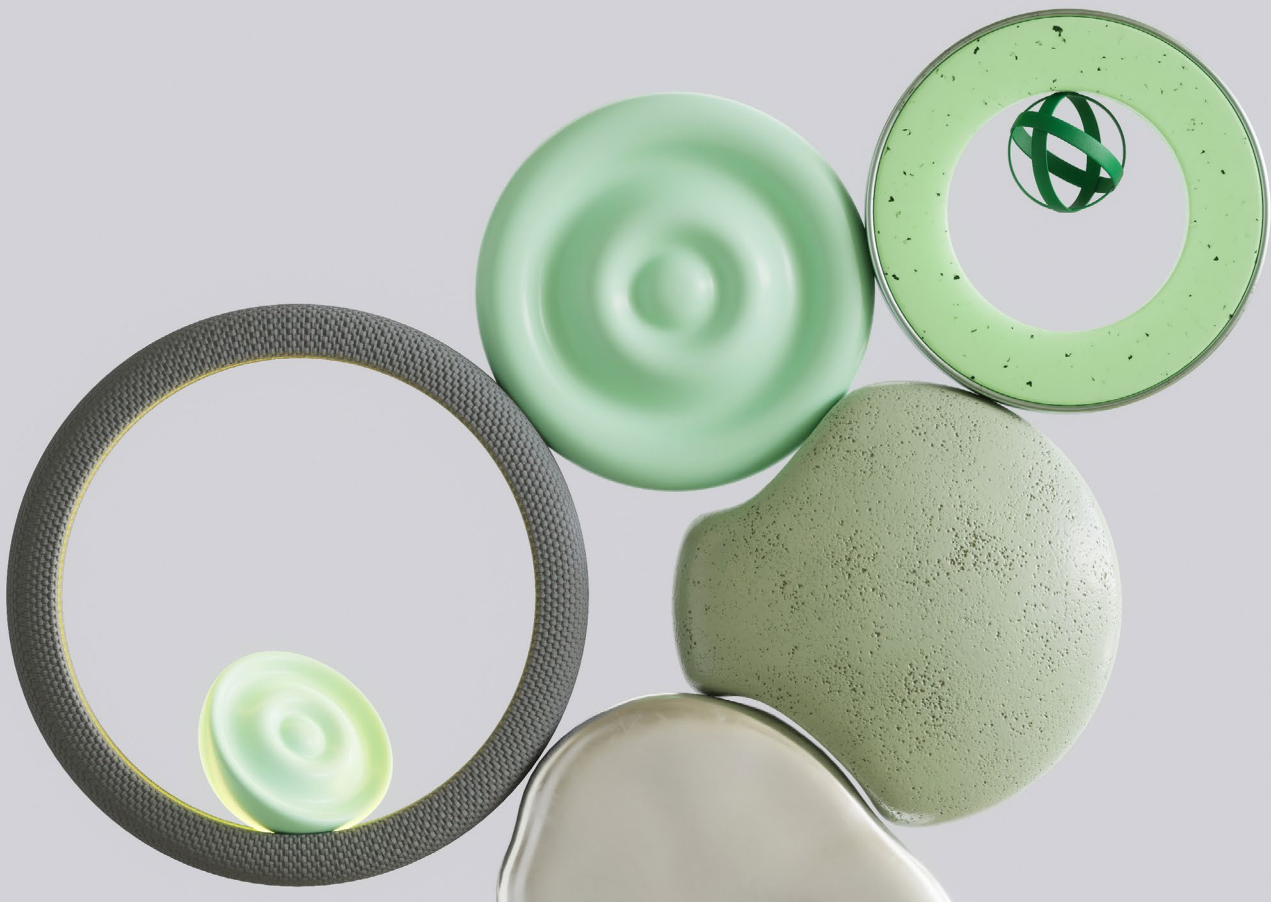
2022 GLOBAL ESG, COMPLIANCE & RISK REPORT

Value creation amid rising global uncertainty



THE AUTHORS

DR. KATHARINA HEFTER

MANAGING DIRECTOR
AND PARTNER

HEFTER.KATHARINA@BCG.COM

DR. BERNHARD GEHRA

MANAGING DIRECTOR
AND SENIOR PARTNER

GEHRA.BERNHARD@BCG.COM

DR. JULIA GEBHARDT

MANAGING DIRECTOR
AND PARTNER

GEBHARDT.JULIA@BCG.COM

HANJO SEIBERT

MANAGING DIRECTOR
AND PARTNER

SEIBERT.HANJO@BCG.COM

PIERRE ROUSSEL

MANAGING DIRECTOR
AND PARTNER

ROUSSEL.PIERRE@BCG.COM

JEANNE KWONG BICKFORD

MANAGING DIRECTOR AND
SENIOR PARTNER

BICKFORD.JEANNE@BCG.COM

JANNIK LEIENDECKER

PARTNER AND
ASSOCIATE DIRECTOR

LEIENDECKER.JANNIK@BCG.COM

TAD ROSELUND

MANAGING DIRECTOR AND
SENIOR PARTNER

ROSELUND.TAD@BCG.COM

REI TANAKA

MANAGING DIRECTOR
AND PARTNER

TANAKA.REI@BCG.COM

LORENZO FANTINI

MANAGING DIRECTOR
AND PARTNER

FANTINI.LORENZO@BCG.COM

MATTEO COPPOLA

MANAGING DIRECTOR AND
SENIOR PARTNER

COPPOLA.MATTEO@BCG.COM

NICOLA NICOL

MANAGING DIRECTOR
AND PARTNER

NICOL.NICOLA@BCG.COM

PAUL O'ROURKE

MANAGING DIRECTOR
AND PARTNER

O'ROURKE.PAUL@BCG.COM

KEN CARLSTEDT

ASSOCIATE DIRECTOR,
GLOBAL TRADE & INVESTMENT

CARLSTEDT.KEN@BCG.COM

JULIANE BUTTERS

PROJECT
LEADER

BUTTERS.JULIANE@BCG.COM

ELISABETH BENAZIR LIPPERT

SENIOR KNOWLEDGE
ANALYST

LIPPERT.ELISABETH@BCG.COM

INTRODUCTION

The global regulatory environment has grown increasingly complex, and now spans a far broader range of issues than in the past. Compliance functions have been heavily affected as a consequence. They must deal with multiple growing challenges, such as sanctions and trade compliance and supply chain risks, as well as a general rise in regulation and regulatory enforcement, especially in the environmental, social and governance (ESG) area. To compound matters further, the pace of change will only accelerate in a highly networked and digitized world.

However, this new world should not only be seen as a challenge to overcome, but also as an opportunity to create value for the company and forge ahead of rivals. As regulators raise the bar for all kinds of risks, the compliance function is set to play a pivotal role in managing these regulatory developments successfully and steering organizations through crises. For example, the proliferation of sanctions over the past year has shone a new light on the crucial role of compliance departments in all industries. Similarly, headlines exposing greenwashing clearly demonstrate how important compliance departments are in guiding implementation of the relevant requirements.

In these demanding conditions, companies need to define the terms of their compliance mandate for their relevant risks, determine the role of their compliance function for these risks, and then optimize the function so that it lives up to the mandate. To create value, the compliance function needs to fulfill different roles, according to the particular topic and specific risk. Companies that succeed in this endeavor will gain sustainable competitive advantage, boost customer loyalty and trust, attract and retain talent, and enhance their reputation for acting responsibly in a testing business environment.

