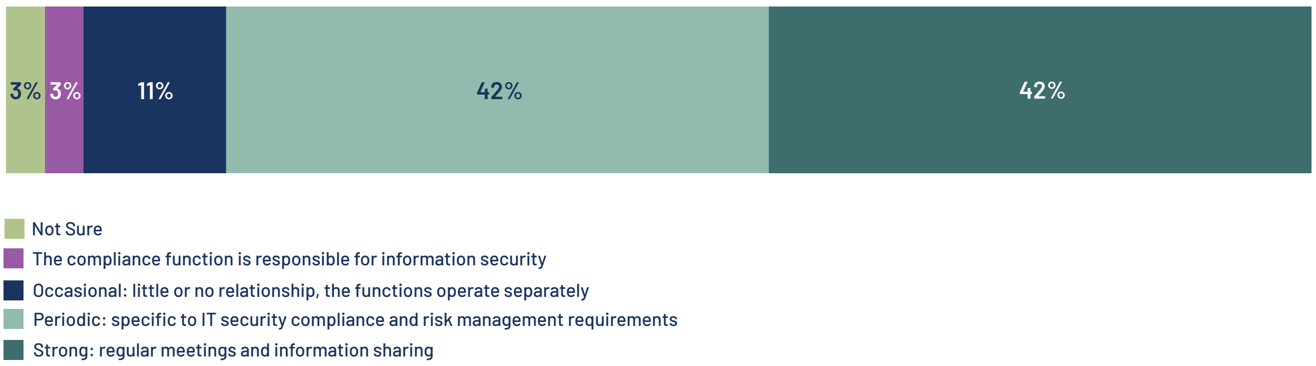
BASE: KNOWLEDGEABLE ABOUT RISK MANAGEMENT (n=1,066)
How important is the management of the following risk areas to your organization?

More than half of respondents said managing *Data privacy and IT/information security risk* were *absolutely essential* to their organization. Again, this puts InfoSec at the top of the priority list, above *Operational risk* and *Compliance risk*.

The importance of InfoSec risk, data privacy and its implications for R&C professionals cannot be overstated. The necessity of Compliance working closely with the IT/ InfoSec function is crucial and will only grow in importance. Fortunately, more than two-fifths of respondents (42%) said the relationship between Compliance and IT was *strong* in their organization. The same proportion said the relationship was *periodic*, and driven by specific IT security risk compliance requirements. While there is always room for improvement, this does mean 84% of respondents indicate there is strength in the Compliance and InfoSec relationship – an encouraging sign. Looking at regional differences, respondents in Germany were less likely to say their Compliance and InfoSec relationship was *strong*, with only 28% indicating such a dynamic.

Going forward, interdependence between IT and Compliance will only increase. Noting that a key focus of strong compliance programs is to support a strong culture, successful companies will embrace cybersecurity and data protection as part of their culture, just like the expectation of ethical behavior and adherence to company policies. By closely coordinating the efforts of the CCO and CISO, organizations can better manage risk, address privacy regulations, and create a cohesive culture.

Compliance function's relationship with Information Security



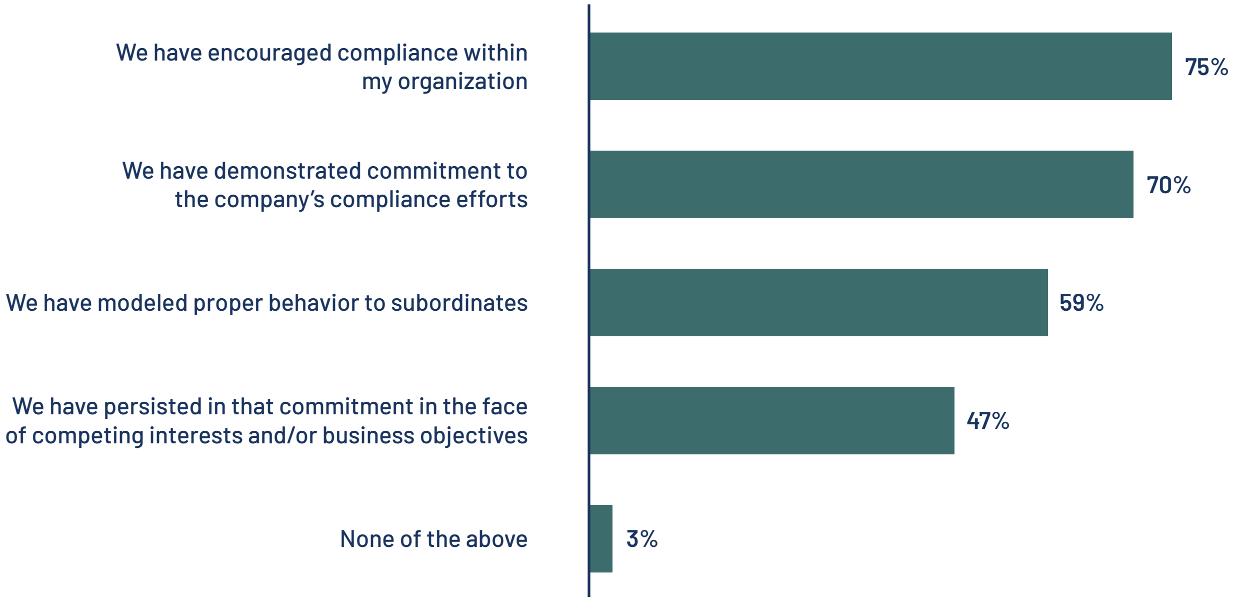
BASE: ALL QUALIFIED RESPONDENTS (n=1,315)
Which of the following statements best describes compliance function's relationship with the information security function / Chief Information Security Officer (CISO) at your organization?

3 Senior management commitment to ethics and compliance

Findings from this year's survey show that most respondents believe their senior leaders take their role in encouraging compliance seriously. Three-quarters of respondents indicated that senior leaders encourage compliance within the organization, and nearly as many report that senior leaders demonstrate their commitment to compliance to employees. Overall, this is an encouraging sign to see senior leadership holding strong in their commitment to compliance.

However, the disconnect between the demonstrated commitment to compliance efforts, and the persistence of this commitment in the face of competing interests and business objectives, continues as we have seen in past surveys. While overall, 70% of respondents said senior leaders demonstrated a commitment, only 47% said the commitment persisted in the face of competing interests or objectives. It is also notable that, while 52% of U.S. respondents said senior leaders persisted in their commitment in the face of competing interests, only 33% in France, 34% in Germany and 41% in the U.K. said the same.

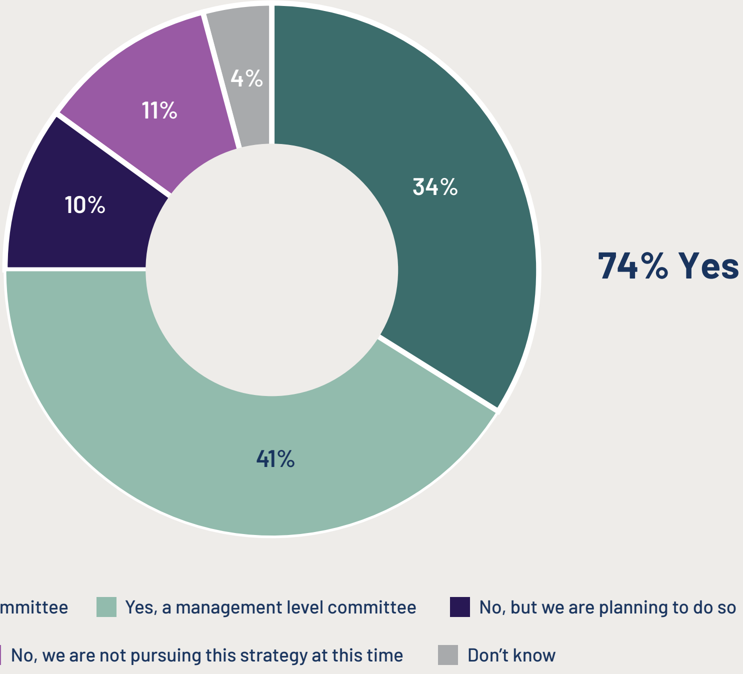
Senior leadership role in compliance



BASE: KNOWLEDGEABLE ABOUT ETHICS & COMPLIANCE (n=977)
Which of the following statements are true about your organization's senior leadership? Please select all that apply.

As another reflection of leadership's commitment, a combined 74% of respondents indicated their organization had established a board- or management-level committee to address enterprise-wide risk integration, (34% and 41% respectively). Leadership seems to be prioritizing this issue.

Have a committee to address risk integration enterprise-wide

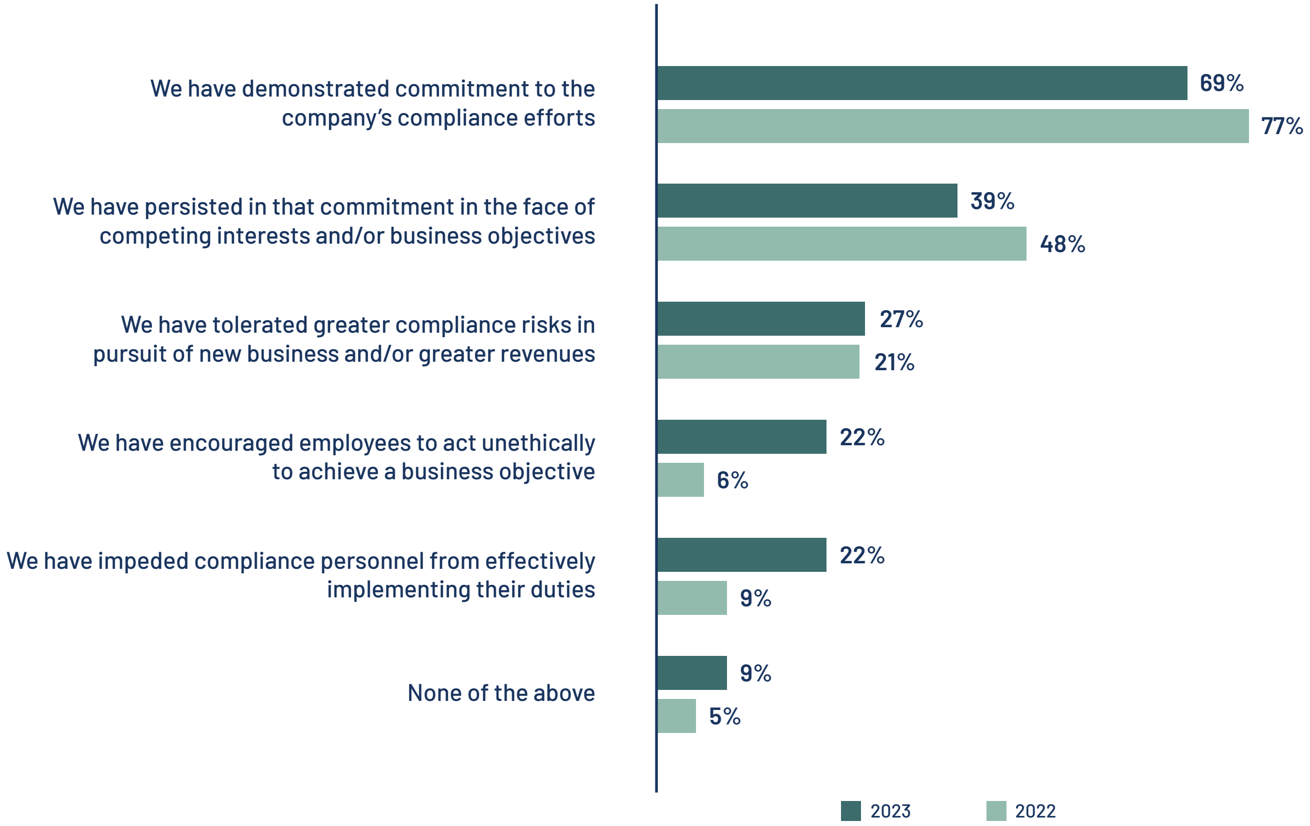


BASE: KNOWLEDGEABLE ABOUT RISK MANAGEMENT (n=1,066)
Does your organization have a committee to address risk integration enterprise wide?

Management's declining commitment is a red flag

While senior management commitment to ethics and compliance is encouraging, it appears that this commitment is somewhat lower among mid-level management, as all measures in this area have slipped compared to 2022.

Management role in compliance



BASE: KNOWLEDGEABLE ABOUT ETHICS & COMPLIANCE (n=977)
Which of the following statements are true about your organization's managers? Please select all that apply.

Specifically, respondents indicated that, among management, "commitment to compliance efforts" and "commitment in the face of competing interests" dropped by 8 and 9 percentage points respectively. The data also suggests that organization's *tolerance* for greater compliance risk, unethical behavior and impediments to compliance personnel all increased in 2023 – in some cases by as much as 16 percentage points.

Interestingly, respondents in Germany were much more likely to call out negative behaviors among managers – 45% said managers tolerated greater compliance risk in the pursuit of business objectives; 39% said managers encouraged employees to act unethically; and 44% said managers impeded compliance personnel from doing their duties.

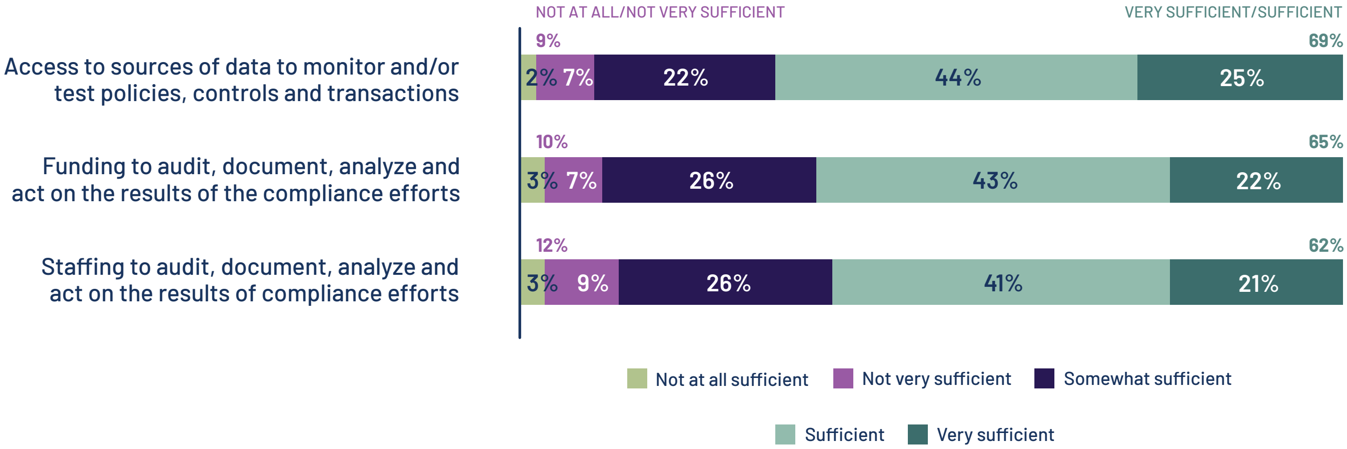
This dissonance between perceived leadership commitment to compliance and what respondents say is the behavior at the mid-manager level is concerning, especially given the precipitous drop seen in the 2023 data. One possible explanation is that managers feel unusually high pressure from leadership to reach business objectives, while executive leadership is unaware of the ethical and/or compliance compromises being made to achieve those objectives.

4 Access to and use of cross-functional data

This year, respondents indicated there is plentiful data available to help successfully inform and operate their risk and compliance program. Yet the extent to which organizations are efficiently leveraging that data to achieve desired outcomes is a more complicated story.

A substantial majority of respondents (69%) said their *access to sources of data to monitor and/or test policies, controls and transactions* was either *sufficient* or *very sufficient*, the top two options to indicate positive performance. Only 9% said their access was either *not at all sufficient* or *not very sufficient*, the lowest of the options.

Organization program access

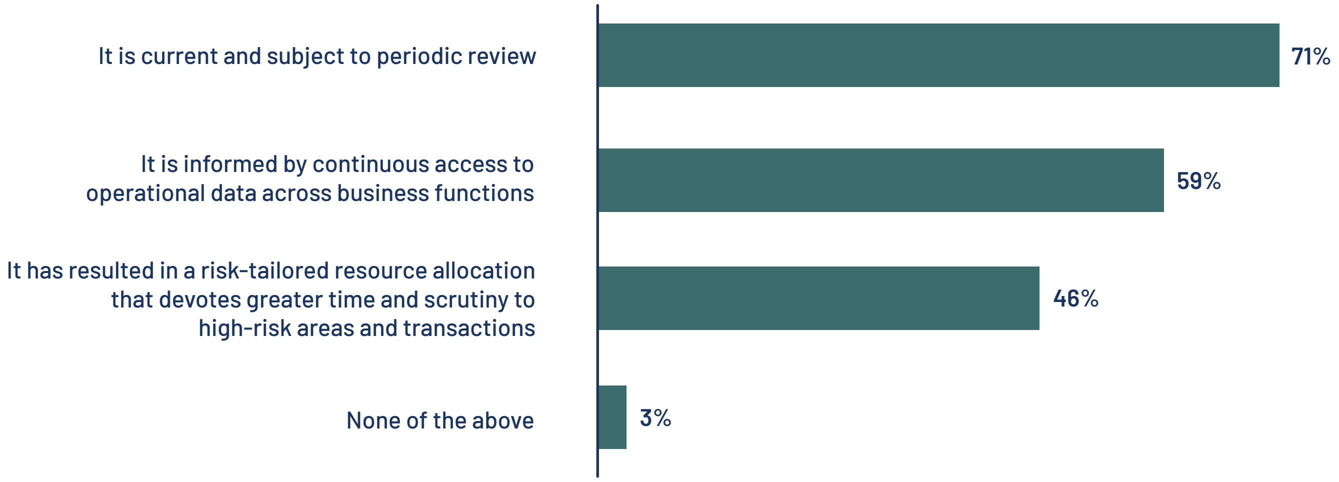


BASE: KNOWLEDGEABLE ABOUT ETHICS & COMPLIANCE (n=977)
How would you rate your organization's program access to each of the following?

It is good news that most respondents feel they have sufficient access to needed data. Today's digital-oriented, dispersed and supply chain-dependent business operations require risk and compliance professionals to have visibility and influence over far-flung aspects of the organization.

Separately, 59% said their risk assessment is informed by continuous *access to operational data across business functions*. This is a slightly different framing than the question regarding overall access to data – risk assessments involve the reconciliation of different "languages" of risk across different business units, making it uniquely complex. Again, it is good to see most respondents indicating that their risk assessment benefits from visibility across those silos. Seven out of ten also said their risk assessment is kept current and subject to periodic review.