But exactly how are companies reacting to the changing compliance landscape in order to gain an advantage and get closer to their Target Operating Model (TOM)? Following our first RISK AND COMPLIANCE SURVEY FROM 2021, we repeated the exercise in May and June 2022, this time with the goal of identifying and then analyzing the core issues relating to risk and compliance. We interviewed 250 compliance professionals from companies across various industries around the world, and asked them to name the foremost issues and challenges faced by compliance organizations, and how are they fulfilling their compliance mandates. In asking these questions, we wanted to build a complete picture of the risk and compliance function, and how companies in general are coping with various types of risk and the myriad growing uncertainties in the global landscape.

In a more complex world, simply writing policy guidelines and instructing employees to follow the rules will not be enough to stay ahead of the game. Every company needs a strategy not just to manage current risks but also to adapt quickly as circumstances, rules, regulations, and expectations develop. The goal of this study is to provide companies with the perspective and tools they need to develop their compliance strategy, and then implement it successfully in the face of diverse and evolving compliance risks.

Our analysis revealed the following seven core topics and conclusions:

1. COMPLIANCE MANDATE

The clearer the mandate of the compliance function, the more it can create value for the company.

2. GEOPOLITICS

If a company is equipped with crisis response plans, and with procedures for swift action in response to volatile developments in supply chains and sanctions, the company will prove more resilient during times of geopolitical tension.

3. ESG COMPLIANCE

Taking concerted action to mitigate risk of ESG regulation enforcement only works if the gaps between ESG expectations and the reality are significantly narrowed.

4. DIGITIZATION

Adequate operating models enable companies to meet future challenges and seize the opportunity to reduce the cost of compliance.

5. CYBERSECURITY

Insufficient investment in cybersecurity, resilience and testing, resulting in a failure to keep pace with digitization or respond to escalating cyber threats, could have a significant impact on business performance and lead to an erosion of customer trust.

6. BUSINESS ETHICS

Consequent implementation of a defined ethical culture is the crucial step to establish a sustainable compliance awareness across the organization.

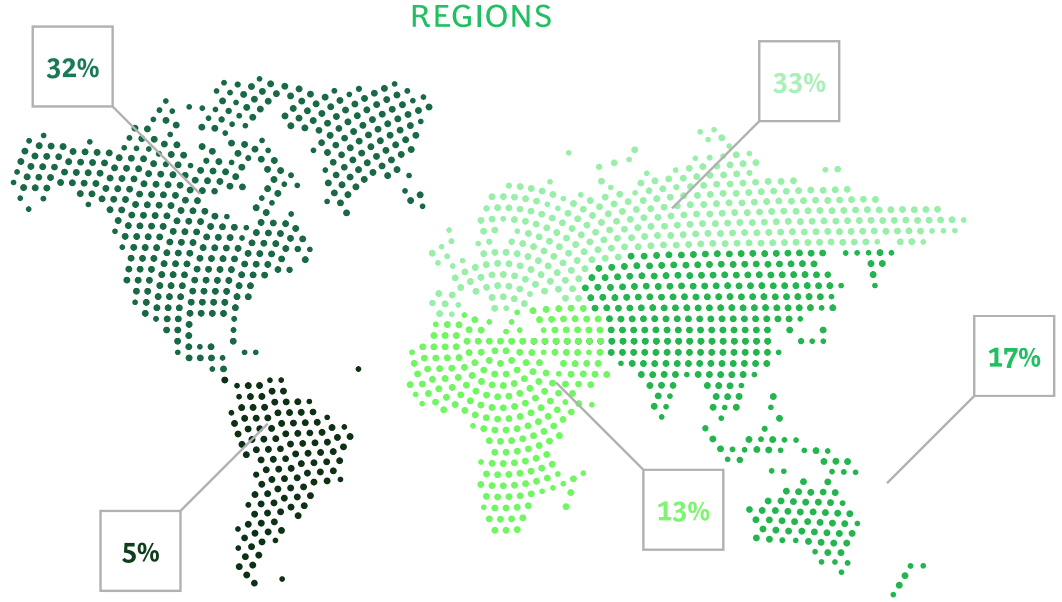
7. WORKFORCE

A strong workforce strategy, involving carefully considered recruitment, training, and retention, is essential in unleashing the potential for compliance as a competitive advantage.

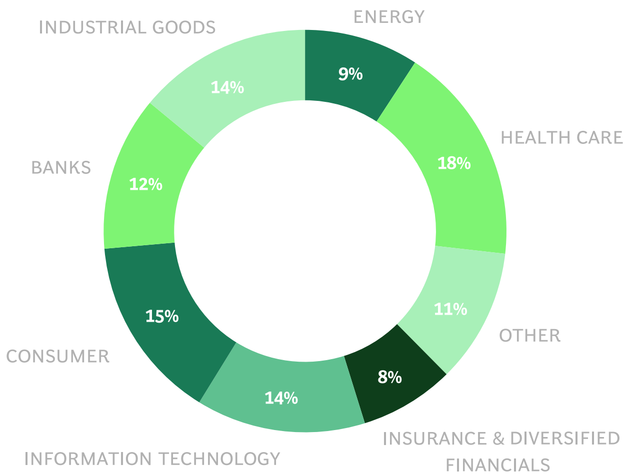
SURVEY PARTICIPANTS

FIGURE 1: OUR FINDINGS ARE BASED ON FEEDBACK FROM 250 COMPANIES …

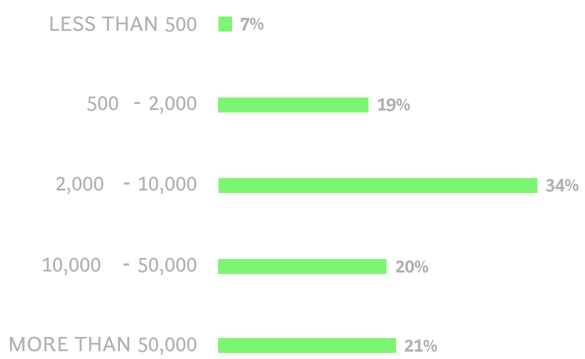
REGIONS



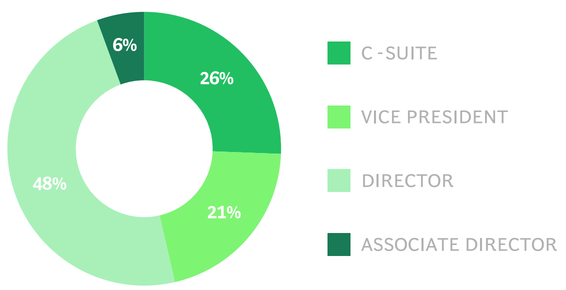
INDUSTRIES



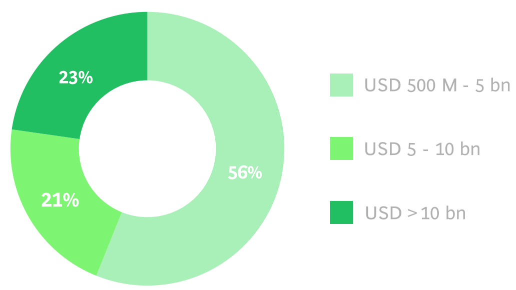
COMPANY SIZE (#FTE)



PARTICIPANTS



COMPANY REVENUE



1. COMPLIANCE MANDATE: Emphasizing value creation

Against a background of diverse and evolving compliance risks and rising uncertainties, setting out the compliance mandate and the role of the compliance function for different types of risk is critical. The survey reveals that compliance organizations are already dealing with a wide range of risk categories: fraud and financial crime risk, competition risk, information security/ information technology risk, corporate and capital market risk, and employee risk. Interestingly, our analysis reveals that key ESG-related topics, such as sustainability, environmental law and human rights, are on average only included in the compliance mandates of around half to two thirds of organizations.

FIGURE 2: KEY RISKS UNDER COMPLIANCE MANDATE (IN %)

This point highlights a crucial theme when it comes to the value creation ambitions of a compliance function - the importance of cross-collaboration in ESG, risk and compliance management. The management of risk is not the sole preserve of the compliance and risk functions. Individual departments have in the past often used their own piecemeal risk management methods to keep up with regulations. One frequent example is the procurement department. This siloed response fails to protect the business from financial penalties and negative public opinion. As many risks affect a variety of departments and processes within an organization, effective collaboration is vital.

The key to creating true value from these cross-functional collaborations is a clear delineation of roles, setting out which function has overall ownership of a particular area, and which is responsible for each part of the process. The role of the compliance function can range from advisor to central oversight. One real-world example would involve compliance departments collaborating closely with their colleagues in software and product development during agile development phases, making sure that they are involved early in the process and achieving speed to output.

2. GEOPOLITICS: Responding to global events

Much of the everyday work of compliance functions is currently taken up with responding to the requirements of economic and trade sanctions during geopolitical tensions, and with the handling of global crises such as the pandemic.

As the sanctions landscape becomes more complex and dynamic, sanctions compliance systems must become more sophisticated in response, and must interface seamlessly with broader trade compliance capabilities. Resolute consensus among governments is forcing companies to take a political stance, willingly or not. This has become particularly true with economic flows being increasingly used as a strategic weapon in foreign and security policy.

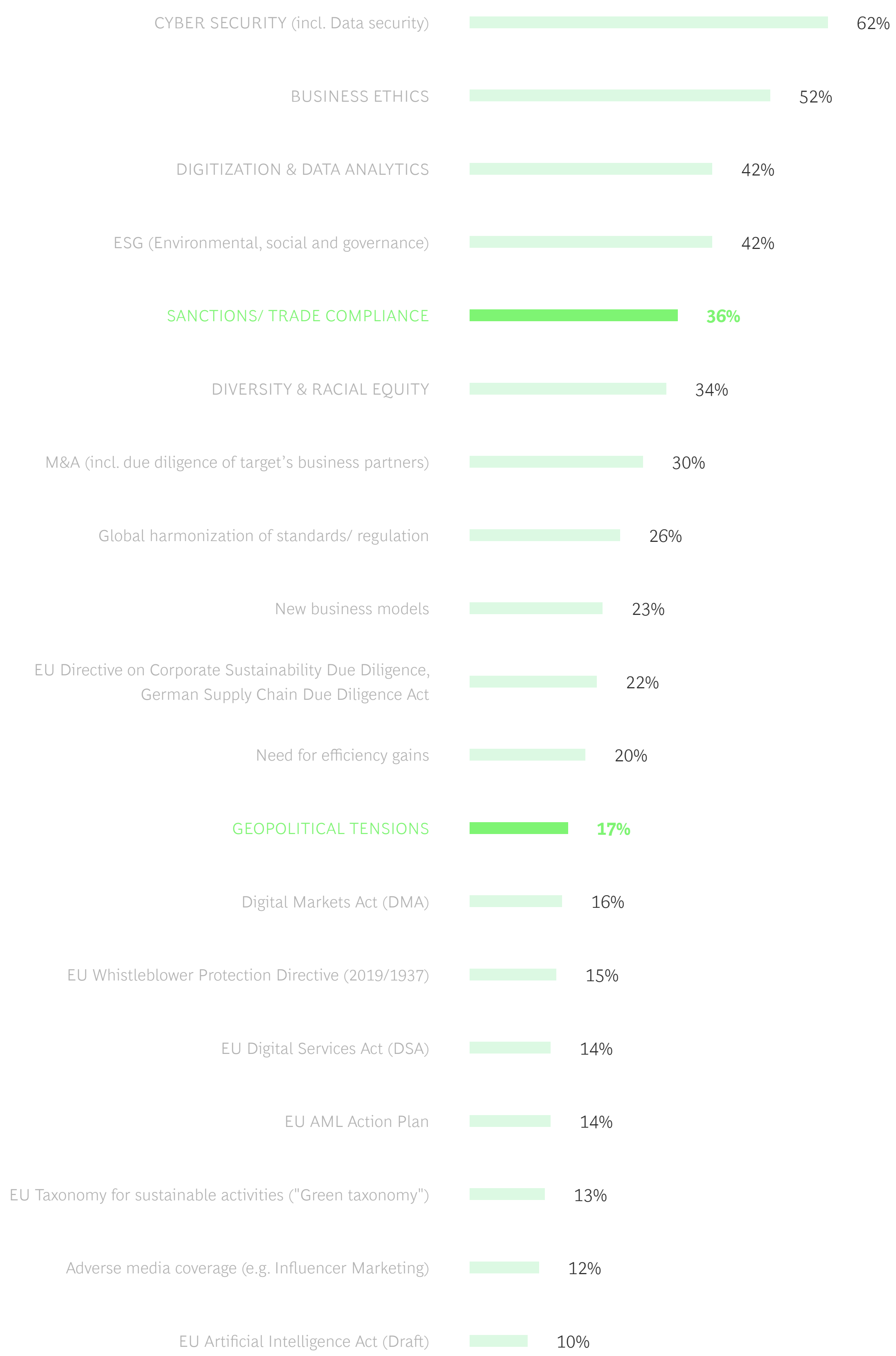
Companies need to be careful not to circumvent the growing number of financial and trade sanctions, including the recent wave of export controls related to high-end semiconductors. They need to develop a comprehensive organizational strategy that allows them to monitor the details of an avalanche of newly introduced sanctions and respond accordingly in a timely manner. The limited ambition simply to follow rules will not be sufficient in a world that is moving so quickly. This year's survey shows that sanctions and trade compliance have become even more important to compliance organizations, and now ranks among the top five key topics. This is a jump of 15 places from our previous survey in 2021.

Even without changes in regulatory or governmental requirements, any kind of upheaval can destabilize the environment in which the companies are operating. The global pandemic is such an example, and it shows how disruptions in supply chains can pose a major threat to multinational companies. Decisions had to be taken in a shorter time span, while new business partners had to be onboarded or new trade routes identified. Regular processes had to be expedited and different processes implemented. All these changes increased the risk of insufficient due diligence or of overlooking requirements.

Reaction to these global crises in many companies has often been too slow. A company's previous work to establish transparency on these risks as well as its preventive measures were both crucial during these times and have certainly paid off. There is clearly a need for crisis response plans which facilitate swift decision making in relation to volatile developments in supply chains and government sanctions, as numerous jurisdictions continue to implement and enforce local regulations.

Unsurprisingly, given developments in Europe over recent months, survey participants for the first time rank geopolitical tensions as a key topic for compliance organizations (it is ranked at number 11). This correlates to the upward jump in sanctions and trade compliance, as geopolitical tensions lead to expanded trade regulations and retaliations. A robust compliance operating model ensures resilience against external shocks and uncertainties and strengthens crisis management. The major challenge in crisis management is simultaneously handling a multitude of issues that demand a broad range of skills and capabilities.