Organization risk assessment

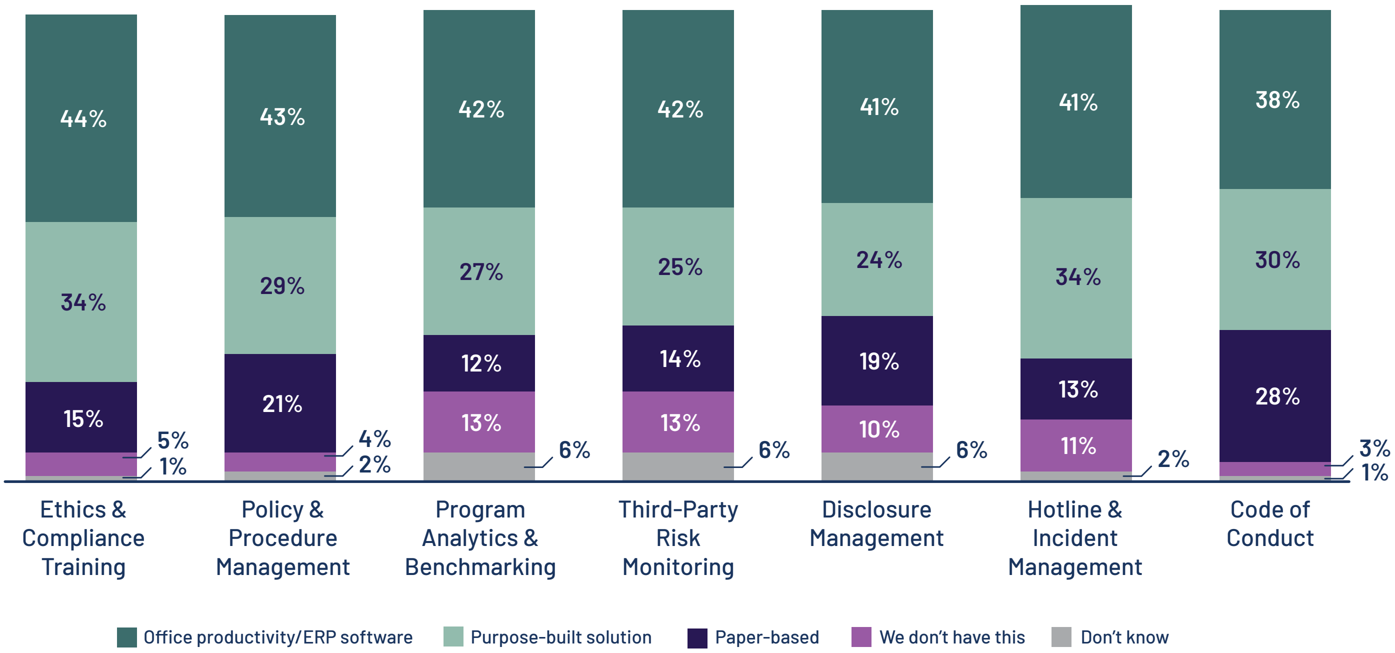


BASE: ORGANIZATION USES RISK ASSESSMENT RESULTS (n=666)
Which of the following are true about your organization's risk assessment? Please select all that apply.

While these findings suggest that nearly 7 out of 10 respondents feel they have access to the data their programs need, far fewer indicate they have a purpose-built solution to administer various program aspects. *Ethics & Compliance Training* and *Hotline and Incident Management* are most likely to have a purpose-built solution (34%), *Disclosure Management* and *Third-Party Risk Monitoring* ranked the lowest (24% and 25% respectively). Depending on the program element, between 12% and 28% are still using a paper-based method to manage the data.

This makes it difficult for a substantial number of programs to efficiently manage, analyze and leverage the operational data they are bringing in. This results in a lost opportunity to increase efficiency and program impact, which can only be achieved through automation. Respondents at larger organizations – those with 5,000 or more employees – were consistently more likely than those at smaller firms to indicate their program used a purpose-built solution.

Administration of E&C program elements



BASE: KNOWLEDGEABLE ABOUT ETHICS & COMPLIANCE (n=977)
How does your organization primarily administer the following Ethics and Compliance program elements?

As noted in our section on program maturity, nearly 20% of respondents said their compliance function is spread across multiple departments. While the consolidation of compliance into a single, dedicated business function will continue to vary, the endurance of these distributed operating models further highlights the value of effective data analysis capabilities.

Looking toward the future, it appears that most respondents feel they have the resources to achieve their goals around data access and utilization. Sixty-five percent of respondents said they had either *sufficient* or *very sufficient* funding to audit, document, analyze and act on the results of compliance efforts. A similar share said the same for their access to staffing.

5 Post-COVID hybrid work model

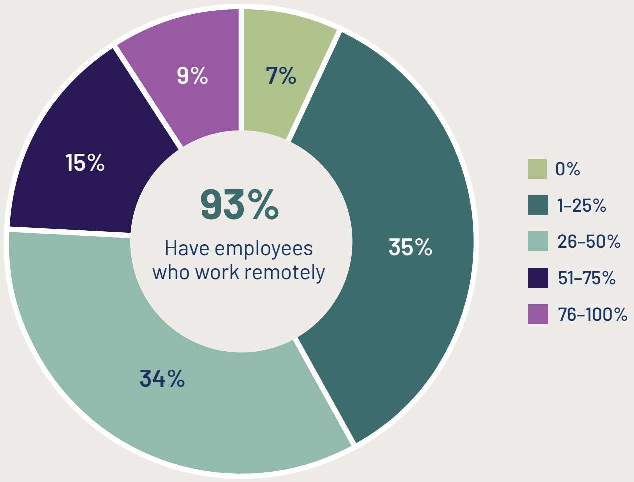
Now that the most disruptive period of the COVID-19 pandemic appears to be behind us, organizations have had the opportunity to assess its impact on the workplace. Most significantly, the transition to remote work at the beginning, and the endurance of a hybrid model now.

Last year, 30% of survey respondents indicated their organizations would likely return to in-office working conditions. An additional 56% predicted a hybrid, in-office/work-from-home scenario. This year, fully 93% of respondents said their organization is now implementing at least a hybrid work model, if not fully remote.

These dynamics are extremely important for R&C professionals. Remote workers are typically under less direct supervision, which could make it more difficult to observe policy and code of conduct violations or other undesired behaviors. It also, as noted earlier, presents more IT security risks.

Further, reporting patterns are also affected. For example, "open door" reporting is difficult for remote workers. Remote and hybrid work may also play a role in motivating employees to use the internal reporting system more. According to NAVEX's 2023 Hotline & Incident Management Benchmark Report, this past year's reporting levels were the highest ever at 1.47 per 100 employees.

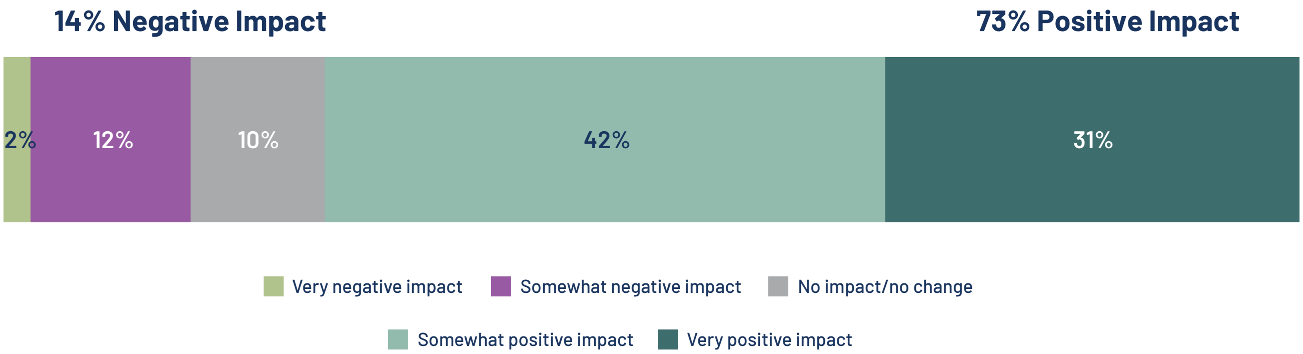
Currently working remotely



BASE: ALL QUALIFIED RESPONDENTS (n=1,315)
What percentage of your organization's employees currently work remotely?

With respect to remote work's effect on corporate culture, the news continues to be good. Last year, 62% of respondents said this flexible working arrangement, work-from-home or hybrid had a positive impact on workplace culture. This year, nearly three-quarters (73%) say it has a *somewhat* or *very positive* impact. Another 10% feel the work-from-home model had no impact, and only 14% said the shift has been negative. Respondents in France and Germany were most likely to cite either a "somewhat positive" or "very positive" cultural impact from work-from-home, at 83% and 79% respectively.

Impact work-from-home models had on workplace culture



BASE: ORGANIZATION'S EMPLOYEES CONTINUE TO WORK REMOTELY (n=1,222)
How much of a positive or negative impact have work-from-home models had on your workplace culture overall?

6 Despite regulatory pressure, Europe lags U.S. in focus on retaliation protection

The much-discussed EU Whistleblower Protection Directive, meant to protect whistleblowers who report misconduct from retaliation, is currently in implementation across all member states. Yet despite this regulatory pressure, survey responses paint a puzzling picture – that compared to respondents in the U.S., European respondents indicated relatively lower prioritization of non-retaliation, whistleblowing and related program elements.

More the half of all respondents indicated that *Whistleblowing, Reporting & Retaliation* was either a *very important* or *absolutely essential* compliance issue for their organization, with the following distribution in select countries: U.S. 71%, U.K. 66%, France 60%, Germany 59%.

Experienced R&C professionals know that a strong non-retaliation policy is necessary for a reporting program to work. However, only 61% of U.S. organizations indicated they had a non-retaliation policy in place as a part of their confidential reporting and investigatory program. In Germany, 41%, followed by the U.K. at 36% and France with only 27% indicating there is a non-retaliation policy at their organization.

Issue rated very important or absolutely essential to the organization	TOTAL	France	Germany	U.K.	U.S.
Whistleblowing, reporting and retaliation	68%	60%	59%	66%	71%

Select policies implemented	TOTAL	France	Germany	U.K.	U.S.
A non-retaliation policy a part of their confidential reporting and investigatory program	51%	27%	41%	36%	61%
Data privacy included in ESG program	54%	49%	47%	50%	61%
Planning ethics & code of conduct training in the next 2-3 years	58%	38%	45%	49%	66%

Without a strong, well-communicated, trusted non-retaliation policy, reporters may not feel safe using an internal system to report misconduct. This reality cuts across regulatory borders, but the additional pressure of the currently unfolding EU Whistleblower Directive would seem to have prompted a stronger response among EU-located respondents.

A deeper analysis of responses about planned training also raises red flags. Consider that *Ethics & Code of Conduct* training is likely where a non-retaliation policy would be covered. In the U.S., 66% of respondents said their organization planned training in that category in the next two-to-three years. Respondents in Germany said the same at a rate of only 45%, and only 38% of respondents in France said their organization planned *Ethics & Code of Conduct* training over that period.

And, despite nearly 40% of respondents indicating their organization's headquarters was based in Europe, respondents put training on the EU Whistleblower Directive near the bottom overall in terms of their organization's planned training subtopics in the next two-to-three years.

Finally, it is interesting to note that more respondents indicate that their organizations have data privacy included in their ESG program than have a non-retaliation policy as a part of their confidential reporting and investigatory program (as referenced in the earlier charts). The gap is especially wide in Europe. There is a seeming disconnect between the intent of the EU Whistleblower Directive – whistleblower protection – and the focus many organizations are taking.

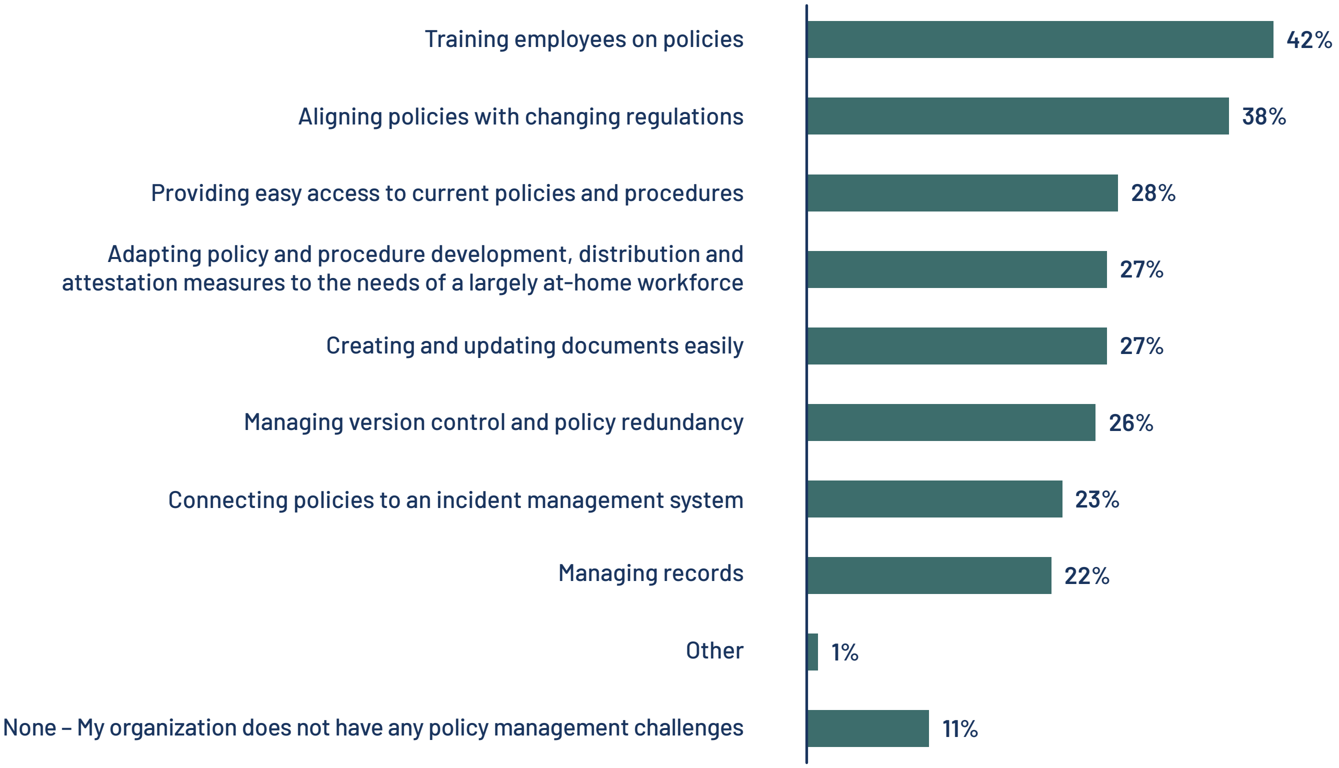
Policy and procedure management

Training on policies remains top – though diminishing – challenge

As in 2022, respondents said *training employees on policies* (42%) and *aligning policies to changing regulations* (38%) were among the top three policy management challenges for their organizations. This comes as no surprise. The pace and complexity of regulatory change seem to accelerate every year, requiring organizations to be increasingly agile to keep up. This shifting landscape also requires organizations to provide increasingly robust employee training at-scale.

This finding shows improvement over 2022 as fewer respondents said training employees on policies was a top policy management challenge in 2023 (42%) versus 2022 (48%).

Top policy management challenges

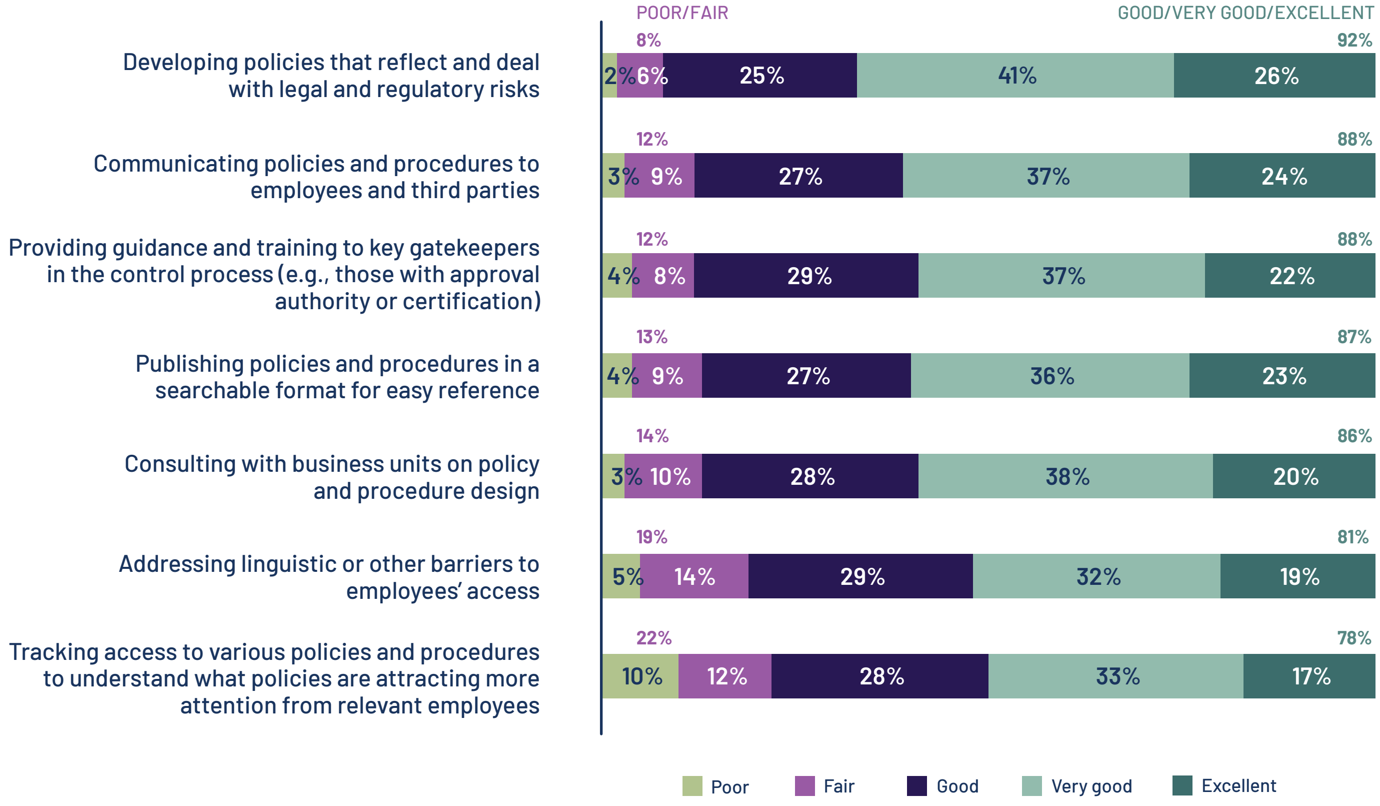


BASE: KNOWLEDGEABLE ABOUT ETHICS & COMPLIANCE (n=977)
What are your organization's top policy management challenges? Please select your top three challenges.