FIGURE 3: KEY TOPICS FOR COMPLIANCE ORGANIZATIONS



3. ENVIRONMENTAL, SOCIAL AND GOVERNANCE (ESG): Meeting stakeholder expectations

Environmental, social and governance (ESG) issues have become a critical component of modern business practices. The reasons are clear – rising regulatory expectations, an increasing awareness of the threat of global warming, and more concern about the impact of company operations on the world around them.

Since 2018, authorities worldwide have issued more than 170 new or amended ESG regulations. Guidelines such as the EU Corporate Sustainability Reporting Directive (CSRD) are set to be further codified by clear standards currently being developed by the European Financial Reporting Advisory Group (EFRAG) (see the recently published BCG paper "ESG COMPLIANCE IN AN ERA OF TIGHTER REGULATIONS").

Companies must handle changing ESG regulations on topics such as climate change, human rights, and diversity. Given the major gap between expectations and current reality, ESG compliance has placed companies under considerable pressure. While cross-divisional collaboration can help to accelerate action and mitigate the risk of regulatory enforcement or losing investors and clients, breaches of so-called social compliance lead to significant reputational risks.

DEEP DIVE: THE NEED FOR AN HOLISTIC APPROACH

In February 2022, the EU Commission adopted a proposal for a directive on corporate sustainability due diligence. The aim of this directive is to foster sustainable and responsible corporate behavior, and to anchor human rights and environmental considerations in companies' operations and corporate governance.

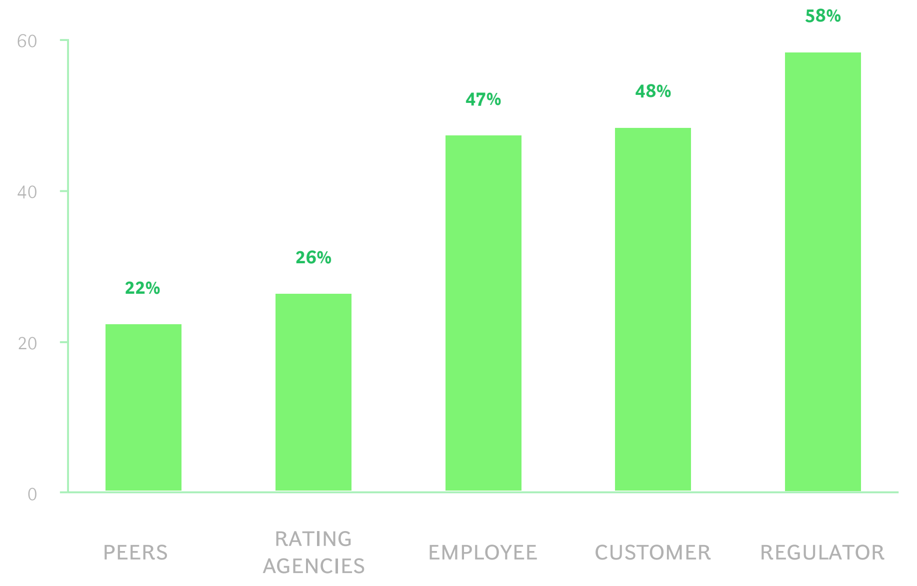
The draft regulation requires large EU companies, and some non-European companies with significant business operations in Europe, to assess their actual and potential human rights and environmental impact throughout their operations and their supply chains, and to take action to prevent, mitigate, and remedy the harms to human rights and the environment that have been identified.

Similarly, the soon-to-be-implemented German Supply Chain Due Diligence Act is designed to protect human rights and the environment in supply chain operations. Companies need to respond with a holistic rather than a siloed approach. Indeed, a governance triangle should be formed: the procurement function should examine vendors in detail; the human resources function should look at how employees are treated in the supply chain; and a human rights department can be introduced to consolidate the company's overall approach and manage reporting (see recently published BCG paper "MANAGING SUPPLY CHAIN RISK – AN UPDATE ON LEGAL AND STRATEGIC REQUIREMENTS"). Some jurisdictions, such as Australia, actually have a regulatory requirement to nominate a human rights officer. A holistic process is also necessary for ESG measurement, steering and reporting, where similar methodologies should be used throughout the organization.

The increasing importance of ESG is clearly reflected in our survey results, irrespective of the particular company's region, industry or size. A significant proportion (43%) of respondents selected ESG as one of the top five trends or topics that are most relevant for their compliance organization.

Moreover, a large majority (79%) reported that their commitment to ESG has intensified over the past two years. This is in part because they see a notable increase in the amount of ESG regulation, and greater enforcement of these regulations for companies which engage in greenwashing or have not implemented the required changes to their products, services, reporting mechanisms or organizational structure. Indeed, approximately 60% of respondents say that regulators are having the greatest impact on their ESG efforts. After regulators in the ranking come customers (48%), and employees (47%). Respondents are fully aware that increasing regulatory demands threaten a company's survival. If its pursuit of ESG is less than comprehensive, it will buckle under the weight of sanctions and a worsening reputation.

FIGURE 4: MAIN DRIVERS FOR ESG EFFORTS



The survey reveals that the role of the compliance function differs from company to company. It can range from oversight over all ESG topics to responsibility for certain selected areas. The role of the compliance function for ESG in each company should be appropriate for the relevant business, operating model and ESG factors. However, given that ESG spans several existing risk categories that typically fall within the compliance mandate, the compliance function usually plays an important role in ESG management. In particular, its experience of risk management systems should be sought when setting up governance, standards and reporting lines so that the compliance function can create the greatest possible value in a given area.

4. DIGITIZATION: Making up for lost time

Dealing with burgeoning regulation can easily lead to spiraling costs. So how then do companies and their compliance functions manage to inject efficiency into this process while still operating in the most effective way possible?

Digitization is the most common answer to this question. However, it is important to have a clear definition of what this entails. Companies need to understand what their problems are, what needs to be done and how digitization can help to reach these objectives. Upgrading the front end while the back-end processes are still manual and inefficient does not add up to genuine digitization. Cross-divisional collaboration for rethinking the end-to end client journeys is necessary, focusing at all times on what benefits the client experience. In that regard, digitization can certainly contribute greatly to raising efficiency, for example by streamlining labor-intensive processes such as Know Your Customer (KYC), transaction monitoring, screening and risk assessments, making controls more automated and data-driven, and reporting. Automated document capture and read-out of relevant data such as "use of goods" can reduce the cost of compliance and error rates (see, for example, the BCG LinkedIn article "FUTURE PROOFING COMPLIANCE WITH TECHNOLOGY & DIGITAL").