Tracking policy access is most vulnerable performance area

Between 50% and 67% of respondents chose either *excellent* or *very good* to describe their policy and procedure management program's performance across a variety of areas. Tracking access to various policies and procedures to understand what policies are attracting more attention from relevant employees seems to be especially tricky; such tracking can be a useful risk signal to identify areas of employee questions or concerns. Tracking this access is also an expectation of the U.S. Department of Justice in their guidance on Evaluation of Corporate Compliance Programs.[3]

Rating organization's compliance program's performance in terms of policy & procedure management



BASE: KNOWLEDGEABLE ABOUT ETHICS & COMPLIANCE (n=977)
How would you rate your organization's compliance program's performance in the following areas of policy and procedure management?

[3] https://www.justice.gov/criminal-fraud/page/file/937501/download

Key country differences

Some aspects of policy and procedure management rated more positively across different countries, according to respondents. For example, respondents from Germany rated communication of policies to third parties higher than respondents from France. Differences were also evident in the metrics used to measure effectiveness of policy management programs.

Areas of policy and procedure management of an organization's compliance program's performance rated excellent or very good	TOTAL	France	Germany	U.K.	U.S.
Developing policies that reflect and deal with legal and regulatory risks	67%	54%	67%	68%	70%
Communicating policies and procedures to employees and third parties	61%	55%	70%	61%	61%
Addressing linguistic or other barriers to employees' access	52%	47%	68%	50%	51%

Metrics used to measure effectiveness of policy management programs	TOTAL	France	Germany	U.K.	U.S.
Improved efficiencies in completing policy management tasks	39%	55%	44%	33%	38%
Employee accessibility to search and find policies quickly	34%	30%	44%	35%	33%
Policy contribution to improve organizational/ employee culture	34%	26%	41%	41%	33%
Reduction in policy-driven compliance failures	33%	44%	38%	29%	33%
Reduction in legal and regulatory fines	29%	16%	36%	36%	29%

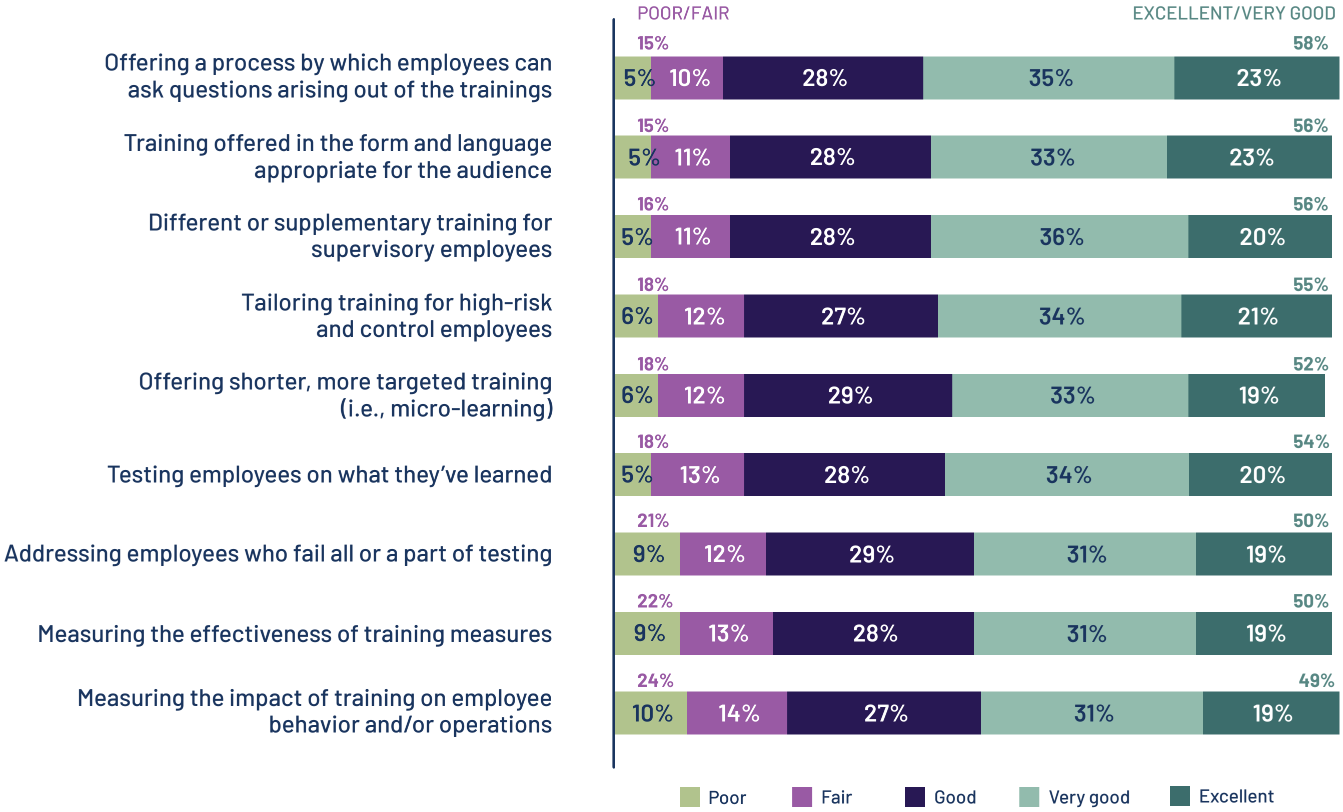
Ethics and compliance training

Many cite weaker protocols in evaluating training impact

A significant majority of respondents indicated that their E&C training programs were at least *good* across different program aspects. As a positive standout, nearly a quarter (23%) rated their program at the top level of *excellent* when it came to offering employees a channel to ask follow-up questions as they arise out of training. The same share rated their program as *excellent* in offering training in a manner and language appropriate for the audience.

Yet looking at the opposite end of the spectrum, nearly a quarter (24%) of respondents said their program was either *fair* or *poor* in measuring the impact of training on employee behavior and/or operations. This is an area where a well-integrated R&C program can have an advantage. Has relevant training impacted the rate of reporting for a particular issue across a certain job class or work site? Has training on incident reporting led to an increase in reporting rates? R&C professionals who can look at these metrics through a cohesive system are more likely to be able to measure the impact of their training.

Rating organization's performance in terms of ethics & compliance training



BASE: KNOWLEDGEABLE ABOUT ETHICS & COMPLIANCE (n=977)
How would you rate your organization's performance in the following aspects of ethics and compliance training?

Key country differences

R&C professionals in Germany were more likely to say their ability to measure the impact of training on employee behavior and/or operations was *excellent* or *very good* than those in France and the U.S. In the U.S., respondents said they were more likely to be offering training on certain high-priority compliance topics in the next two to three years.

Aspects of ethics and compliance training rated excellent or very good	TOTAL	France	Germany	U.K.	U.S.
Measuring the impact of training on employee behavior and/or operations	49%	48%	63%	53%	47%

Compliance topics that organizations will provide trainings for in the next 2-3 years	TOTAL	France	Germany	U.K.	U.S.
Cybersecurity	60%	57%	47%	56%	64%
Ethics & Code of Conduct	58%	38%	45%	49%	66%
Data privacy	57%	46%	54%	46%	62%

Hotline and incident management

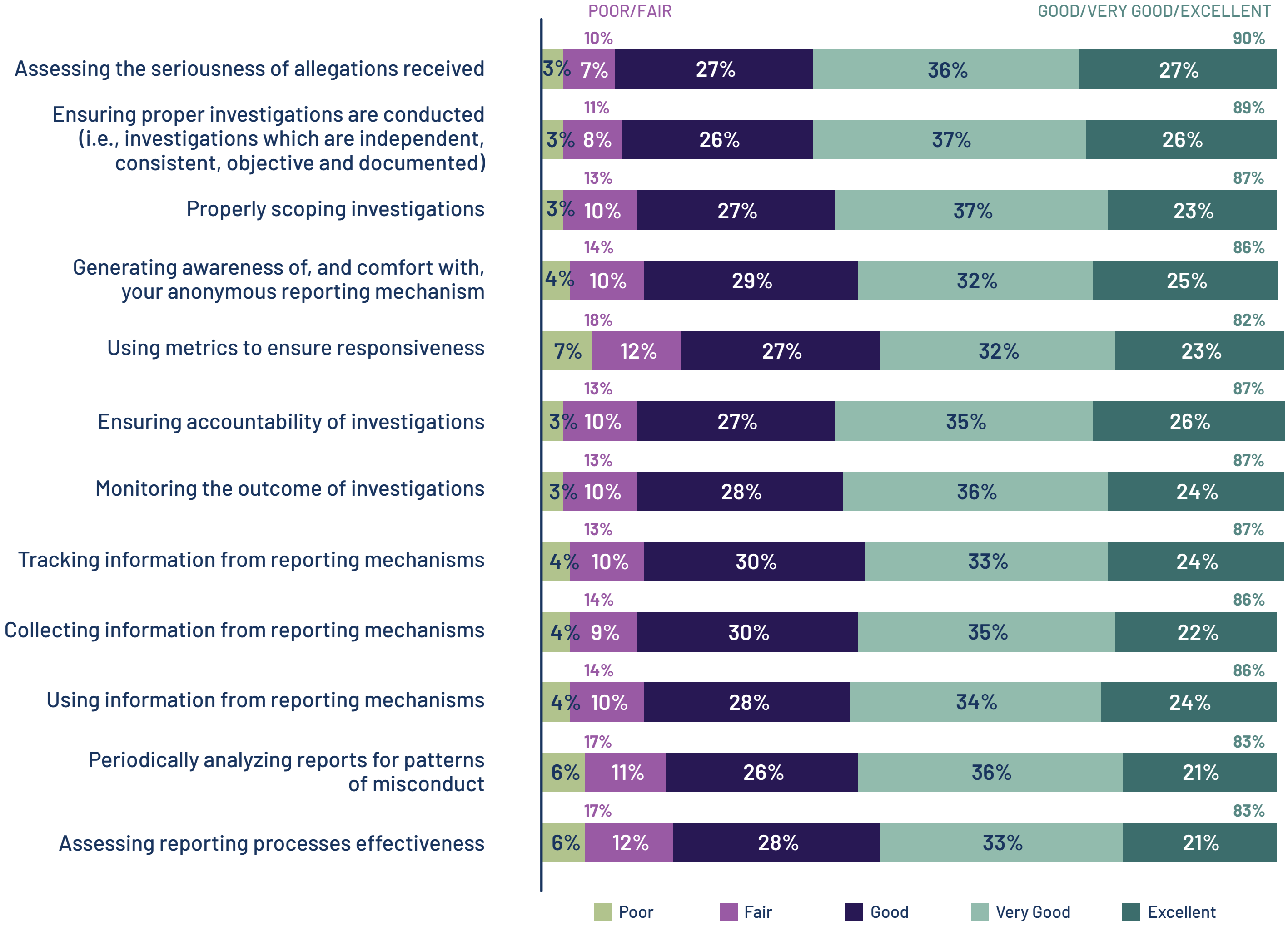
Use of metrics and analytics requires attention and support

A significant majority of respondents said their organization is at least *good* in the various elements of a hotline and incident management program (82-90%). In addition, between 21% and 27% of respondents rated individual program elements at the top level - *excellent*.

A well-functioning, trusted mechanism to receive and investigate allegations of misconduct is a key element of an effective risk and compliance program. Seeing that a significant majority of respondents consider their program elements at least *good* is a very positive signal for our industry.

These findings also show that some programs have an opportunity to increase their positive impact on the organization by moving program elements closer to the *excellent* end of the spectrum. This appears to hold most true for leveraging metrics and data – nearly one-in-five respondents (18%) said their program was either *poor* or *fair* in "using metrics to ensure responsiveness." For those looking to better understand how to measure and benchmark their hotline and incident management programs, NAVEX's 2023 Hotline & Incident Management Benchmark Report provides extensive guidance.

Rating organizations compliance program performance in terms of hotline and incident management



BASE: KNOWLEDGEABLE ABOUT ETHICS & COMPLIANCE (n=977)
How would you rate your organization's compliance program's performance in the following aspects of hotline and incident management?

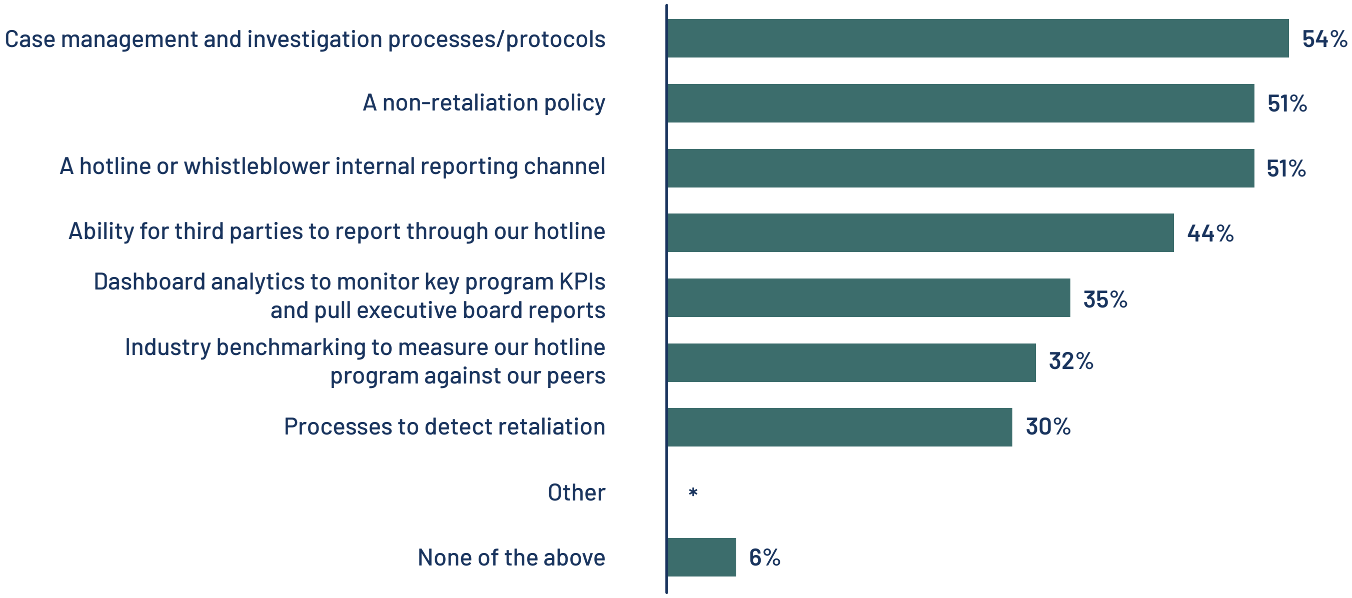
Non-retaliation policies and hotlines are absent from half, a sharp erosion over last year

About half of respondents to this year's survey did not list a non-retaliation policy or a hotline or a whistleblower internal reporting channel as an aspect of their program. This is an increase over last year, possibly because a larger proportion of respondents this year came from the EU and U.K. where many programs are still in the developing phase.

Respondents from larger organizations – those with 5,000 employees or more – were more likely to respond as having an internal reporting channel in place (60%). Only 46% of respondents at smaller organizations said the same. As described in NAVEX's 2023 hotline benchmark report, smaller organizations actually see *higher* overall reports per 100 employees than larger ones – a well-implemented hotline and incident management program is an expected program element.

R&C professionals in the U.S. were more likely than their European peers to report having a hotline or whistleblower internal reporting channel, at 57% which is actually quite surprising in 2023. The next-highest rate was for respondents in Germany, at 44%. Respondents in France were the least likely, at 34%. Also concerning, as noted earlier, is that nearly half of organizations do not have a non-retaliation policy even though many countries have, or are passing, regulations designed specifically to protect whistleblowers from retaliation.

Confidential reporting and investigations

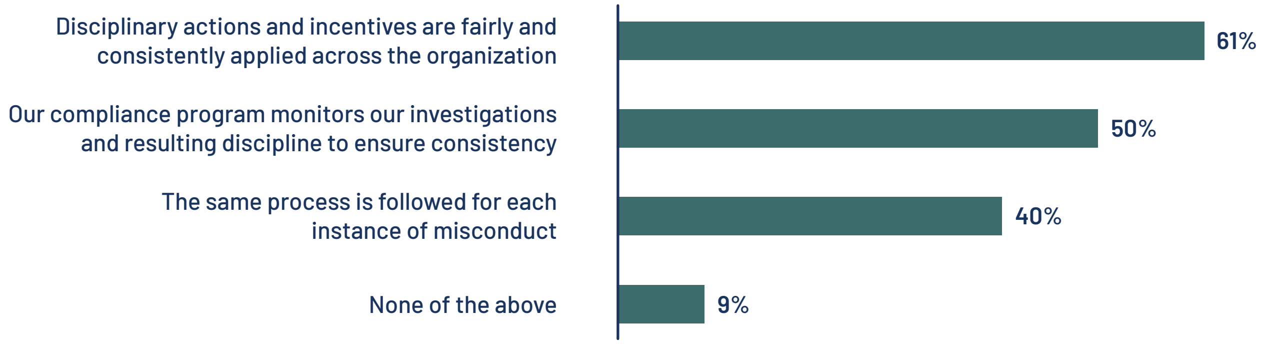


BASE: KNOWLEDGEABLE ABOUT ETHICS & COMPLIANCE (n=977)
Which of the following are part of your organization's confidential reporting and investigatory program? Please select all that apply.

Disciplinary actions are not always applied fairly

Consistency in discipline is one measure employees use when determining their level of trust in their organization. However, only 61% of respondents say that disciplinary actions and incentives are fairly and consistently applied across their organization, and far fewer, 40%, said the same process is followed for each instance of misconduct. It's possible this is due to the structure in place; only half of respondents said their organization's compliance programs are in charge of monitoring investigations and can therefore influence the resulting discipline to ensure consistency.