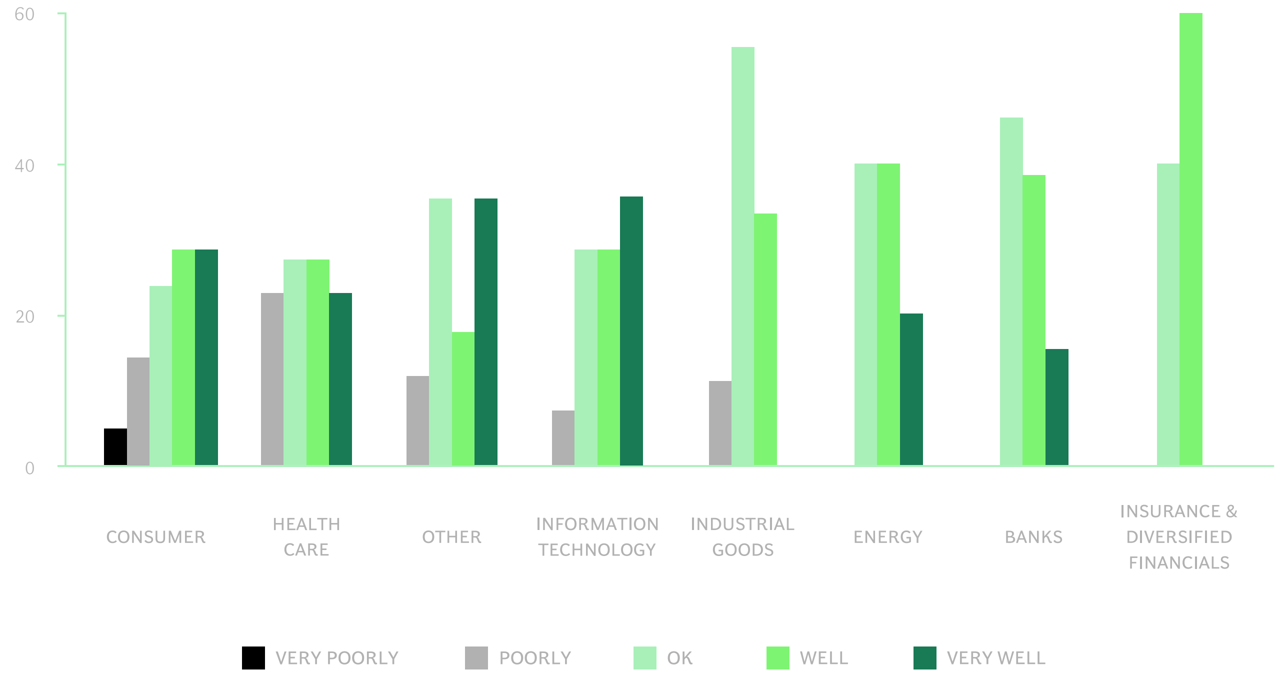
Despite digitization's potential, many companies are not properly preparing their operating model to meet future challenges, and are missing the opportunity to reduce the cost of compliance. Indeed, a TOM and an integrated architecture (processes, data, applications, and tools) are often lacking, despite the fact that digitization requires an overarching strategy and clear objectives. For example, universal banks have often invested in tools which come from various sources and are disconnected from each other. As a result, businesses often lack support when it comes to data, artificial intelligence, anti-financial crime and fraud efforts, and getting ahead in the war for talent.

Respondents to our survey certainly see the importance of digitization. They cited digitization and data analytics as one of the top five trends in compliance, and one third of respondents pointed to it as a key challenge for their compliance organization. Moreover, the integration of business and digital goals is seen as a major challenge among the participants. More than half (54%) claim they are well or very well positioned to adapt to the digitization trend.

However, more detailed questions on digitization maturity show there is much work still to be done. Although the majority say they are well or very well positioned to adapt to the digitization trend, more than half of respondents (52%) state that they have not advanced very far along this road. They are only just starting to air ideas and introduce pilots for one-off digital initiatives within selected parts of their compliance organization, but are not fully aware of the digital use cases that exist.

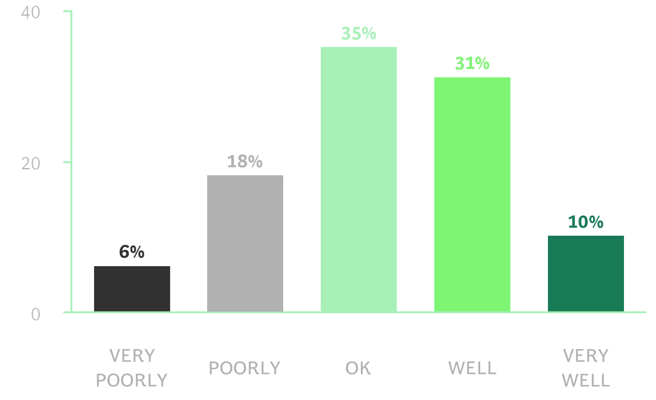
Companies with a more advanced Compliance TOM appear to have started the digitization journey earlier. They are more aware of the role digital can play, and understand data strategy. Those who say they have made considerable progress attribute their success to making digital compliance their top priority and an integral part of the CEO agenda. This finding reaffirms the hypotheses reached in the BCG ESG, COMPLIANCE AND RISK REPORT 2021.

FIGURE 5: DIGITIZATION READINESS



At the other end of the scale, 24% of respondents admitted they are dealing with the development of digital compliance strategy either poorly or very poorly. Indeed, respondents at every level of compliance maturity said they are still working on the development of a fully digitized compliance function.

FIGURE 6: DIGITIZATION READINESS



The effective application of technology in compliance requires excellent planning and careful orchestration of many different elements. Companies need to be able to analyze the vendor landscape, and ensure that the selected compliance technology fits neatly with operational needs. This in turn requires deep knowledge of data protection regulation in different jurisdictions, and an innovative, digitally oriented mindset. As with cybersecurity, the compliance workforce must comprise a diverse range of subject matter experts if it is to implement a successful digital compliance strategy. There is a growing demand for cyber risk professionals, who can bring risk domain expertise to address the increasing risks of cyberattacks and compromise.

Indeed, the slow pace of digitization within the compliance function can be mainly put down to a lack of sufficient know-how and tools. Many companies are keen to tackle the know-how gap by developing a comprehensive people strategy to attract talent with the required expertise to exploit the potential of digital across the compliance unit. A good example of such upskilling efforts would involve building up a hub team, staffed with data scientists and engineers, as well as a spoke team, comprising data scientists and engineers who only work with compliance-related projects and hence build subject matter expertise.

As companies deploy transformative Artificial Intelligence (AI) tools, they must ensure that they introduce these solutions in a responsible way, mitigating any potential risks to their business and protecting consumers. With the imminent arrival of the European Union's AI Act, one of the first broad-ranging regulatory frameworks on AI, the failure to implement Responsible AI successfully will lead to serious implications (see BCG paper "RESPONSIBLE AI FOR AN ERA OF TIGHTER REGULATIONS"). To have people who are carefully and diligently working on and learning from these technologies is of critical importance for organizations and for the people who will suffer the consequences of AI systems that are not equipped with ethical guardrails.

5. CYBERSECURITY: Addressing critical gaps

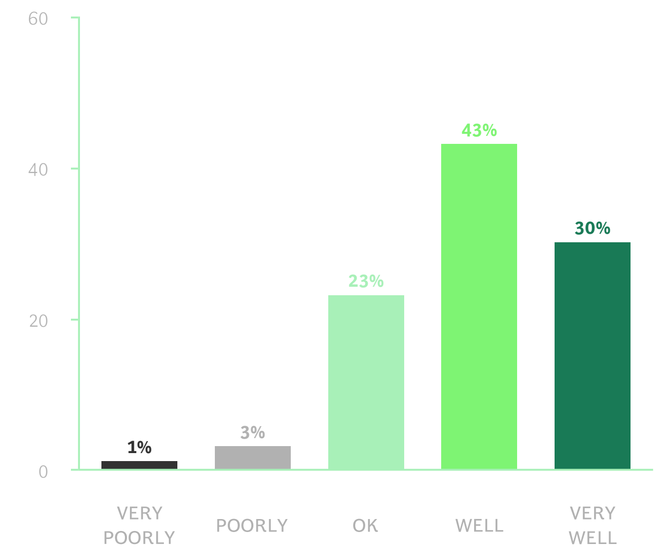
Increasing impacts from cyber and privacy attacks continue to escalate in prominence and frequency. As companies operate in an increasingly digitized way, the more they will need to assess and enhance their cyber-resilience.

When asked which topic was most relevant for their compliance organizations, the clear winner was cybersecurity. Indeed, the topic was cited by 62% of respondents, 10 percentage points more than business ethics, the next most cited topic. This comes as no surprise, given the considerable risks—to the business, customers, and reputation—in neglecting cybersecurity. Cyber threat actors are becoming more aggressive, more sophisticated, more persistent and more successful. Companies have therefore been strengthening their commitment to cybersecurity, especially amid heightened geopolitical tensions.

Many companies do not yet have adequate cybersecurity capabilities, management and governance processes, with insufficient investment in security, resilience and testing. They currently lack the right monitoring, controls and warning indicators to both prevent, respond to and recover from cyber threats. Lack of security investment, resulting in a failure to keep pace with digital investment, can exact a high price at an unknown later date. Regulation is tightening in this sphere too, for example with the Cyber Incident Reporting for Critical Infrastructure Act, signed into law in the United States in 2022. The law sought to ensure that critical private sector entities report cyber incidents and ransomware payments to the US government.

It is therefore encouraging that 73% of respondents say they are already well or very well positioned to improve performance in this regard, thanks largely to the fact that their compliance mandates include cybersecurity regulations and data protection laws.

FIGURE 7: CYBERSECURITY READINESS



Strong cybersecurity also requires good IT infrastructure management. However, more than a third (38%) of respondents say that adequate IT infrastructure remains one of their three biggest challenges, and 27% say they are not well equipped to deal with it.

To overcome these challenges and rapidly improve cybersecurity, a committed senior management must implement a top-down strategy with a persistent emphasis on identifying and protecting their highest risk assets, while the compliance departments should always be closely involved to ensure that key regulatory developments are managed and governed effectively.

Companies will need to introduce a range of cross-functional initiatives, designed to encourage collaboration, and spread diverse subject matter expertise among business units and corporate functions. Such collaboration is critical, with the goal of establishing resilient cybersecurity processes comprising various elements, such as IT, operational risk, business continuity, anti-fraud and data protection.

A critical element of cybersecurity is effective staff education and awareness of the required cyber practices. Stolen credentials are responsible for more than half of ransomware attacks, not least because passwords such as “123456” or “qwerty” are still very commonly used. Enforcing password requirements, multi-factor authentication and applying security patches are important contributory factors to the effective prevention of attacks. Threats and risks will still flourish if companies continue to overlook the human element of cybersecurity, no matter how substantial the investment in security tools and network defense. The first, and in this context the last, line of defense against cyberattacks needs to be enabled in order to ensure secure operations. Organizations should provide employees with time, education, and resources to learn more about cybersecurity, and take a human-centric approach to designing training, cyber practices and incident responses in the event of attacks.

Above all, companies need to know what cyber-risk profile they are aiming to achieve, and where the most important gaps remain. Scenario-driven exercises that simulate cyberattacks assist teams to build and develop the critical skills and experience needed for effective incident response. A comprehensive cybersecurity strategy is necessary. It should be supported by management and receive the required level of investment to maintain the organization’s cyber-risk profile within its risk appetite.

An innovative approach would be to bring customers and other stakeholders on board in striving to boost cybersecurity. A trend exists at the moment to offer hackers a bonus (bug bounties) if they manage to enter the relevant company’s system and then log and report their activity. Moreover, there is an increasing focus on collaboration and information sharing between organizations, industry sectors, governments and consumers. Cyber is a collective problem, requiring a collective response.

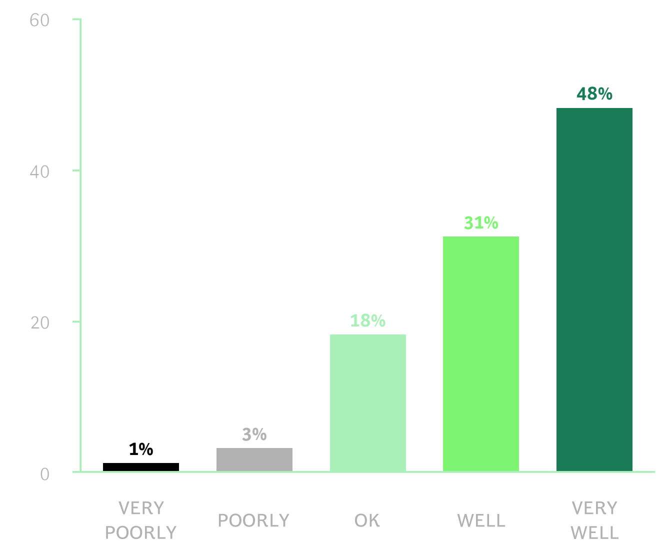
6. BUSINESS ETHICS: Establishing a culture of integrity

A culture of integrity, where employees actually practice what the company preaches on ethical business behavior, nurtures prudent decision making in difficult situations and elevates compliance departments to the position of influential and sought-after advisor.

The importance of this topic was clearly reflected in our survey. More than half of all respondents - regardless of industry and region or maturity stage - included business ethics among the top five topics most relevant to their compliance organizations. All respondents said that business ethics is a key component of proper governance.

Given the significance attached to this area, companies are keen to promote ethical behavior in their business practices. A high percentage (79%) rank themselves as either well or very well positioned in this regard, while just 4% say they are poorly or very poorly prepared. Respondents generally agree that their written codes of conduct are now well established, and have been clearly communicated to all employees (70%). Moreover, a majority report that their compliance mandates include specific risks related to business ethics.

FIGURE 8: TREND ADAPTION BUSINESS ETHICS



However, our survey suggests that many companies still struggle to create effective whistleblowing systems that promote a culture of speaking out in response to non-compliant behavior.

DEEP-DIVE: WHISTLEBLOWING

Recent regulatory action has made whistleblowing a clear priority for all compliance departments. In 2019, for example, the European Union (EU) passed their Whistleblower Directive, aimed at protecting whistleblowers. By 2023, companies with more than 250 employees in scope of the German Supply Chain Due Diligence Act must implement a system in which employees and external third parties can report potential misbehavior. In 2019, the EU passed the EU Whistleblower Directive, aimed at the protection of whistleblowers. From December 2021, companies with more than 250 employees have needed to implement a system where employees and third parties can report potential misbehavior These organizations therefore need to put in place a complaints mechanism where all people, regardless of their connection to the company, can report incidents relating to violation of human rights and certain environmental protection laws. Whistleblowers can choose to report their concerns either internally or to external authorities. In specific circumstances, they can even report their concerns publicly, through social media for example, leading to reputational damage. The identity of whistleblowers and any third parties mentioned must always remain confidential.

Given its importance in the effectiveness of whistleblowing, it is perhaps not surprising that a significant number of participants (30%) state that culture is one of their top five overall compliance challenges. A sustainable ethical culture with robust compliance and a strong sense of integrity leads to three major commercial benefits: it creates economic advantage for companies, prevents substantial fines and reputational damage, and helps to attract and retain key talent.

But what are the necessary elements that combine to create such a sustainable compliance culture? One important success factor, widely accepted in the compliance community, is clear leadership behavior. The success of an ethical culture greatly depends on executives setting the tone from the top, acting as role models in living up to cultural standards. One quarter of our respondents say that establishing a "sense of urgency from senior management" is among the top five challenges for their compliance organization. Every employee should be fully aware that compliant behavior is vitally important for the whole organization and that senior management will be held accountable for any misconduct.