Organization disciplinary process



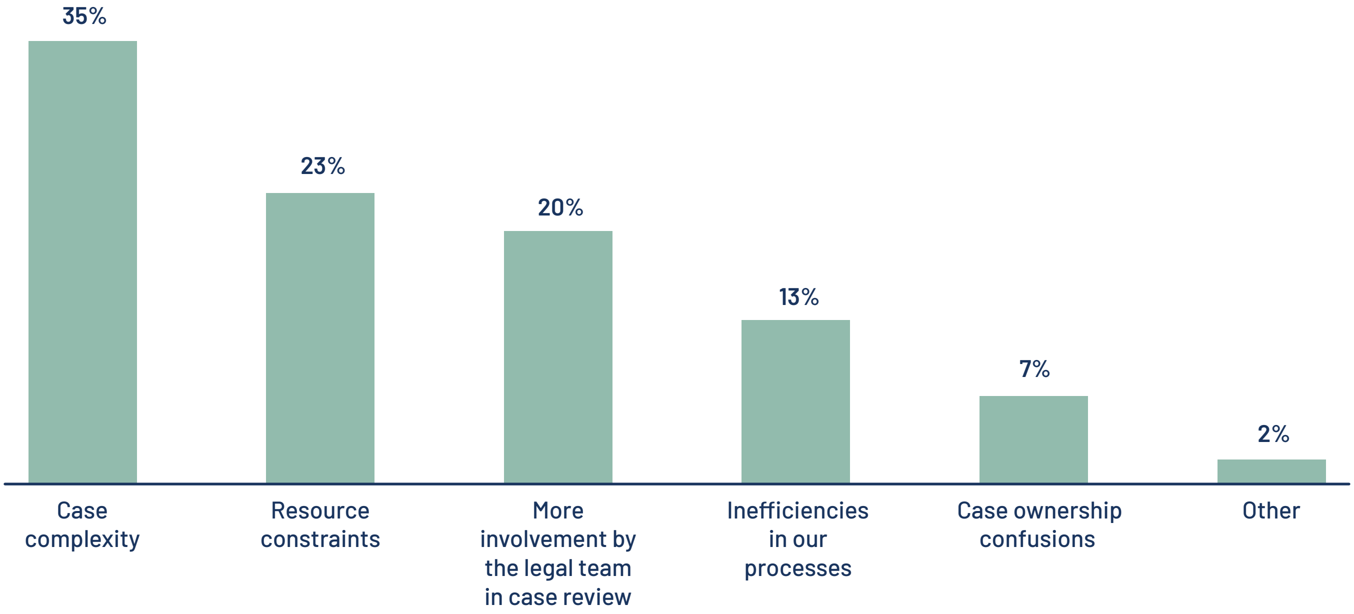
BASE: KNOWLEDGEABLE ABOUT ETHICS & COMPLIANCE (n=977)
Which of the following statements accurately describe your organization's disciplinary process? Please select all that apply.

Legal team involvement is rising as an obstacle in closing cases

The time it takes to investigate and close a case is another metric that employees and others look to when assessing their level of trust for an organization and the effectiveness of it ethics and compliance program. Closing cases efficiently indicates that an organization takes allegations of misconduct and investigations seriously. Like last year, case complexity (35%) and resource constraints (23%) are most commonly cited as having the biggest impact on the time it takes to close a report.

Interestingly, and perhaps reflective of the larger European sample, *more involvement by the legal team in case review* is also an increasingly salient data point. This answer rose significantly by almost three-fold year-over-year, from 7% to 20%. Respondents in Germany were most likely to cite this as their top obstacle, at 31%. France respondents still pushed up the average, with 24% citing this as their top issue. Yet even in the U.S., 18% of respondents chose this option in 2023. Looking at these rates, a picture emerges that regulatory and legal complexity is a significant current challenge for the operations of risk and compliance programs.

Biggest impact on time it takes to investigate and close a report



BASE: KNOWLEDGEABLE ABOUT ETHICS & COMPLIANCE (n=977)
What has the biggest impact on the time it takes to investigate and close a report in your organization? Please select one.

Key country differences

Respondents in Germany and the U.S. were more likely than their peers in France to rate certain key aspects of their hotline and incident management program as *very good* or *excellent*. Country-specific responses varied in affirming various aspects of an organization's disciplinary process. In the U.S., respondents were more likely to say they possessed certain aspects of a confidential reporting and investigatory program. And in France, respondents were far more likely than those in Germany and the U.K. to cite case complexity as the greatest impact for the time needed to investigate and close a report.

Aspects of hotline and incident management rated excellent or very good	TOTAL	France	Germany	U.K.	U.S.
Assessing the seriousness of allegations received	63%	48%	70%	62%	66%
Properly scoping investigations	60%	47%	70%	58%	62%
Generating awareness of, and comfort with, your anonymous reporting mechanism	57%	47%	65%	56%	58%

Accurate description of organization's disciplinary process	TOTAL	France	Germany	U.K.	U.S.
Disciplinary actions and incentives are fairly and consistently applied across the organization	61%	46%	56%	67%	65%
Our compliance program monitors our investigations and resulting discipline to ensure consistency	50%	46%	71%	42%	49%
The same process is followed for each instance of misconduct	40%	42%	51%	33%	38%

Aspects of organization's confidential reporting and investigatory program	TOTAL	France	Germany	U.K.	U.S.
Case management and investigation processes/protocols	54%	45%	47%	46%	59%
A non-retaliation policy	51%	27%	41%	36%	61%
A hotline or whistleblower internal reporting channel	51%	34%	44%	41%	57%
Ability for third parties to report through our hotline	44%	44%	32%	37%	47%

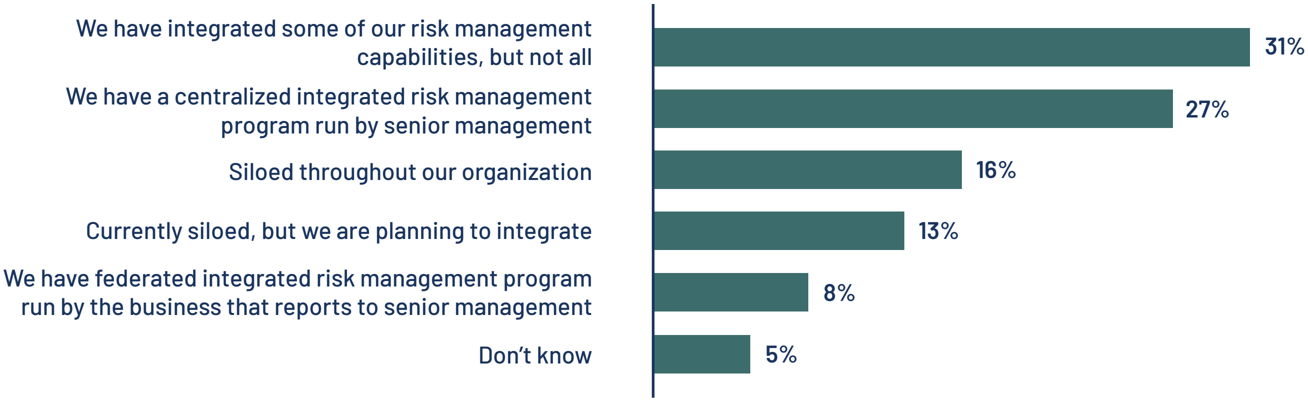
Biggest impact on time it takes to investigate and close a report	TOTAL	France	Germany	U.K.	U.S.
Case complexity	35%	45%	30%	29%	36%
More involvement by the legal team in case review	20%	24%	31%	18%	18%

Integrated risk management and approach to third parties

Integrated risk management remains a work in progress

Integrated risk management describes a cultural, operational and software-driven approach to monitoring risks across the business in a cohesive way. Currently only about one-quarter of respondents (27%) said their organization has a centralized integrated risk management program run by senior management. Another third (31%) said they have integrated some, but not all, of their capabilities. Taken together, this slight majority (58%) have taken steps in the right direction. This percentage is expected to increase as more organizations adopt governance, risk and compliance (GRC) information systems that bring the different functions of risk and compliance into a single platform.

Risk integration management capabilities



BASE: KNOWLEDGEABLE ABOUT RISK MANAGEMENT (n=1,066)
How integrated are your organization's risk integration management capabilities?

Third-party risk management is rated positively, with room to optimize

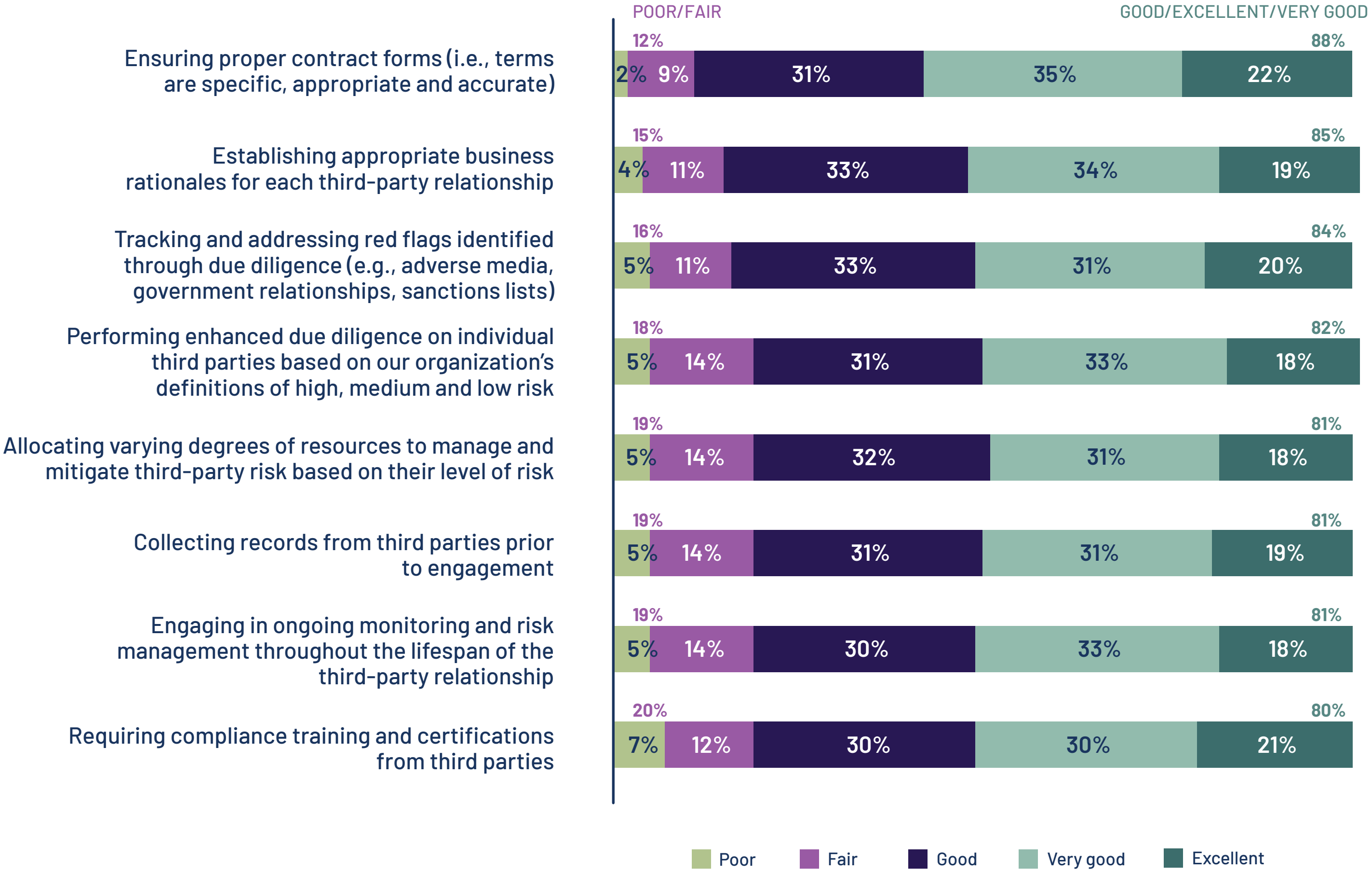
The majority of respondents rate their organization as at least *good* in the various elements of a third-party due diligence program (80-88%). This is a positive sign at a time when even very small organizations can rely on scores of external vendors to accomplish basic business processes that are intrinsic to their operations.

Falling towards the bottom of the list is *requiring compliance training and certifications from third parties*, where a combined 20% of respondents rated their program as either *poor* or *fair*. This is indeed a challenging area, but an important one, as third parties need to operate effectively as an extension of the client organization and should evoke the same ethos and expectations required of internal employees. Still, this is hardly cause for alarm, as 80% of respondents said their organizations are at least *good* in this area.

Respondents from larger companies (5,000 employees or more) were most likely to rate their third-party due diligence program elements as *very good* or *excellent* (55-65%). Only 45-53% of smaller organizations (less than 5,000 employees) said the same across various program elements.

Perhaps not surprisingly given the activation of the German Supply Chain Act in 2023, more than half of respondents in Germany rated their third-party due diligence program elements as either *very good* or *excellent* (53-64%). This included in the area of requiring compliance training and certifications from third parties, with 59% percent of respondents in Germany choosing one of the top-two self-assessment options, compared to 45% in France.

Rating of compliance program's performance of third-party due diligence

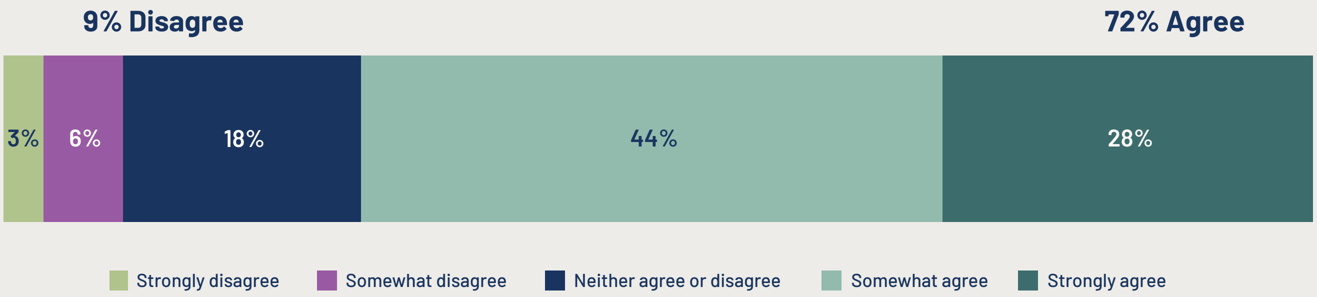


BASE: KNOWLEDGEABLE ABOUT ETHICS & COMPLIANCE (n=977)
How would you rate your organization's compliance program's performance in the following aspects of third-party due diligence?

Organizational approach to third parties varies significantly

In 2023, the majority of respondents (72%) believe their third-party due diligence program significantly reduces their legal, financial and reputational risks.

Our third-party due diligence program significantly reduces our legal, financial and reputational risks

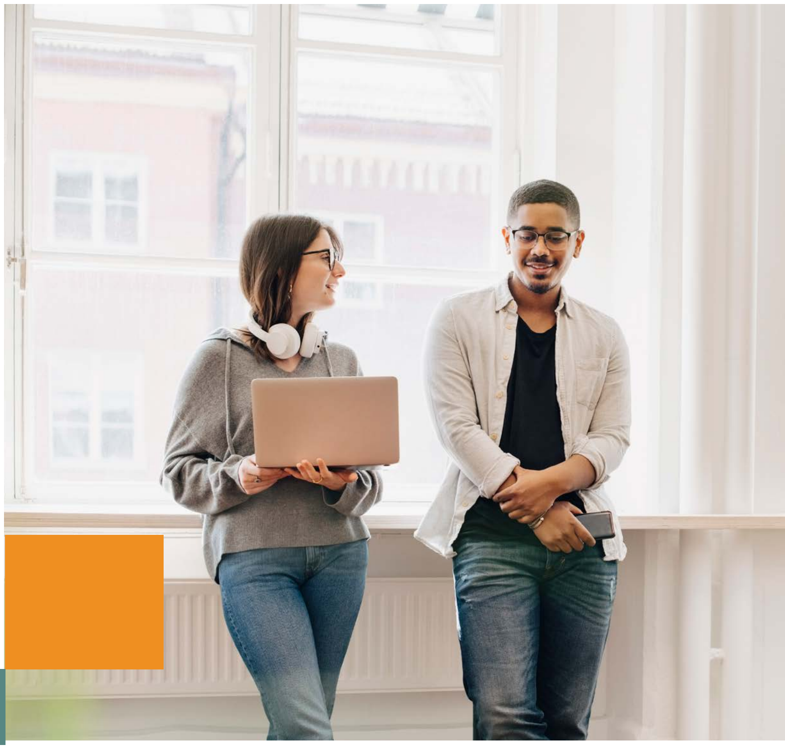


BASE: KNOWLEDGEABLE ABOUT ETHICS & COMPLIANCE (n=977)
Rate your agreement with the following statement: Our third-party due diligence program significantly reduces our legal, financial and reputational risks.

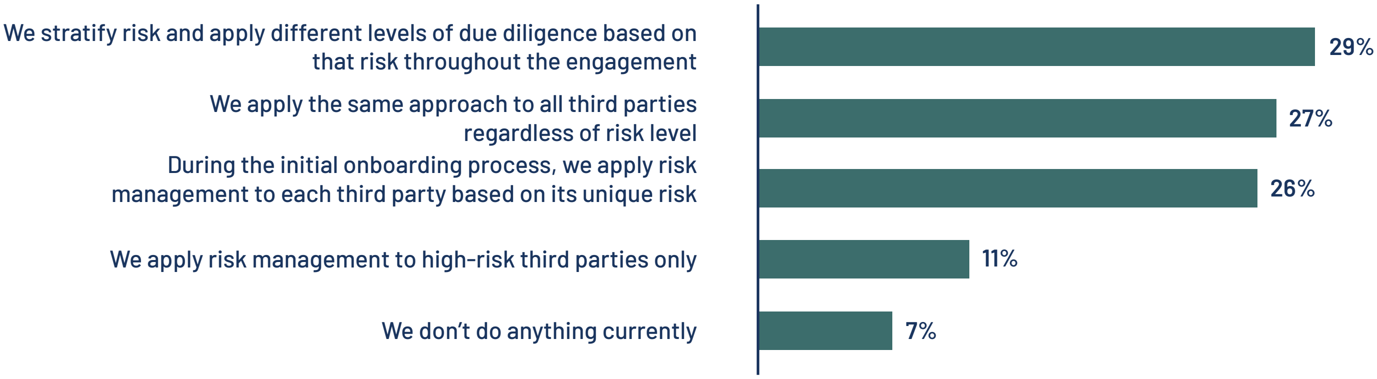
Not surprisingly, there is no universal strategy when it comes to dealing with third parties. Less than 3 in 10 (27%) respondents said their organization applies the same risk management approach to all third parties regardless of risk level. Another 3 in 10 (26%) said their program relies on unique factors during the initial onboarding process. And yet another 3 in 10 (29%) said their organization stratifies risk and applies different levels of due diligence based on risk throughout the engagement.

This latter approach is optimal – applying the appropriate level of resources to monitoring a third party based on the level of risk and extent to which that third party is critical to business operations.

In one positive sign, respondents were less likely to say they don't do anything currently in their approach to third parties compared to last year – 7% in 2023, down from 12% in 2022.



Organizational approach to third parties



BASE: KNOWLEDGEABLE ABOUT ETHICS & COMPLIANCE (n=977)
Which best describes your organization's approach to third parties? Please select one.

Key country differences

R&C professionals in the U.S. and U.K. were more likely than those in France and Germany to cite management of certain key risk areas as *very important* or *absolutely essential*. Respondents in the U.K. France and Germany were more likely than those in the U.S. to say their organization has (or plans to have) a management level or board level committee to address risk integration enterprise wide. Finally, levels of integration for various risk management capabilities varied across countries, according to survey responses.

Management of risk areas as absolutely essential or very important	TOTAL	France	Germany	U.K.	U.S.
Reputational Risk	76%	69%	60%	77%	80%
Operational Risk	75%	73%	63%	78%	77%
Audit	73%	63%	62%	73%	76%

Have a committee to address risk integration	TOTAL	France	Germany	U.K.	U.S.
Yes (management or board level) or plan to	84%	92%	90%	90%	80%

Position responsible for managing risk integration strategy	TOTAL	France	Germany	U.K.	U.S.
Chief Risk and Compliance Officer (CRCO)	18%	23%	28%	23%	14%
Chief Risk Officer (CRO)	15%	17%	13%	22%	14%

Level of integration of risk integration management capabilities	TOTAL	France	Germany	U.K.	U.S.
We have integrated some of our risk management capabilities, but not all	31%	20%	31%	34%	32%
We have a centralized integrated risk management program run by senior management	27%	25%	26%	30%	26%
Siloed throughout our organization	16%	22%	14%	8%	18%
Currently siloed, but we are planning to integrate	13%	25%	15%	12%	10%
We have a federated integrated risk management program run by the business that reports to senior management	8%	7%	13%	9%	7%

Environmental, social and governance

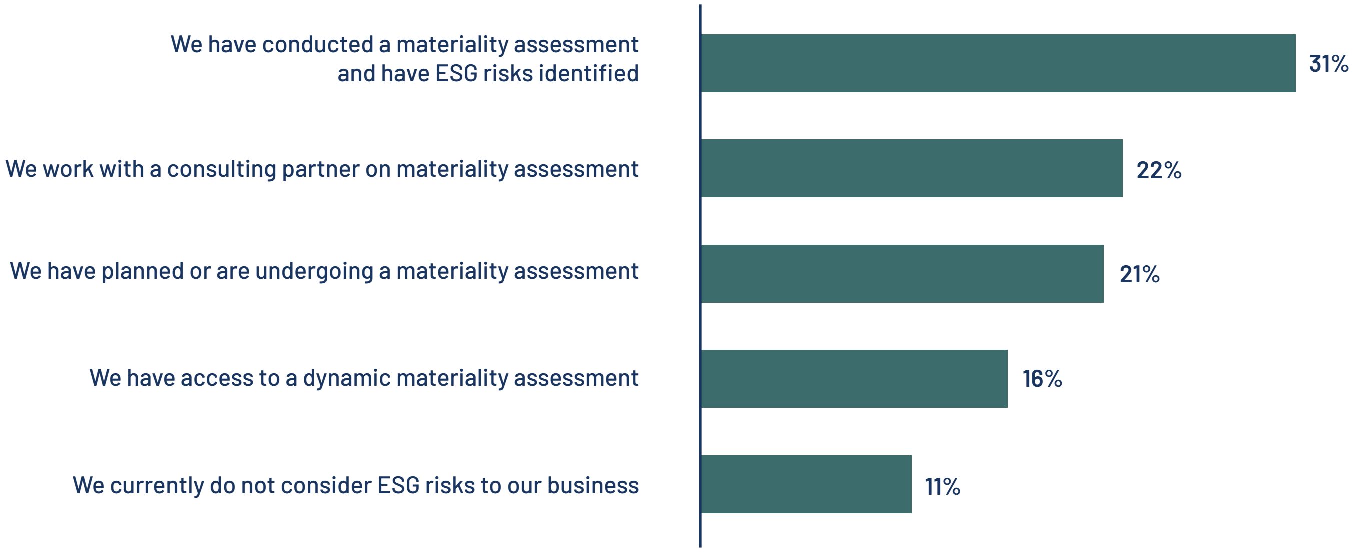
Large majority of organizations are sizing up ESG risks, far more than in the past

Today, nearly one-third of respondents (31%) said their organization has conducted a materiality assessment and has ESG risks identified; one-fifth (22%) said they work with a consulting partner on the materiality assessment; and another one-fifth (21%) said they are currently undergoing/planning a materiality assessment.

Only a small segment (11%) said their organization does not consider ESG risks at all. This is a notably sharp drop from 2022 (31%), which could possibly be explained in part by the inclusion of more European respondents, which tended to indicate ESG as a greater priority, this year. However, it is worth noting that ESG remains a very prominent issue for many U.S. organizations – not to mention their shareholders and customers.

Respondents in the U.S. (84%) were less likely than their European peers to consider *any* ESG risks (84% vs. 97% France and 97% Germany), yet still more than 4 in 5 in the U.S. do.

Determining ESG risks to business

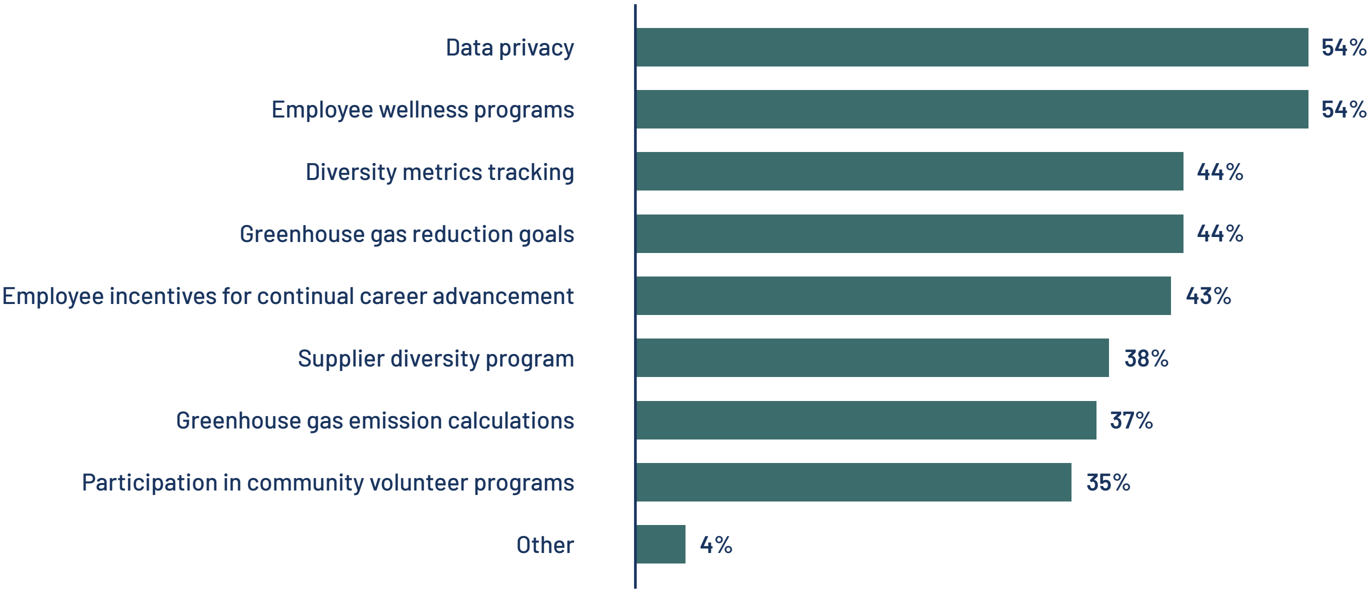


BASE: KNOWLEDGEABLE ABOUT ENVIRONMENTAL, SOCIAL & GOVERNANCE (n=787)
How does your organization determine ESG risks to its business?

HR-centric elements are top ESG activities

Data privacy and employee wellness programs are the most common elements respondents said are included in ESG programs (54% each). These categories speak to the diversity of elements under the broad umbrella of ESG, and given that they are connected with the InfoSec and HR functions, also speak to the need for R&C professionals to discuss risks across silos to support the success of a program. Respondents said supplier diversity is also a part of many ESG programs (38%), which is not surprising given the proliferation of third parties for a typical organization.

Aspects of ESG program



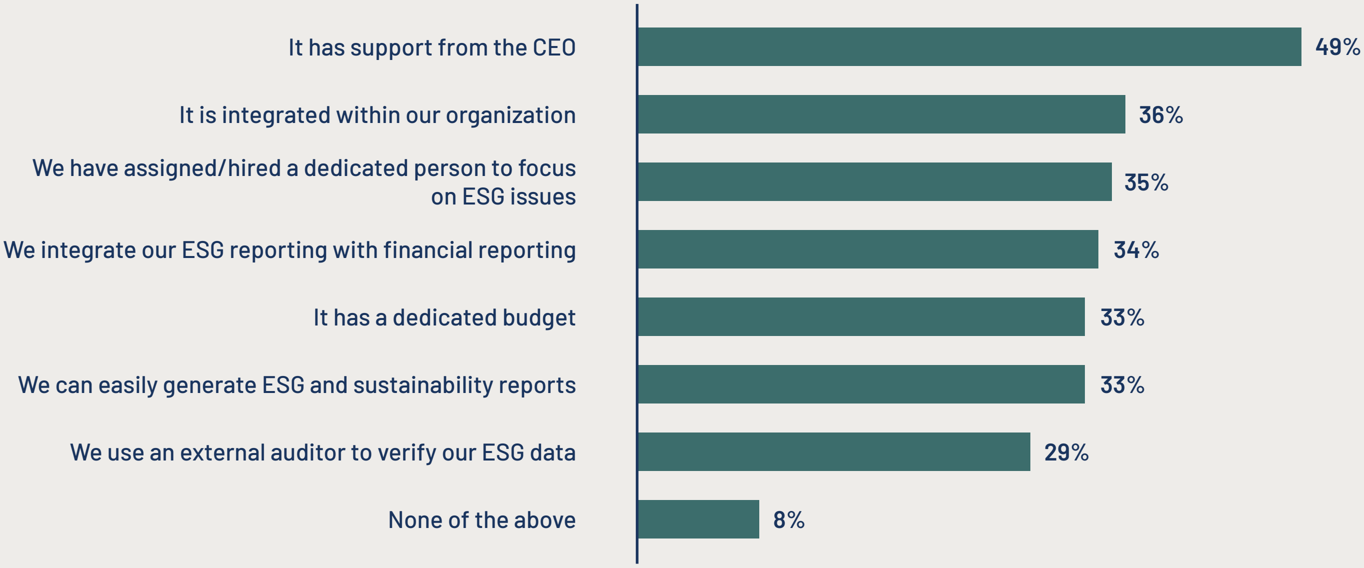
BASE: KNOWLEDGEABLE ABOUT ENVIRONMENTAL, SOCIAL & GOVERNANCE (n=787)
Which of the following are included in your organization's ESG program? Please select all that apply.

Generating ESG reports is still a challenge, but not as much as last year

Only one-third of respondents (33%) indicated that they can easily generate ESG and sustainability reports. This comes as no surprise given the diverse range of data sources that fall under the umbrella of ESG – and the challenge of pulling those inputs together into a cohesive story for internal and external stakeholders. This is a clear improvement over last year when only about 1 in 5 respondents (17%) found it easy to generate ESG and sustainability reports.

As a positive signal, nearly half (49%) of respondents said their ESG program has support from the CEO.

True of organization ESG program

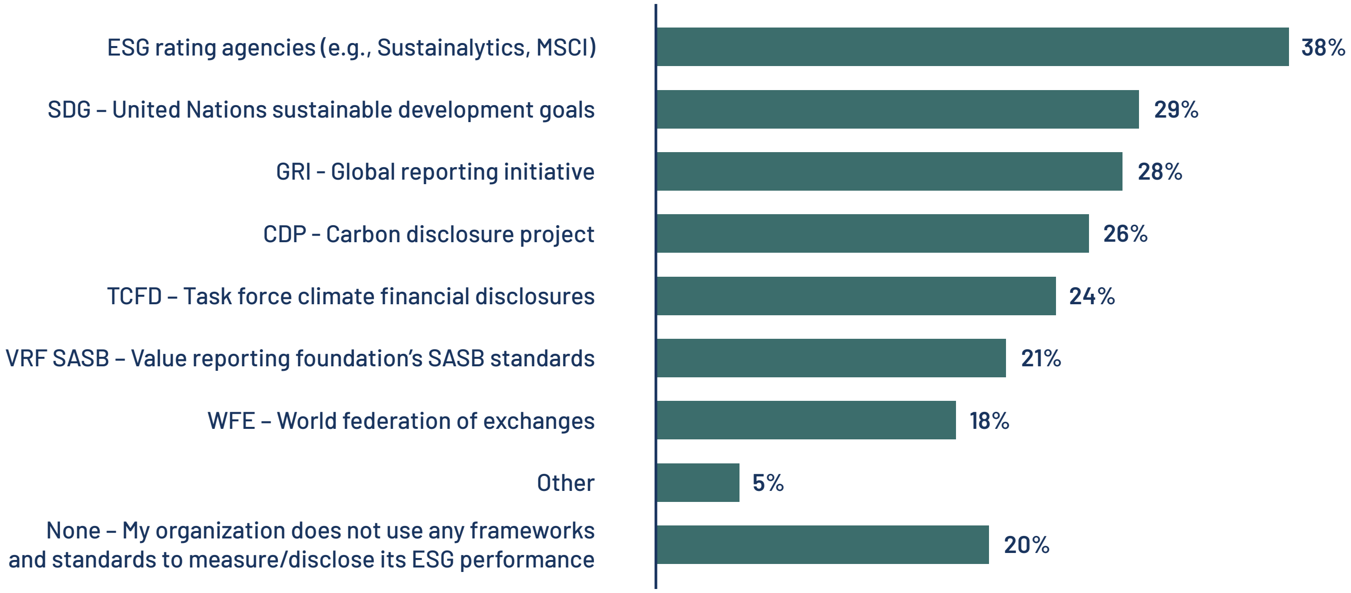


BASE: KNOWLEDGEABLE ABOUT ENVIRONMENTAL, SOCIAL & GOVERNANCE (n=787)
Which of the following are true for your organization's ESG program? Please select all that apply.

ESG performance frameworks are evolving; greater reliance on agencies

As was the case in 2022, survey responses indicate that organizations use a wide range of frameworks and standards to measure and disclose ESG performance. Yet two notable trends seem to be developing. First, the proportion of respondents who said their organizations rely on nothing – no standards and frameworks at all – has dropped considerably, from 48% in 2022 to 20% today. And by contrast, on a sharp incline, nearly two-fifths of respondents to the latest survey (38%) said their organization uses ESG rating agencies (more than double the 17% in 2022). While organizations continue to stitch together a variety of approaches, it appears more consensus may be coming.

Frameworks and standards used to measure/disclose ESG performance



BASE: KNOWLEDGEABLE ABOUT ENVIRONMENTAL, SOCIAL & GOVERNANCE (n=787)
Which frameworks and standards does your organization use to measure/disclose its ESG performance? Please select all that apply.

Key country differences

Respondents in France were significantly more likely than other countries of focus in this study to rate *corporate social responsibility and ESG compliance* as *very important* or *absolutely essential* in their ESG program. Additionally, large majorities in France, and also Germany, said they considered any ESG-related risks as risks to their businesses. Despite these strong signals for ESG in those countries, France- and Germany-based respondents were less likely than those in the U.K. or U.S. to say that their ESG program had CEO support.

Management of environment, social & governance issues as absolutely essential or very important	TOTAL	France	Germany	U.K.	U.S.
Corporate social responsibility	67%	73%	61%	63%	67%
ESG compliance	65%	74%	59%	66%	63%

Determination of ESG risks to business	TOTAL	France	Germany	U.K.	U.S.
Consider any risks	89%	97%	97%	88%	84%

Included in ESG program	TOTAL	France	Germany	U.K.	U.S.
Data privacy	54%	49%	47%	50%	61%
Diversity metrics tracking	44%	35%	28%	48%	51%
Participation in community volunteer programs	35%	21%	30%	29%	42%

True of organization's ESG program	TOTAL	France	Germany	U.K.	U.S.
Has support from the CEO	49%	41%	41%	54%	52%

Frameworks and standards to measure/disclose ESG performance	TOTAL	France	Germany	U.K.	U.S.
Any frameworks or standards	80%	85%	89%	81%	73%

8 Program-specific findings by company size

In recognition of distinct programmatic pressures, NAVEX conducted a special examination of survey data across three organizational size cohorts in 2023. For the purpose of this report, *small* represents organizations with fewer than 5,000 employees, *medium* represents those with between 5,001 and 9,999 employees, and *enterprise* represents those with 10,000 or more employees.

Most results largely followed the overall findings in this report. Yet some showed distinctions for how respondents at small-, medium- and enterprise-sized organizations were assessing their programs, or were notable in themselves for tracking overall global trends. The following points are areas our analysis found to be meaningful in examining each subgroup.

Respondents at small organizations were generally similar to their large-enterprise peers in calling out various program priorities. However, survey results indicated that respondents were less likely to view their programs as mature.

Smaller organizations may have fewer available resources to build out a robust risk and compliance program. It is also important to note that best practice in an enterprise organization may not look the same in a smaller organization. Yet those that have the appropriate size and risk-based infrastructure and practices in place to help development of an ethical and compliant culture for their growing organization will realize a competitive advantage in terms of employee retention, marketplace reputation, and more.

Respondents at enterprise-sized organizations were more likely than those at smaller firms to cite mature practices in various aspects of their R&C programs. This includes planned training around relevant R&C topics, possession of certain key program elements, and likelihood of having a purpose-built solution to accommodate those elements.

That said, larger organizations may to be subject to size and operational thresholds that would trigger various regulatory mechanisms globally – highlighting the importance of program maturity. These larger organizations are more likely, based on respondents, to plan training on whistleblowing, for example – suggesting an awareness around the importance of this critical R&C function.

As might be expected, responses reflecting medium-sized organizations appeared to place them somewhere in the middle in areas such as maturity and likelihood to possess important program elements. Respondents from the medium cohort were more likely to indicate usage of purpose-built R&C solutions than those from small organizations, yet not as likely as those at the enterprise level, for example.

Notable findings

E&C program maturity

- While smaller organizations tend to have fewer available resources for risk and compliance than their large-enterprise peers, nearly half (46%) of small-organization respondents still placed their program in one of the top-two levels of maturity on the ECI maturity spectrum. Respondents at medium organizations were more likely to do so, at 56%. However, respondents at enterprise organizations were far more likely (74%) to categorize their program in those top maturity levels. Only 17% of small-organization respondents said their program was at the highest maturity level of *optimizing*, compared to 24% from medium firms and 37% of responses from enterprise.
- A majority of respondents at small, medium and enterprise organizations alike ranked various compliance issues as *very important* or *absolutely essential*. This included regulatory compliance, data privacy, harassment and discrimination, and organizational culture.
- Enterprise organizations were said to be most likely to possess a purpose-built solution for various aspects of their E&C program than medium or small. This included: *hotline & incident management* (48% enterprise, 34% medium, 29% small); *policy & procedure management* (44% enterprise, 28% medium, 25% small); *third-party risk monitoring* (40% enterprise, 25% medium, 20% small); and *ethics & compliance training* (49% enterprise, 28% medium, 31% small).

Policy and procedure management

- Small, medium and enterprise respondents commonly applied positive ratings to the aspects of their policy and procedure management programs. This includes d*eveloping policies that reflect and deal with regulatory risks*, *communicating policies and procedures to employees and third parties*, and *providing guidance and training to key gatekeepers in the control process*.
- While most still gave their programs positive marks in the area, around one-quarter of enterprise respondents (26%) categorized *tracking access to various policies and procedures to understand what policies are attracting more attention from relevant employees* as either *fair* or *poor*. This was on par with the 19% from medium-sized organizations and 22% from small-sized organizations that said the same. As the most likely policy and procedure management program area to attract some negative self-assessments, challenges here appear to cut across the size spectrum.