Companies can find it difficult to establish a compliance culture that incentivizes employees to live a culture of integrity and indulge in the right behaviors. Making guidelines simpler for employees would certainly help. An unwieldy number of rules that are difficult to put into practice hinders effective and successful compliance. Making the processes user-friendly, on the other hand, will boost compliance with standards and foster an ethical culture. The target culture should be articulated clearly, providing enough use cases to demonstrate the connection between concept and business practice, so that employees all immediately recognize what correct behavior looks like and can report things they believe are not right.

Certain factors that are vital in building the right culture - the tone from the top, accountability, incentives and communication - can be measured and controlled. Indeed, data and technology can be put to good use here. Digitization can certainly also make it more straightforward for employees to be compliant due to the greater ease of communicating and following due process. See also the BCG publication PERSPECTIVES ON MONITORSHIPS AND SUCCESSFUL COMPLIANCE TRANSFORMATION – A BCG COMPLIANCE MAGAZINE SPECIAL ISSUE.

7. WORKFORCE: Securing the right skills

Because ESG, risk and compliance have become more complex, and the demands of agile, customizable collaboration models have grown, the compliance team needs to incorporate a more diverse skillset, involving a range of technical know-how, subject matter experts and take on various roles. This increase in demands for compliance workforce coincides with a tense labor market where finding candidates is a challenge already. Qualified employees have more demands and expectations towards ethics and ESG. More than anything else, it is now the quality of the workforce that determines the success of a company's compliance management. A strong workforce strategy – involving recruiting new people and upskilling current employees - is therefore essential in unlocking the potential for compliance as a competitive advantage. A human resources department that effectively manages this strategy and mitigates risks will raise a company's standing in the market.

Attracting new talent, devising hiring strategy, ensuring the availability and capacity of training, and retaining employees in the midst of the Era of Great Resignation, are all issues faced by companies across all industries in our survey. When asked about the challenges they foresaw for their compliance organization, almost 70% of respondents pointed to "attracting talent," a far higher proportion than for any other option.

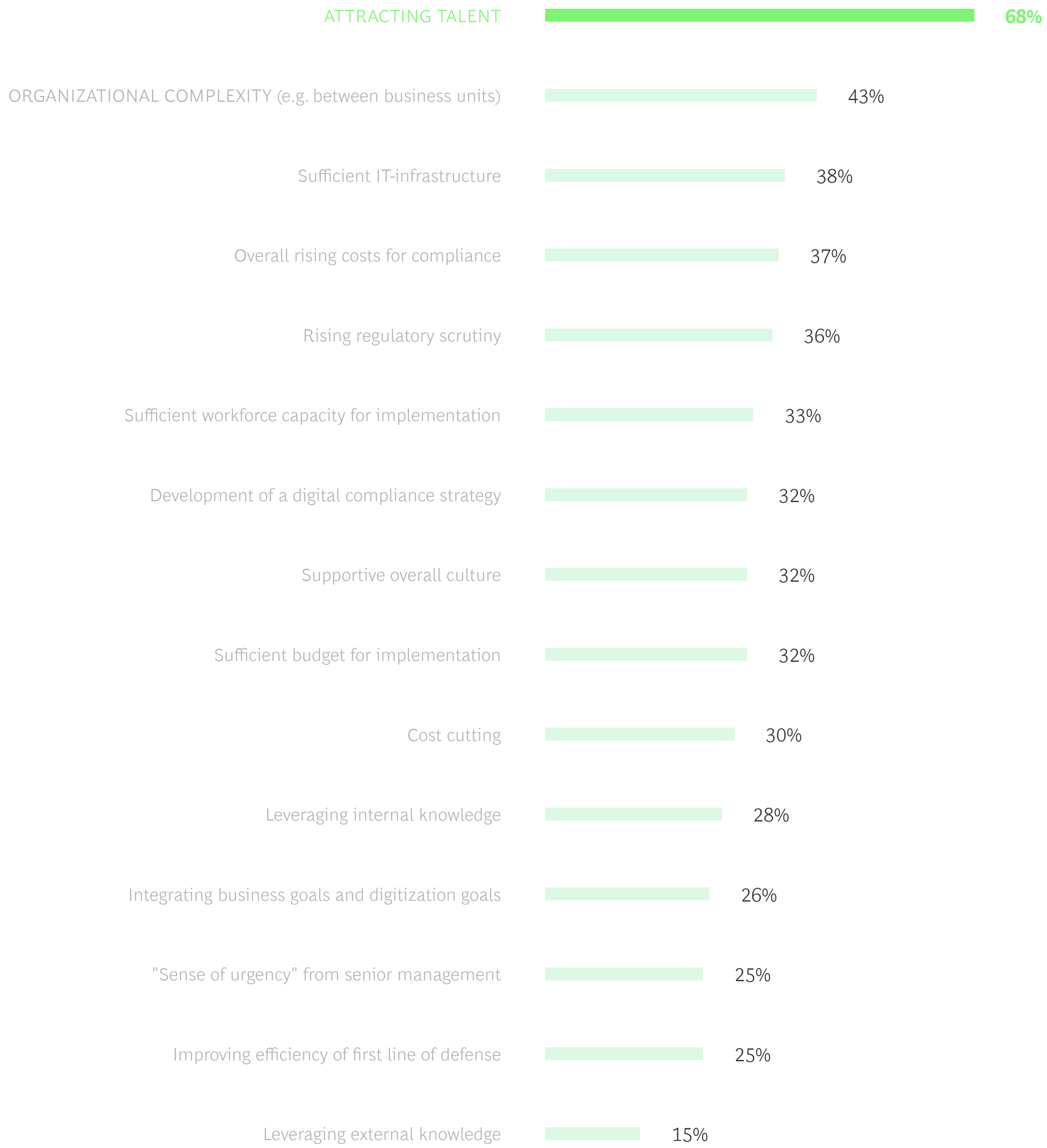
Moreover, the survey reveals that all companies regardless of industry have yet to find the ideal strategy in response, saying that they are merely adequately, or even poorly, positioned for this challenge. Moreover, attracting talent is unlikely to get any easier, given that 68% of respondents say the required range of qualifications for roles in their compliance organizations - comprising skillsets, expertise, and technical qualifications - is only likely to expand, and a further 18% say it will expand significantly.

The growing importance of cybersecurity and the digitization of compliance activities are a major concern among respondents when considering the future of the workforce. Subject matter expertise, cross-functional collaboration, and an awareness of the ever-growing inventiveness of hackers and cybercriminals will be essential. The workforce of the future will need to stay up to date technologically and adapt quickly to changing risks and regulations.

As was reflected in respondents' concerns, the requirements for the future workforce extend well beyond technical know-how. As the risk and compliance environment grows increasingly complex, the emphasis on strong business ethics will only increase, encouraging employees to make their own ethical assessments of what is right and wrong. Simply ticking boxes indicating compliance with various regulations will no longer suffice.

The growing emphasis on ESG and other topics obliges the compliance workforce to keep abreast of developments, see the bigger picture, apply their expertise to new areas and think along more global lines, while keeping pace with the required new collaboration model to manage risk cross-departments. As the social component of ESG grows in importance, companies will need to be sensitive to the human rights risks that flow from working with multiple suppliers and global sources.

FIGURE 9: CORE CHALLENGES FOR COMPLIANCE ORGANIZATIONS IN THE FUTURE



Political issues are encroaching more than ever on the global economy. Compliance professionals must therefore be able to identify and analyze complex scenarios, and consider both political and economic factors. This will help to ensure that their company's compliance strategies, and how they are implemented, are flexible enough not just to react to events but to anticipate them and prepare accordingly.