E&C training

- Respondents at small-to-medium-sized organizations were generally much less likely than those at large enterprises to cite plans for training around various topics over the next 2-to-3 years. This included *whistleblowing, reporting & retaliation* (34% small, 36% medium, 58% enterprise), *cybersecurity* (57% small, 58% medium, 71% enterprise), *ethics & code of conduct* (56% small, 60% medium, 66% enterprise) and *harassment & discrimination* (50% small, 48% medium, 62% enterprise).
- Survey data showed a similar comparison for planned training on subtopics. For example, small-to-medium organizations were shown to be less likely to be planning training on gift giving (28% small, 34% medium, 53% enterprise) and the EU whistleblower directive (17% small, 20% medium, 30% enterprise).

Hotline and incident management

- Significant majorities of respondents rated various aspects of their organization's hotline and incident management programs as *at least good* – a strong signal of confidence. Still, small-organization respondents were slightly less likely to do so than those from the medium or enterprise level. The largest difference was seen in *using metrics to ensure responsiveness* (78% small, 87% medium, 88% enterprise).
- Enterprise organizations were more likely than small firms to possess certain elements of their confidential reporting and investigatory program, according to survey results. Medium organizations appeared to trend toward one side or the other, depending on the specific program element. For example; a *non-retaliation policy* (49% small, 45% medium, 64% enterprise), a *hotline or internal reporting channel* (46% small, 52% medium, 67% enterprise), and *ability for third parties to report through our hotline* (38% small, 52% medium, 57% enterprise).

Integrated risk management and approach to third parties

- Smaller organizations were said to be less likely than medium firms and large enterprises to possess a board-level committee to address risk integration enterprise-wide (28% small, 42% medium, 49% enterprise), but more likely to possess one at the management level (43% small, 37% medium, 36% enterprise), according to survey data.
- Large majorities of firms across the size spectrum were said to have *some* form of third-party and supplier screening. Yet respondents at the enterprise level were most likely to call out many individual screening areas, including *business continuity plans/preparedness* (49% enterprise, 45% medium, 34% small); *ESG orientation and transparency* (DEI) (39% enterprise, 44% medium, 26% small) ; and *financial health/stability* (64% enterprise, 49% medium, 54% small).

ESG

- Respondents at organizations across the size spectrum were all very likely – perhaps surprisingly so – to say their firm had some sort of strategy in place to determine ESG risks to the business (98% enterprise, 94% medium, 86% small).
- Smaller-organization respondents were less likely than their enterprise peers to say they have various aspects as part of their ESG program, and responses from medium organizations were more mixed. This included: *employee wellness programs* (53% small, 46% medium, 66% enterprise), *diversity metrics tracking* (40% small, 49% medium, 57% enterprise) and *greenhouse gas reduction goals* (39% small, 43% medium, 65% enterprise).
- Respondents at enterprise organizations were more likely than medium-sized to say that their ESG program has support from the CEO, while responses showed small-sized organizations rested in the middle (56% enterprise, 44% medium, 48% small). Survey data also showed enterprise organizations were most likely to have a dedicated person to focus on ESG issues (54% enterprise, 40% medium, 29% small).

9 Conclusion and next steps

It's clear from this report that many R&C professionals feel their program is rising to the level of today's complex regulatory, risk, consumer and cultural dynamics. Respondents to our survey were more likely than last year to give their program high marks in maturity, and those that did often indicated strong engagement from senior leadership in their organization's compliance program as well. R&C leaders also appear to be evolving in real time to meet the challenges of the day, with majorities indicating they planned training to address the important challenge of information security. To see many citing a *strong* relationship between InfoSec and Compliance is encouraging, demonstrating the kind of cross-silo collaboration that is only becoming more important for the success of every R&C program.

Yet, 2023's findings were not without some areas of opportunity. While respondents indicated stronger program maturity than last year, fewer said they possessed certain program elements and prioritization that are critical to regulatory compliance and program effectiveness. This included concerningly low proportions citing that their organization had a non-retaliation policy; this was especially evident among European respondents – surprising given the current focus on the EU Whistleblower Protection Directive and the transpositions by each of the member states. A relatively low proportion of respondents also cited that their organization had a whistleblower hotline, despite the importance, and long-term acceptance, of such a system.

Survey responses also showed every measure for middle management's commitment to compliance moving in the wrong direction compared to last year, raising the question of whether frontline leaders are shirking in their commitment to compliance when it conflicts with other business objectives or feeling more intense business pressures to deliver results in a tighter economy.

These findings and others in this report raise a point every R&C professional should keep in mind when considering the effectiveness of their programs. Attention to R&C was often said to be more high-profile and strategically important in 2023, but the question remains, are programs succeeding in delivering on the fundamentals?

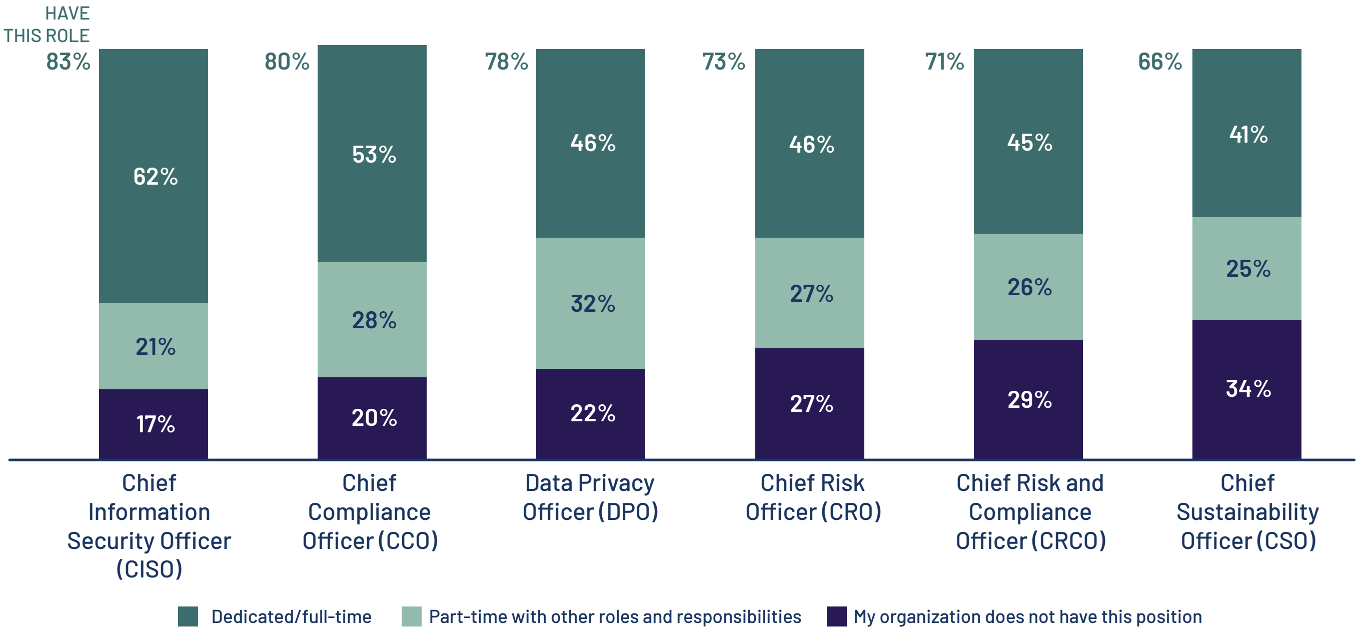
Considering our 2023 key findings, R&C professionals should ask themselves the following questions:

- Does my program have engagement from senior leadership, including my organization's board of directors?
- Is my organization making sufficient efforts to train relevant parties to address information security risk? Is the relationship between leadership in InfoSec and Compliance strong, supporting each function's goals for risk management, compliance and improving ethical cultures?
- Are frontline managers at my organization maintaining a commitment to compliance in the face of competing priorities?
- Am I leveraging my access to sources of data in a way that helps improve and inform the efficacy of my program?
- Is my organization seizing on the positive cultural impacts cited in work-from-home models, especially as it pertains to continued efforts to support compliance and ethics for remote and hybrid workforces?

Our profession must never lose sight of the profound way our work impacts our organizations, our communities and the world. The risk areas and challenges along the way may change, but our mission continues.

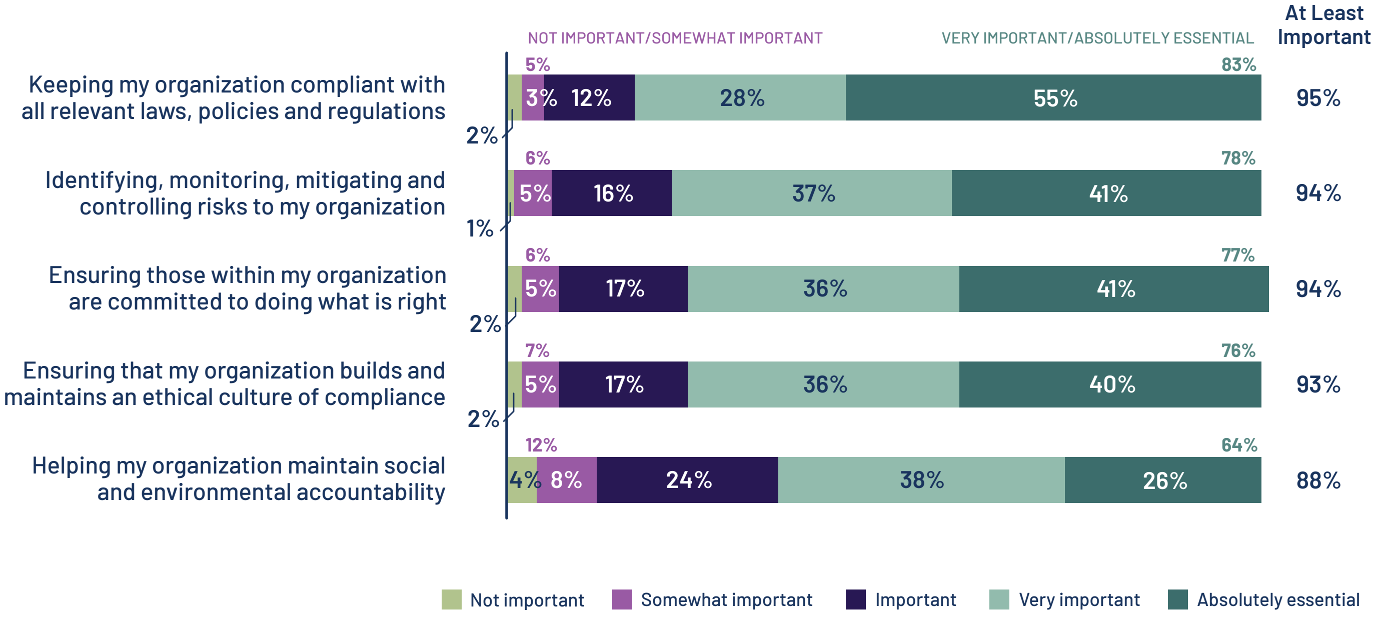
10 Appendix: Additional findings and charts

Position/roles within organization



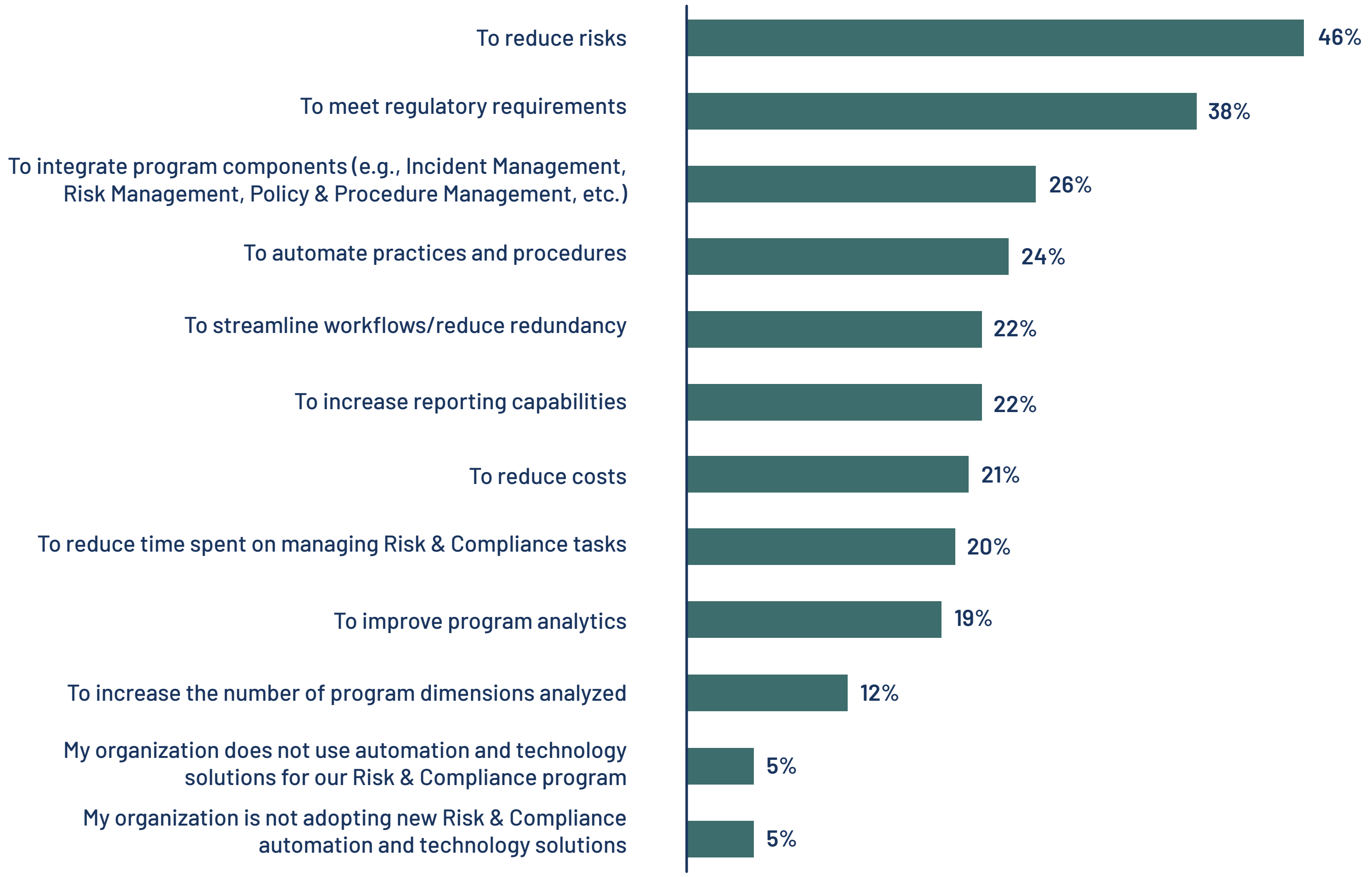
BASE: ALL QUALIFIED RESPONDENTS (n=1,315)
For each of the following positions/roles, please indicate if it's a dedicated/full-time position, part-time position with other roles and responsibilities or if your organization does not have this position.

Importance to organization decision-making



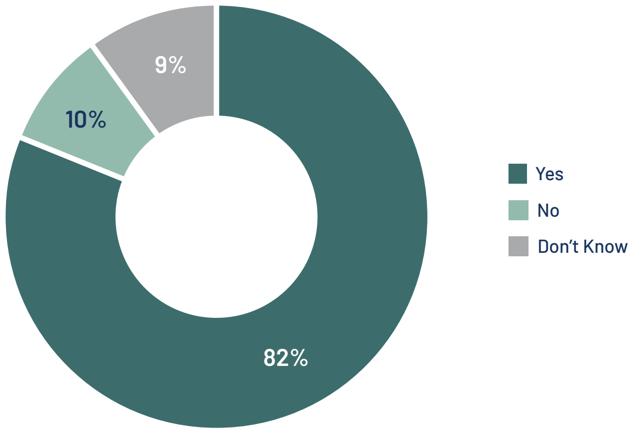
BASE: ALL QUALIFIED RESPONDENTS (n=1,315)
How important are the following considerations to your organization in its decision-making process?

Reasons for adopting new R&C automation and technology solutions



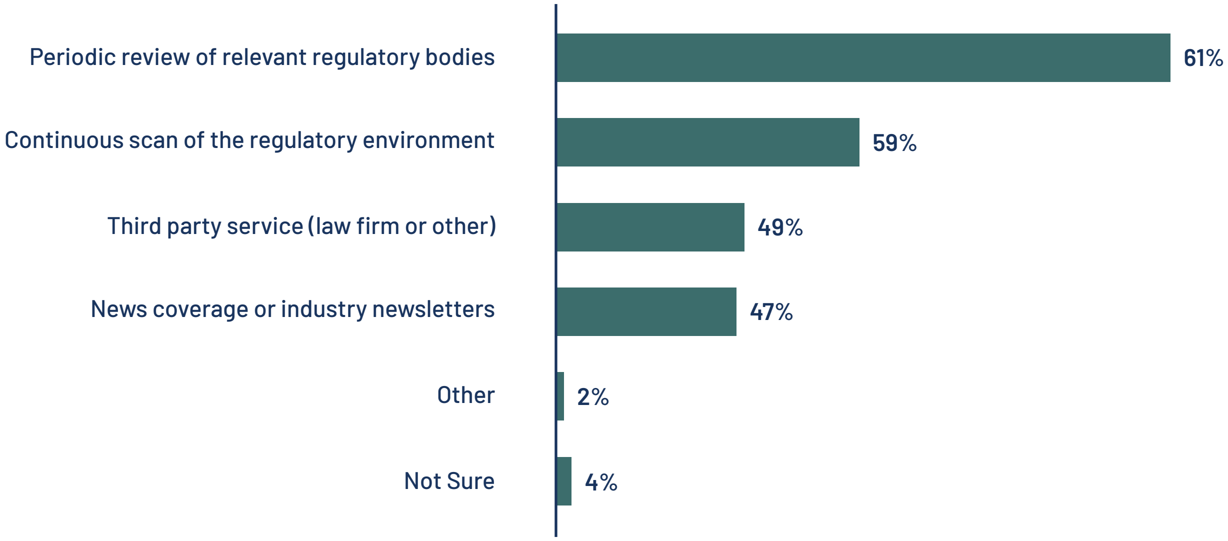
BASE: ALL QUALIFIED RESPONDENTS (n=1,315)
What are your organization's reasons for adopting new Risk & Compliance automation and technology solutions? Please select up to three options.