The attitudes of employees are also changing, and companies must adapt accordingly to attract them and keep them on board. Members of Generation Z in particular—those born between 1995 and 2010—say they want their work to add value to society, and care more about ESG when choosing their employer. Moreover, new employees expect companies to allow for remote working and offer state-of-the-art digital technologies and work processes.

As the talent war intensifies, companies therefore need to manage their ESG-related reputations with care, and think differently about their working practices and their impact on risk and compliance. In some sectors in particular, companies are heavily burdened by the effort required to prevent ESG violations and implement social compliance throughout their supply chains, and by the constant threat of regulatory retaliation and reputational damage.

This is particularly true for industrial goods and healthcare companies. The implementation of due diligence in 3TG (tin, tungsten, tantalum and gold) supply chains enables responsible sourcing of 3TG from countries like Nigeria. New regulations and campaigns against bribery and corruption in many countries have raised the bar for supply chain compliance risk management in all industries. The general population sets higher standards for public or private sector entities in healthcare in particular. Many of these organizations need to make significant enhancements to the current relevant supply chain and business partner due diligence processes, e.g. by raising the level of automation. In this way, they can avoid regulatory scrutiny, negative headlines and loss of face with their own workforce.

Simply advertising for a position will not achieve the requisite results. Companies need to be more imaginative in their talent strategies, more aware of diversity and inclusion, and ready to respond to the demand for a more flexible workplace. They also need to be careful that the rapid expansion of compliance organizations - 57% expect them to increase in size – does not damage efforts to establish the right culture, given the difficulty of transmitting company values to many new joiners at the same time.

Recruiting new people alone will not be sufficient in building the right workforce. As technology advances and workplace strategies evolve, existing employees will need to be trained in relevant new knowledge and skills. Training capacity, including substantial ramping up of relevant IT capabilities, should therefore be greatly expanded.

Indeed, companies need to develop a clear and comprehensive workforce strategy that does not leave the company vulnerable to skills deficiencies at any given time. Our survey makes clear that compliance organizations should be equipped with a diverse skillset that can deal with all relevant types and areas of risk, and can fulfill the various roles required within flexible collaboration models. In a more competitive world, companies should pinpoint exactly what skills they most need, where they can be found and how they can be developed. It is not feasible to fight for talent on all fronts, and companies must therefore focus on their priority areas.

CONCLUSION

Companies need to take action in various areas in order maximize the value creation of their compliance organizations. They need to define the precise mandate of the compliance function for each type of risk, define an adequate approach of its role to address the different demands, and clearly allocate other relevant responsibilities across different departments. Plans for swifter and nimbler crisis response can minimize the impact of major geopolitical events that have bedeviled businesses in recent years. On environmental, social and governance issues, they have to bridge the gap between their communicated ambition and the often much more modest reality.

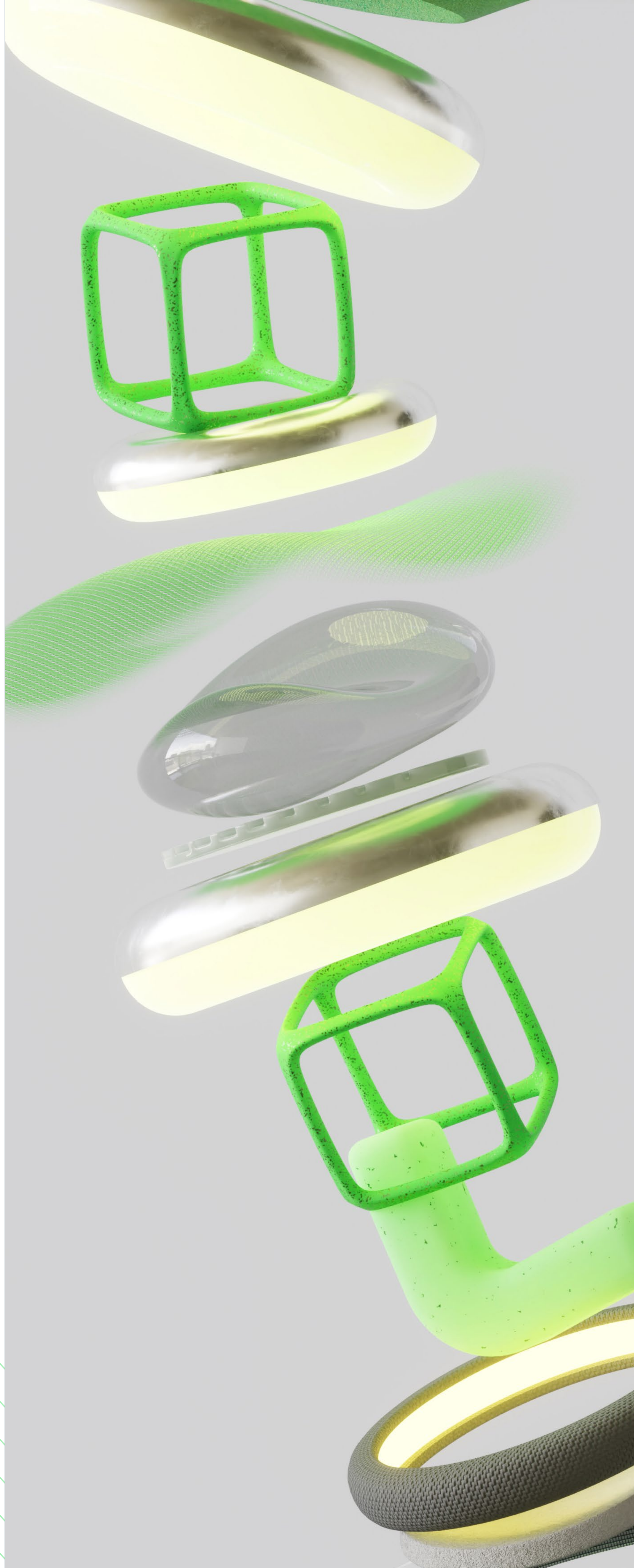
Many companies have fallen dangerously behind in the digitization journey. As they hurry to rectify this situation, they need to maintain their focus on what the clients want and what their business needs. On cybersecurity too, they often have much ground to make up, and senior management should urgently implement a comprehensive value-for-money strategy and a range of cross-functional initiatives. To foster ethical behavior, companies must take the necessary steps to change the culture, and make it simpler for employees to voice any concerns. Regulators, investors, customers and employees are probing this gap with increasing energy and concern.

But of all the factors that make for a successful compliance organization, the right workforce is essential. No such organization can prosper, therefore, without a prudent workforce strategy that considers how best to attract, retain, motivate, and train their people. Given the clear need for a more diverse skillset addressing the functional demand as well as the role flexibility, the definition of an appropriate people strategy is key.

FOR FURTHER CONTACT

If you would like to discuss this report, please contact one of the authors.

11/2022



ABOUT BCG

Boston Consulting Group (BCG) partners with leaders in business and society to tackle their most important challenges and capture their greatest opportunities.

BCG was the pioneer in business strategy when it was founded in 1963. Today, we work closely with clients to embrace a transformational approach aimed at benefiting all stakeholders—empowering organizations to grow, build sustainable competitive advantage, and drive positive societal impact. Our diverse, global teams are passionate about unlocking potential and making change happen, delivering integrated solutions through leading-edge management consulting, technology and design, and corporate and digital ventures.

Whether you want to advance an idea, a capability, or the world at large, BCG is with you every step of the way. We excel in the business of human potential, and believe in its power to shape strategic, organizational, economic, and societal change.