Have a business continuity plan in place



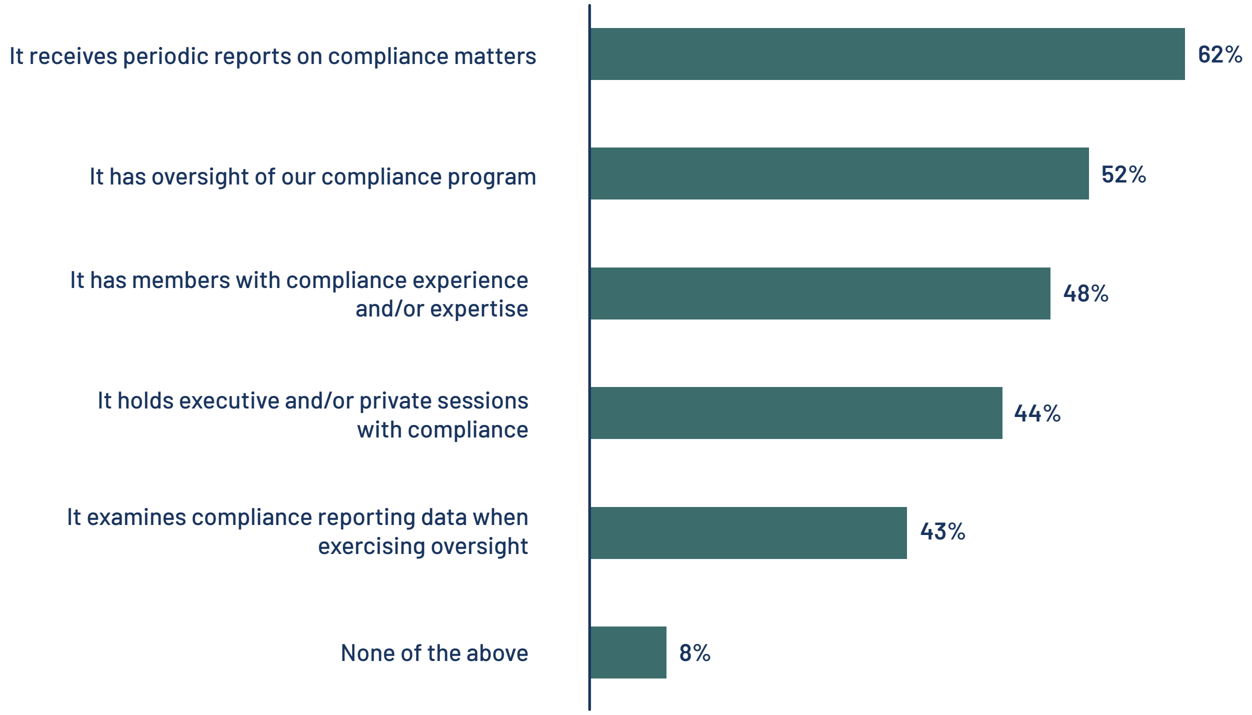
BASE: ALL QUALIFIED RESPONDENTS (n=1,315)
Does your organization have a business continuity plan in place today?

Ways used to obtain information on regulatory compliance issues



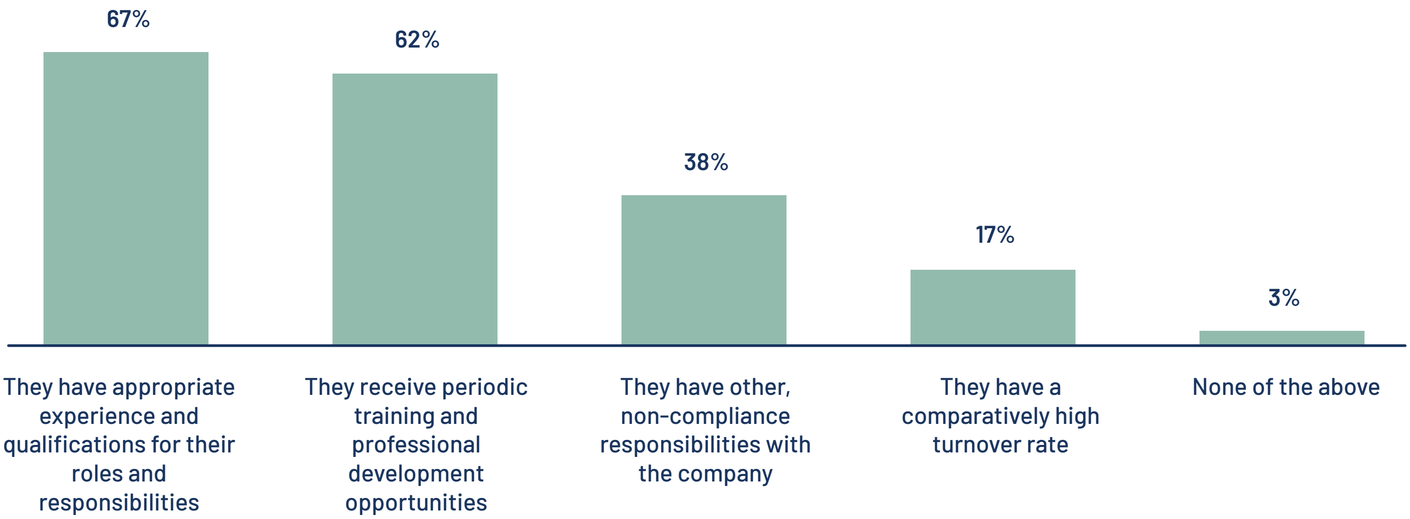
BASE: ALL QUALIFIED RESPONDENTS (n=1,315)
In which of the following ways does your organization obtain information on regulatory changes that affect your business? Please select all that apply.

Board of directors' role in compliance



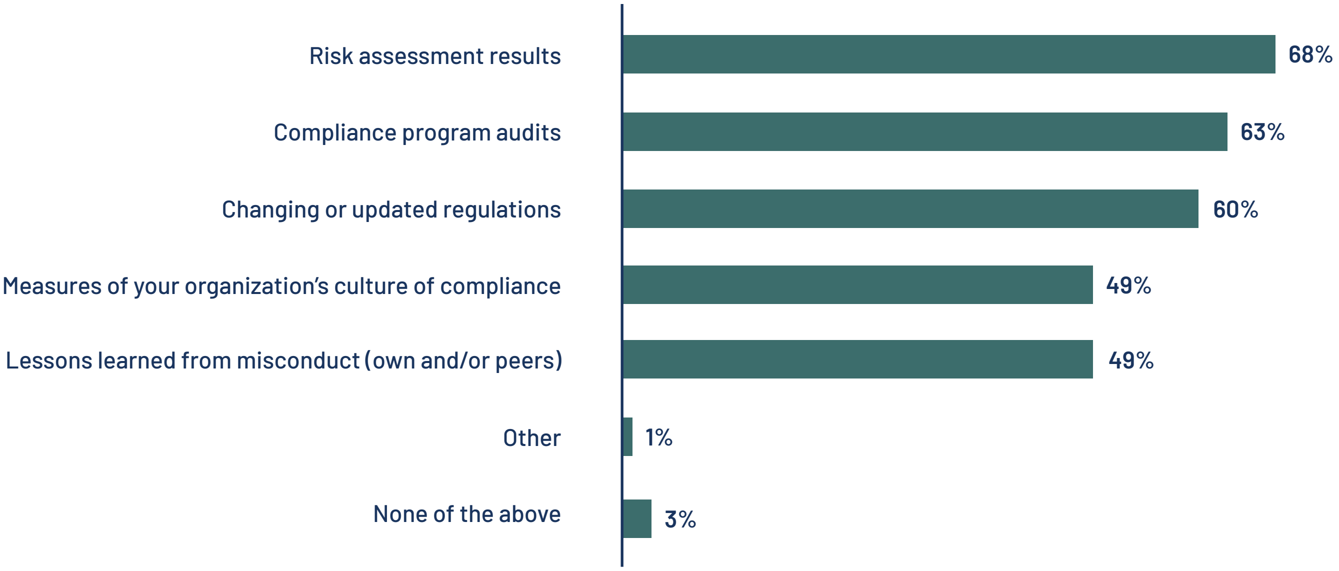
BASE: KNOWLEDGEABLE ABOUT ETHICS & COMPLIANCE (n=977)
Which of the following are true about your organization's board of directors? Please select all that apply.

Compliance personnel qualifications and responsibilities



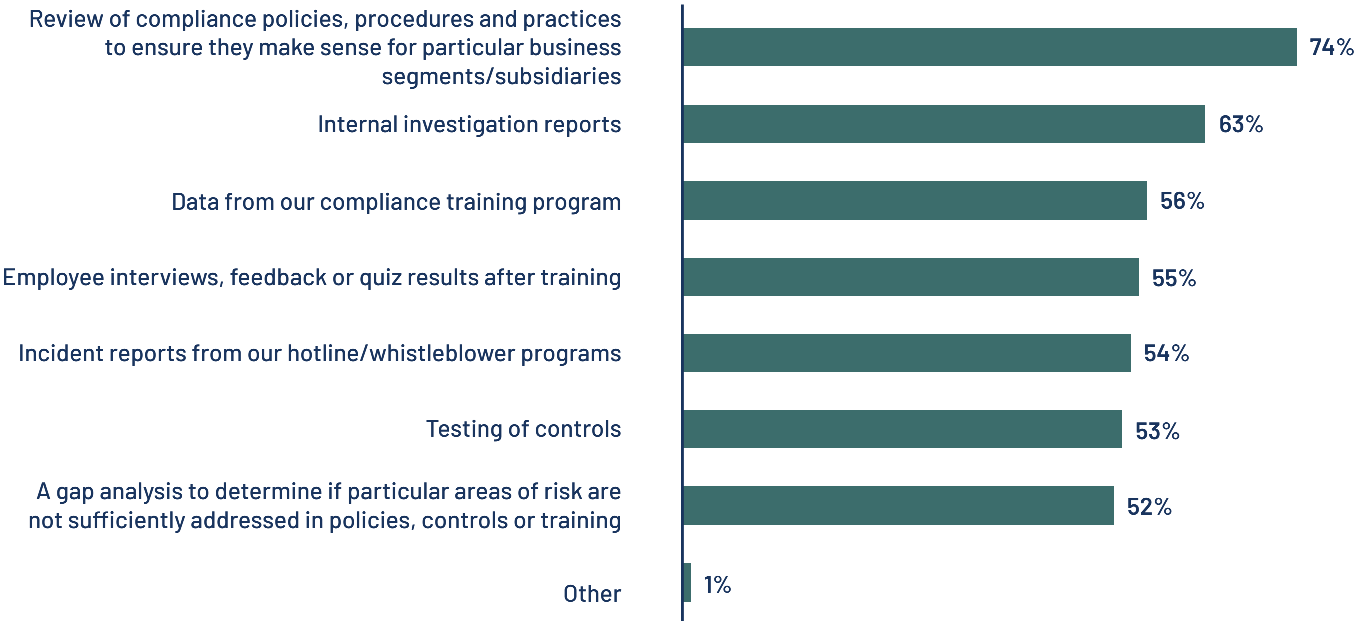
BASE: KNOWLEDGEABLE ABOUT ETHICS & COMPLIANCE (n=977)
Which of the following statements apply to your organization's compliance personnel? Please select all that apply.

Information sources used to review, test and improve R&C program



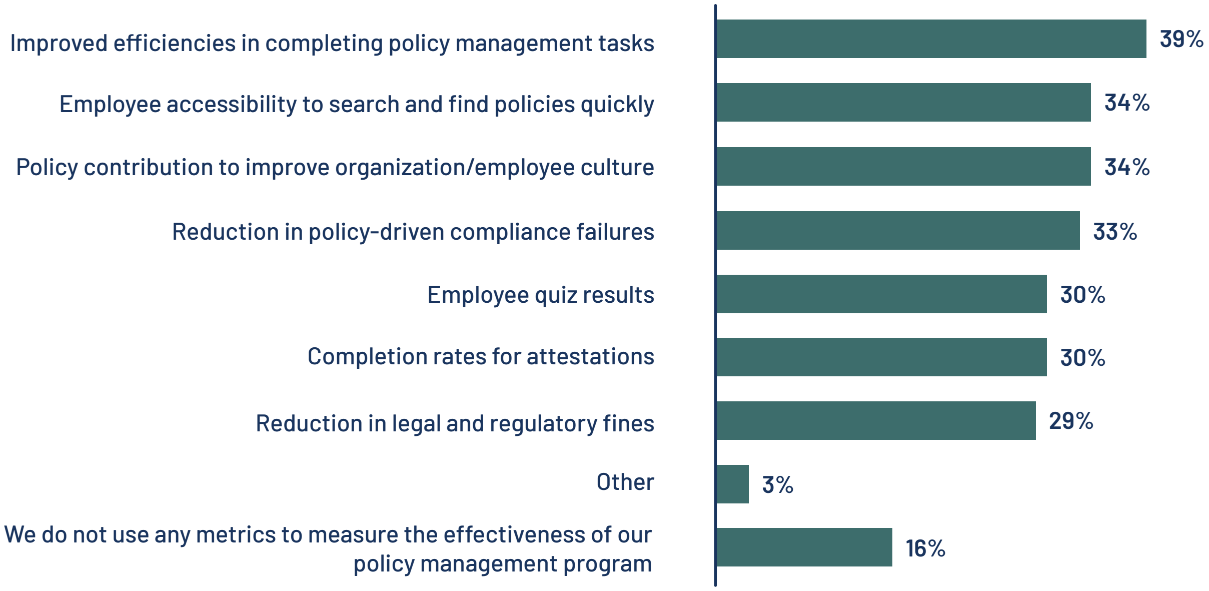
BASE: KNOWLEDGEABLE ABOUT ETHICS & COMPLIANCE (n=977)
Which of the following information sources does your organization use to review, test and improve your risk and compliance program? Please select all that apply.

Organization R&C program audits



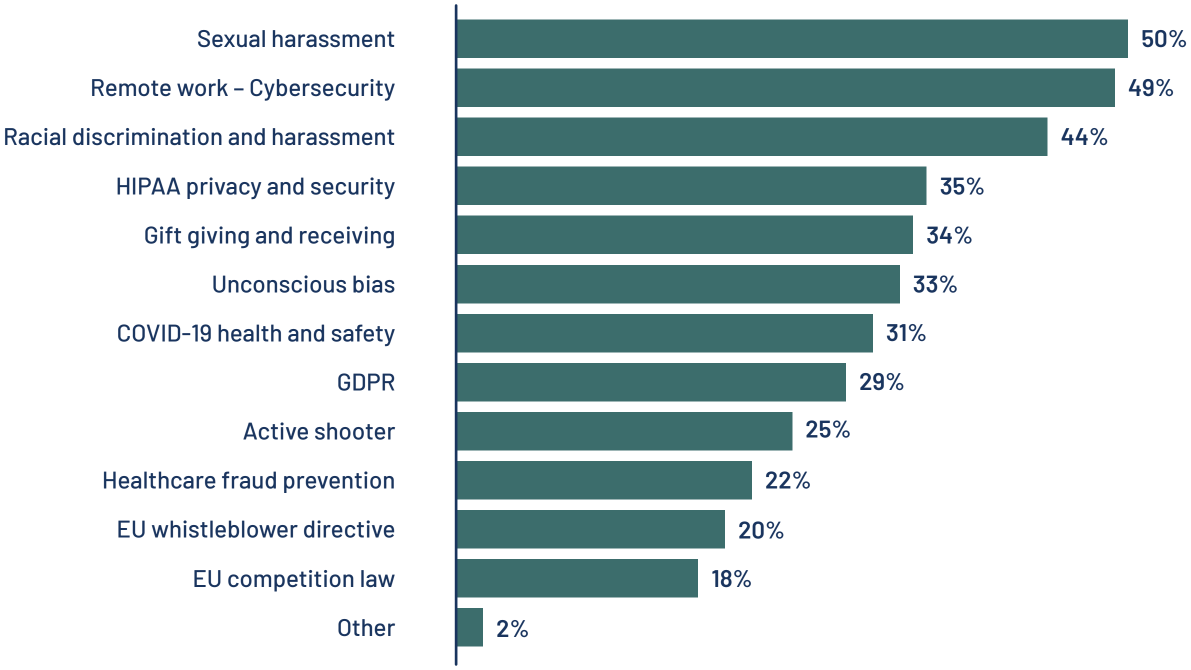
BASE: ORGANIZATION USES COMPLIANCE PROGRAM AUDITS (n=617)
Which of the following are part of your organization’s R&C compliance program audits? Please select all that apply.

Metrics used to measure effectiveness of policy management program



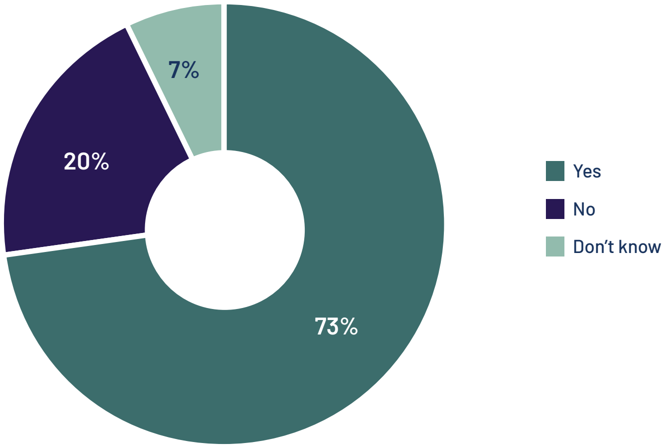
BASE: KNOWLEDGEABLE ABOUT ETHICS & COMPLIANCE (n=977)
Which metrics does your organization use to measure the effectiveness of its policy management program? Please select all that apply.

Compliance subtopics will train on in the next 2-3 years



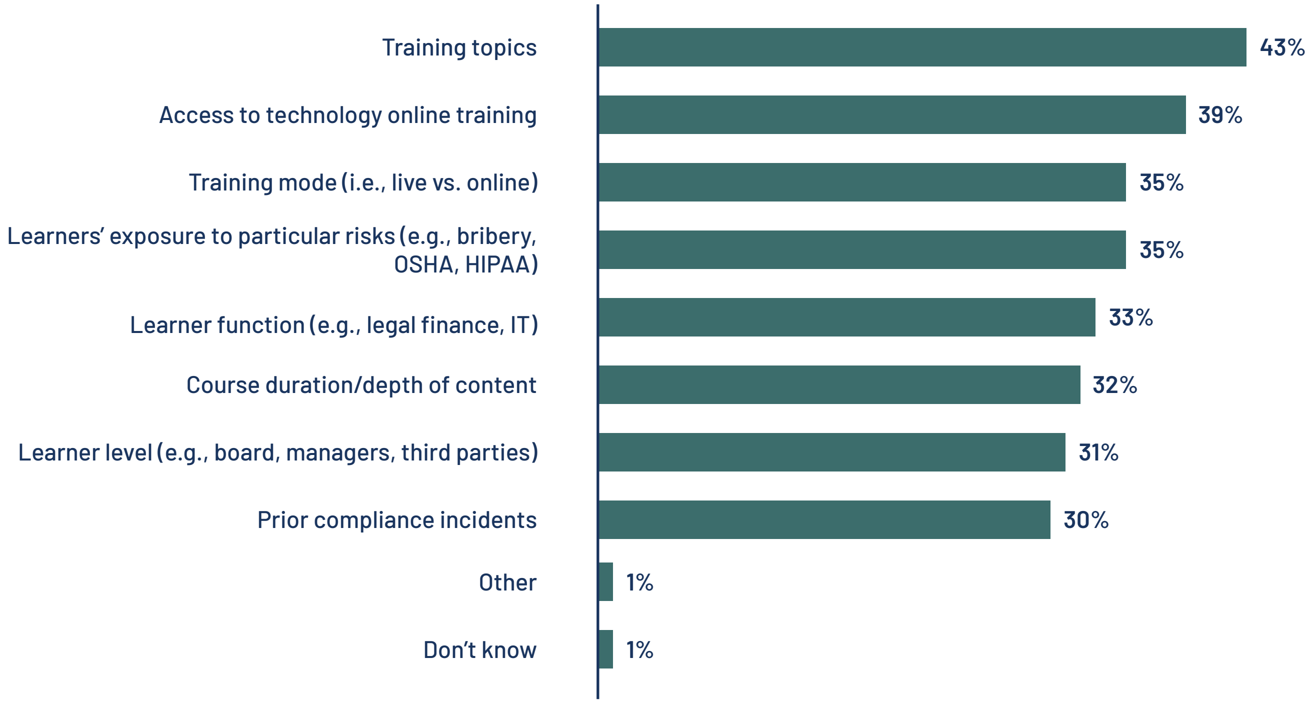
BASE: PROVIDING COMPLIANCE TOPICS TRAINING IN THE NEXT 2–3 YEARS (n=933)
On which of the following compliance subtopics will your organization provide training in the next 2–3 years? Please select all that apply.

Have Risk and Compliance training plan



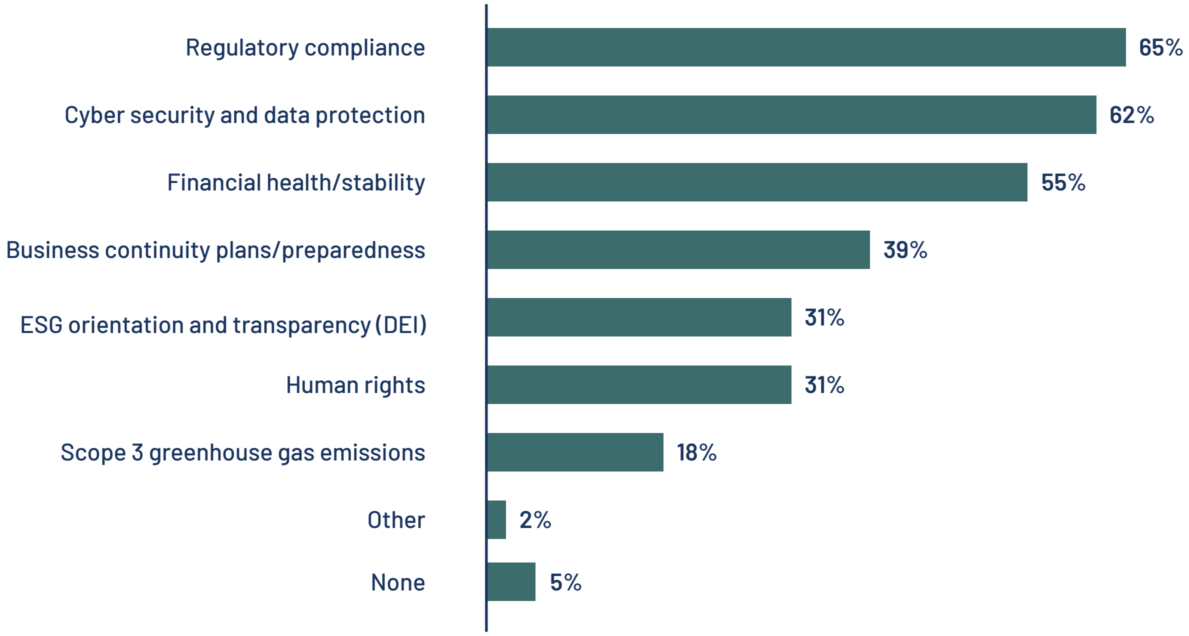
BASE: KNOWLEDGEABLE ABOUT ETHICS & COMPLIANCE (n=977)
Does your organization have a Risk & Compliance training plan?

Risk and Compliance training plan



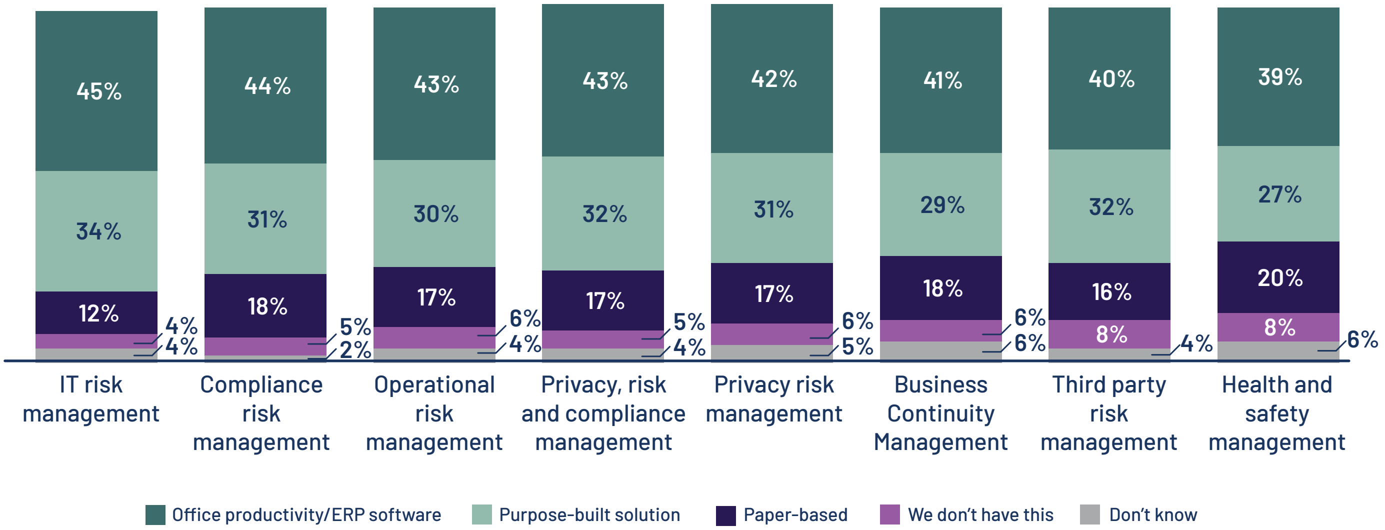
BASE: HAVE A RISK & COMPLIANCE TRAINING PLAN (n=718)
Which of the following does your organization consider in the process of creating its Risk & Compliance training plan? Please select your top three considerations.

Aspects reviewed when screening third parties



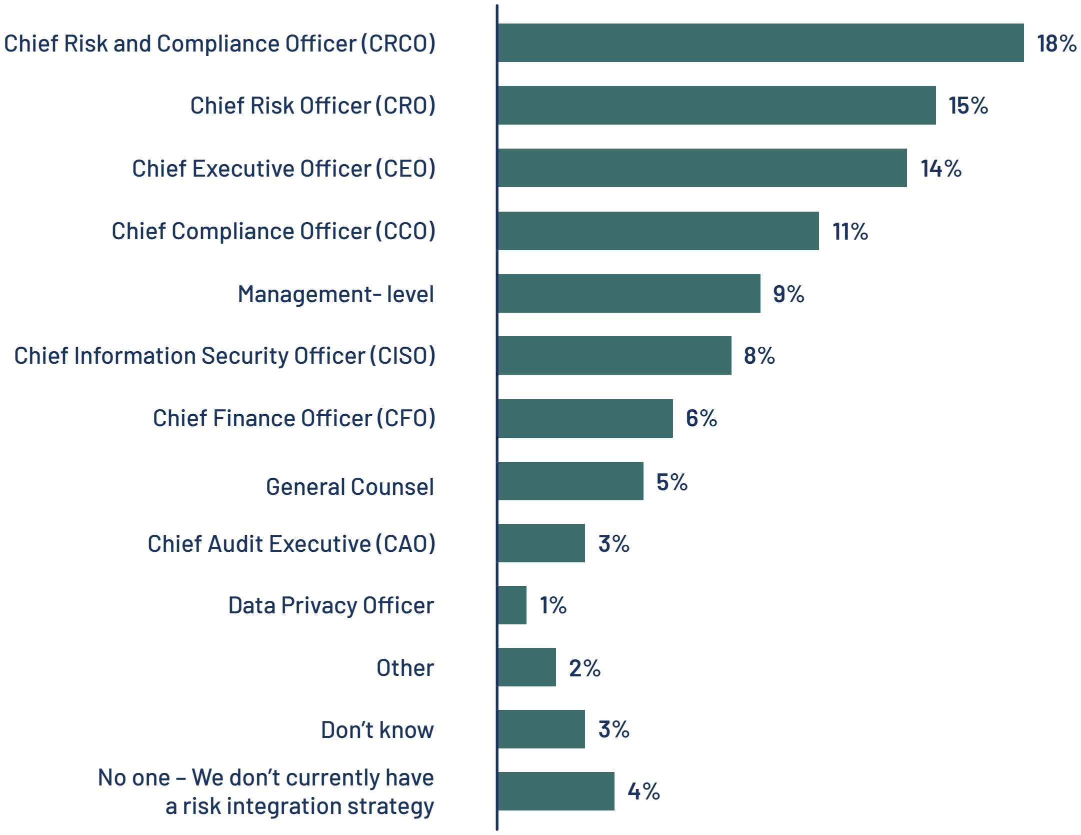
BASE: KNOWLEDGEABLE ABOUT ETHICS & COMPLIANCE (n=977)
Which of the following aspects does your organization review when screening third parties or suppliers? Please select all that apply.

Administration of Risk and Compliance program elements



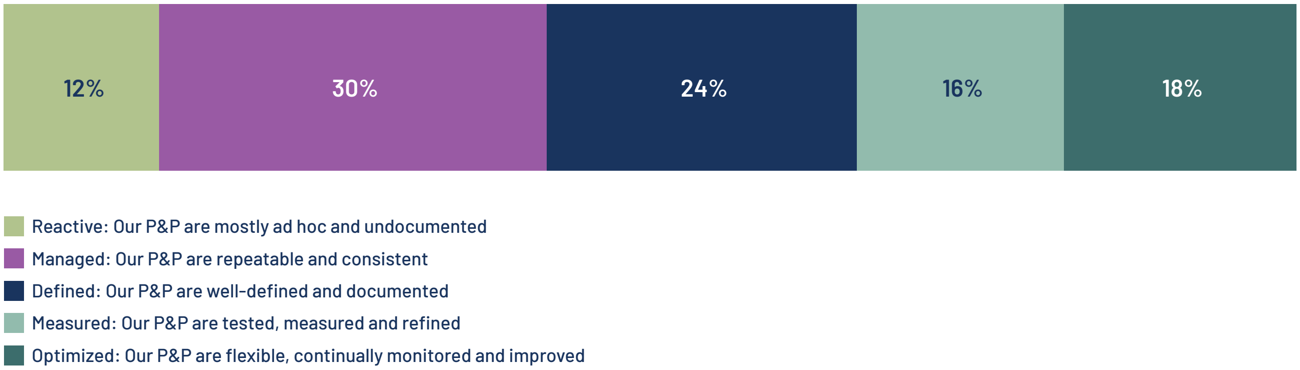
BASE: KNOWLEDGEABLE ABOUT RISK MANAGEMENT (n=1.066)
How does your organization primarily administer the following Risk & Compliance program elements?

Responsible for managing risk integration strategy



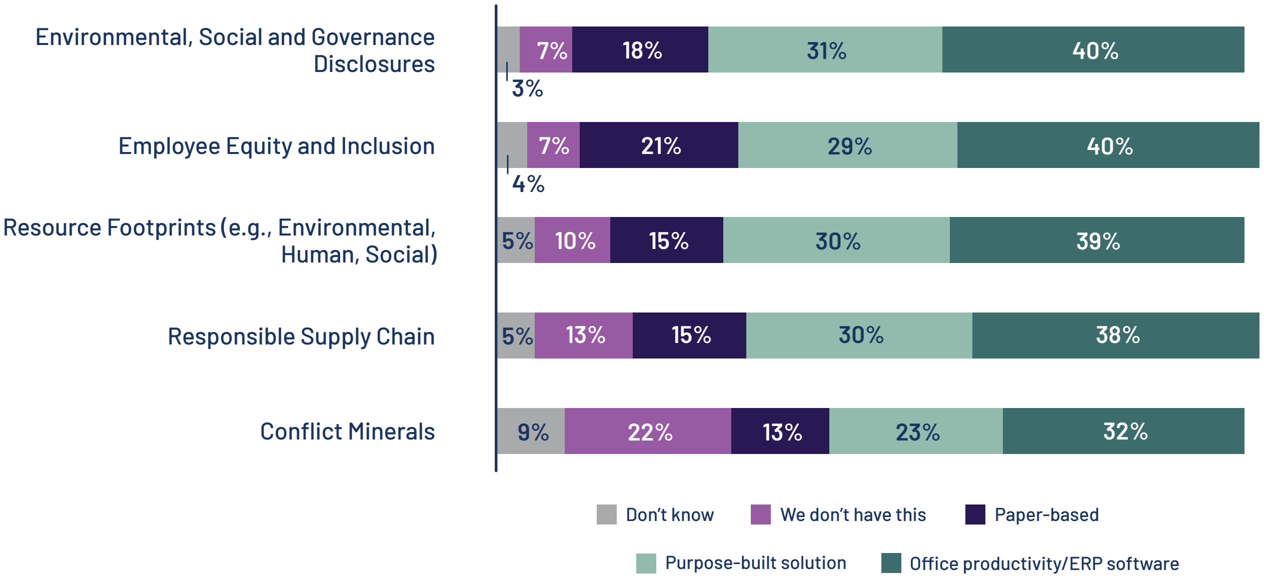
BASE: KNOWLEDGEABLE ABOUT RISK MANAGEMENT (n=1,066)
Who in your organization is responsible for managing risk integration strategy?

Organization's risk management program processes and procedures



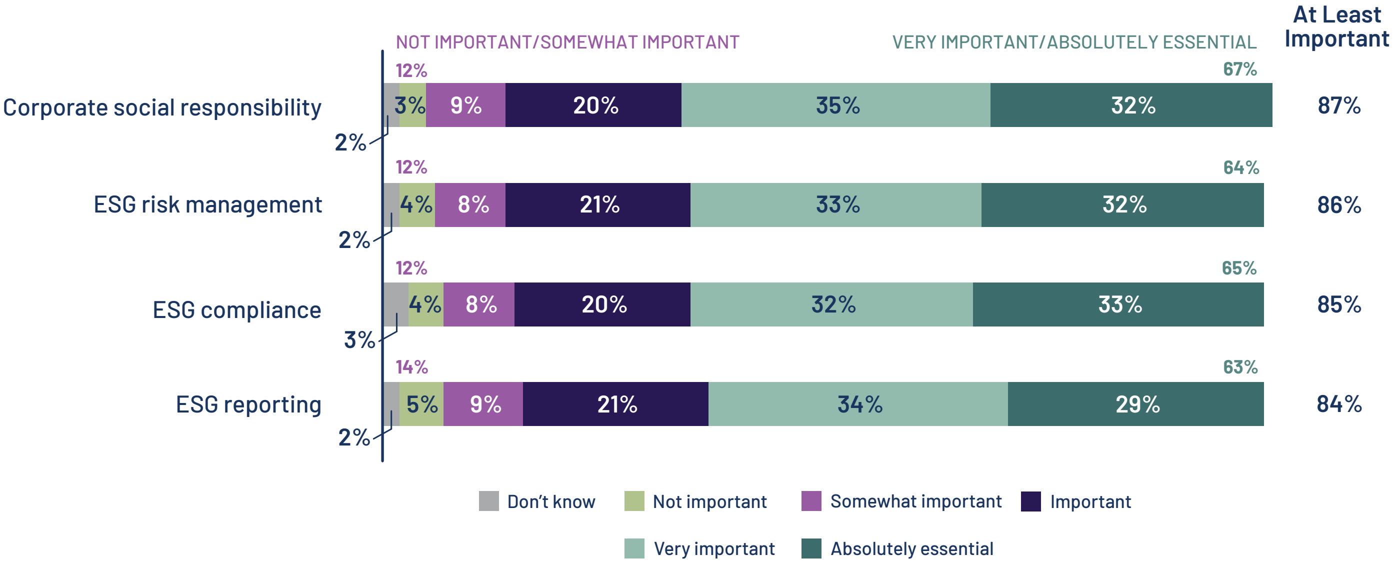
BASE: KNOWLEDGEABLE ABOUT RISK MANAGEMENT (n=1,066)
How would you describe your organization's Risk Management program processes and procedures (P&P)? Please select one response only.

Administration of ESG program elements



BASE: KNOWLEDGEABLE ABOUT ENVIRONMENTAL, SOCIAL & GOVERNANCE (n=787)
How does your organization primarily administer the following Environmental, Social, and Governance Management program elements?

Importance of managing ESG issues



BASE: KNOWLEDGEABLE ABOUT ENVIRONMENTAL, SOCIAL & GOVERNANCE (n=787)
How important is the management of the following environmental, social and governance (ESG) areas to your organization?

About the author

Carrie Penman
Chief Risk & Compliance Officer, NAVEX

As one of the earliest ethics officers in the industry, Carrie Penman previously served four years as deputy director of the Ethics and Compliance Officer Association, now ECI. A scientist by training, she developed and directed the first corporate-wide global ethics program at Westinghouse Electric Corporation between 1994 and 1999. Carrie now leads NAVEX's risk management processes and oversees its internal ethics and compliance program.

Carrie has extensive client-facing risk and compliance consulting experience, including more than 15 years as an adviser to boards and executive teams. Carrie was awarded the inaugural Lifetime Achievement Award for Excellence in Compliance 2020 by Compliance Week magazine. In 2017, she received the ECI's Carol R. Marshall Award for Innovation in Corporate Ethics for an extensive career contributing to the advancement of the ethics and compliance field worldwide.

NAVEX Research Analyst Eric Gneckow also contributed to this report.

About The Harris Poll

The Harris Poll is a global consulting and market research firm that strives to reveal the authentic values of modern society to inspire leaders to create a better tomorrow. It works with clients in three primary areas: building twenty-first-century corporate reputation, crafting brand strategy and performance tracking, and earning organic media through public relations research. One of the longest-running surveys in the U.S., The Harris Poll has tracked public opinion, motivations and social sentiment since 1963, and is now part of Stagwell, the challenger holding company built to transform marketing.

NAVEX®

AMERICAS

5500 Meadows Road, Suite 500
Lake Oswego, OR 97035
United States of America
info@navex.com
www.navex.com
+1 (866) 297 0224

EMEA + APAC

1 Queen Caroline Street
London, W6 9HQ
United Kingdom
info@navex.com
www.navex.com
+44 (0) 20 8939 1650