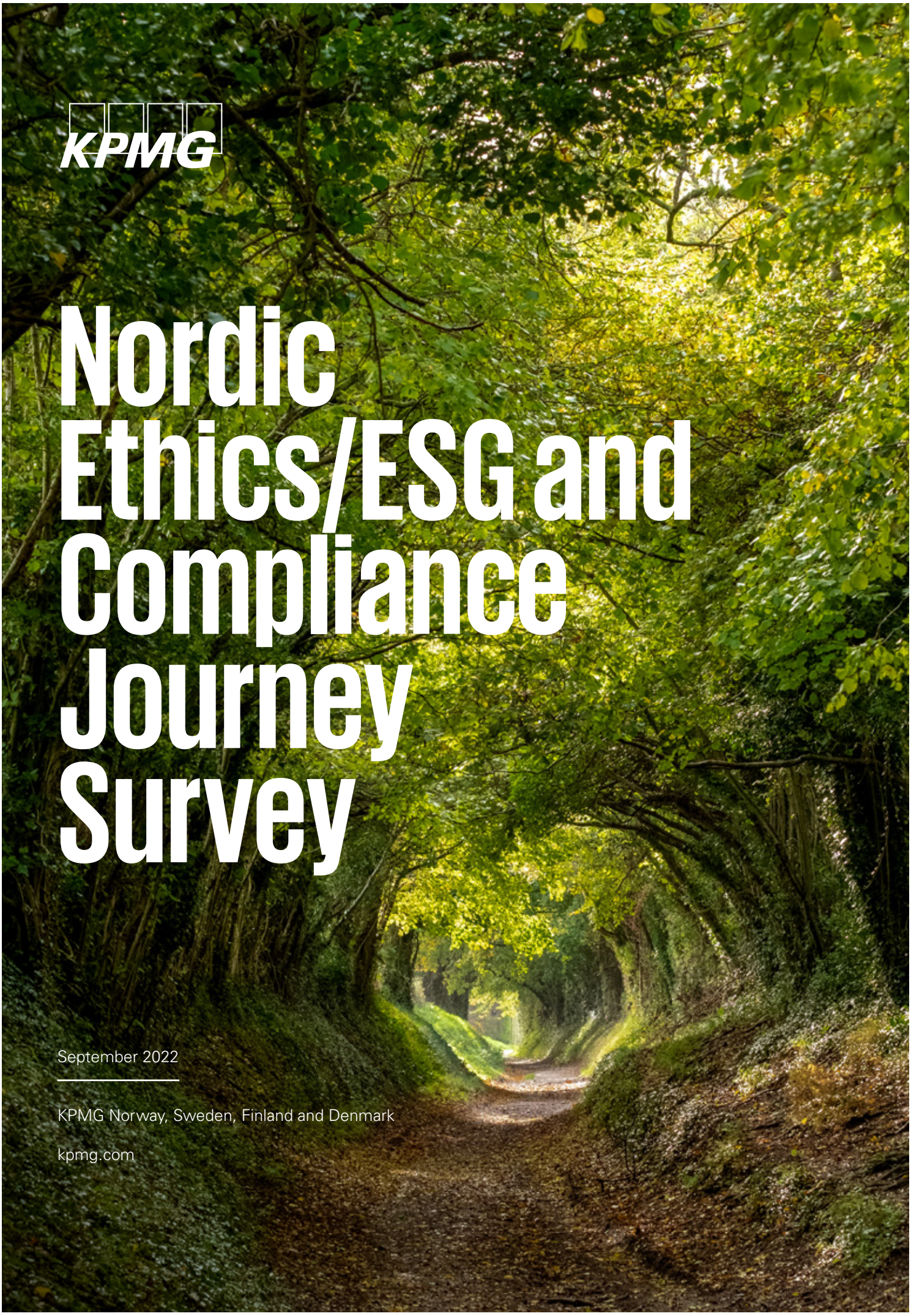


Nordic Ethics/ESG and Compliance Journey Survey

September 2022

KPMG Norway, Sweden, Finland and Denmark

kpmg.com

Contents

Executive summary

→ 4

About the respondents

→ 7

The compliance journey continues

→ 8

Diving into:

9 Tone and action from the top

12 Roles and responsibilites

14 Policies and procedures

15 Risk management

17 People and skills, communication and training

19 Control activities, monitoring, and testing

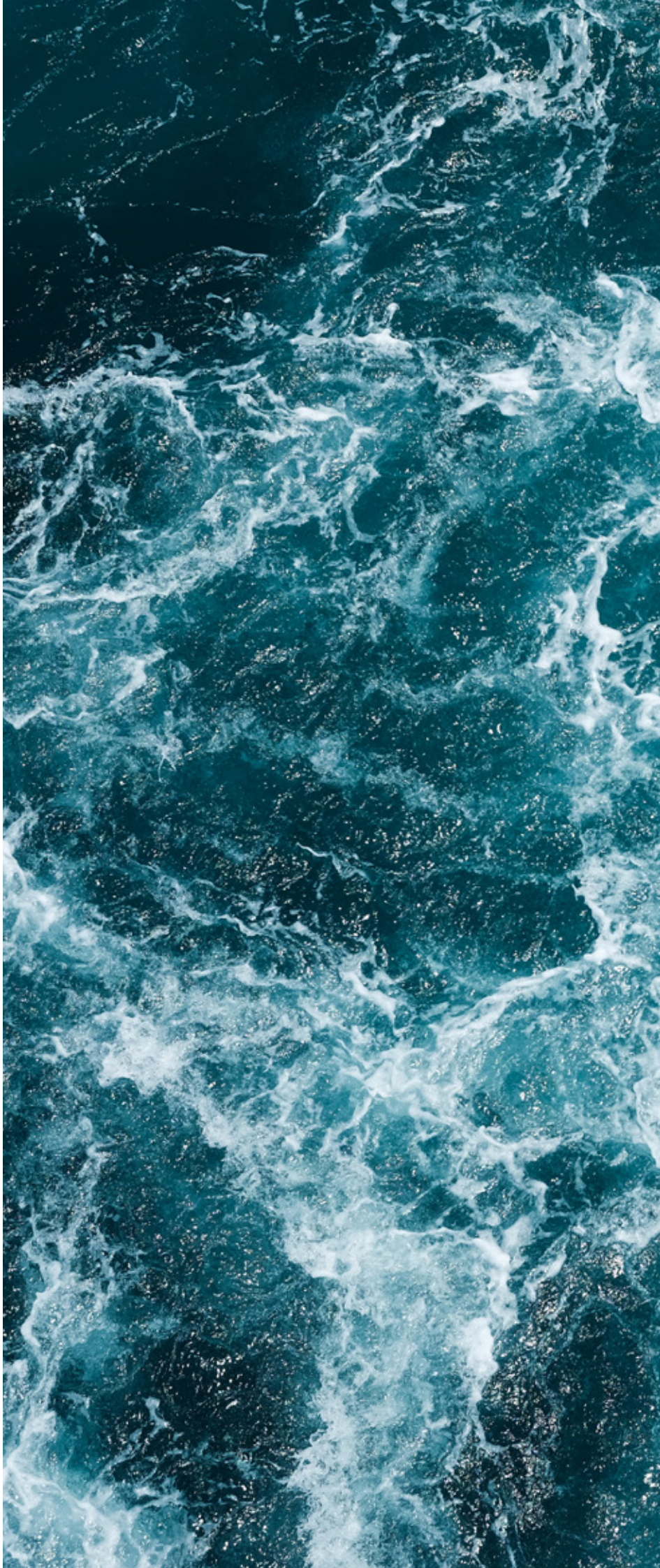
21 Issue management, whistleblower mechanism, and investigation

23 Reporting, consequences and learning

24 Technology and data analytics

Conclusion

→ 25



Preface

We are pleased to share with you the results of this year's Nordic Ethics/ESG and Compliance Journey Survey. Building and maintaining credibility and trust is a key success factor for companies. We hope that this report gives you additional insights useful for your own compliance journey.

The results of the survey reflect that companies are facing complex challenges, implying the need for a consistent and systematic focus on compliance at all levels in the company, starting with the Board of Directors. "Everything is connected to everything," and companies will need to break down the silos between "E", "S" and "G" in terms of roles and responsibilities and processes.

- **The ESG risks are complex and dynamic:** The war in Ukraine, the renewed COVID-19 lockdowns, and supply chain crises are increasing the inherent risk of breaching sanctions, the risk of corruption and facilitation payments, as well as the risk of breaching human- and labor rights and environmental laws and regulations.
- **Regulators are getting tougher on ESG breaches:** There are increasing expectations in laws and regulations related to preventive, detective, and response activities. There is an increasing focus from banks on requests for information on how companies work with ESG. Sanctions and trade controls are highly complex and constantly changing. The Norwegian Transparency Act entered into force in July 2022 and introduced stricter requirements related to human rights in supply chains than seen in most, and likely all, other countries.
- **An increasing amount of data to monitor and control:** An efficient use of new and emerging technologies allows for a more data-driven, efficient, and agile compliance function creating a shared space for cross-functional collaboration and ensuring compliance is a seamless part of day-to-day business operations.
- **Professional investigation and learning processes:** Investigations of reports of misconduct require neutral and professional assessments of factual grounds. Equally important is addressing the root causes of the problems rather than just fixing the symptoms, to ensure learning across the whole organization.

Do not hesitate to contact us; we are happy to meet with you to further discuss the results and our recommendations!

Kind regards,

BEATE HVAM-AXELSEN
Head of Business Integrity & Compliance Partner
KPMG Norway

ANTTI AALTO
Head of Legal Compliance, Finland, Co-Head Global Legal Compliance
KPMG Finland

MARTIN KRÜGER
Head of Forensic
Partner
KPMG Sweden

JON BECK
Head of Audit and Partner
KPMG Denmark

Executive summary

The majority, **73%, of the companies that have participated this year have more than 1000 employees globally, representing some of the biggest companies in the Nordics across industry segments.** Around **40% of the companies have more than 5000 employees.** Most respondents agree that their customers and bank connections have expressed increasing expectations for how the company manages ethics/ESG risks. As a general overarching mandate, applicable external guidelines require that companies "exercise due diligence to prevent and detect criminal conduct" and "otherwise promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law." It is critical that the company's compliance program is **proportionate to the business operations, risk-based, and regularly reviewed and updated.** To demonstrate that the company's Compliance program meets the objectives, external guidelines and regulations, the program should include preventive-, detective and response activities. In the table below we have summarized the key findings per activity.

	Elements of a robust Compliance Program	Maturity	Trend	Summary of key findings, 2022 survey
Prevent	Tone and action from the top			A large majority of respondents, 87%, state that the tone and action regarding ethical behavior is strong and explicit from their top management. The BoD reviews and approves the compliance program in close to 70% of the companies. 57% of the companies have implemented compliance related KPIs. 85% agree that the management understands the actual ethics/ESG risks the company is exposed to. We note a significant improvement since 2021.
	Roles and Responsibilties			Only 50% of the respondents agree that line management takes responsibility for compliance. This is approximately the same result as in 2021. There are only small differences between type of ownership and industry segments. Many companies continue to strengthen the 2nd line compliance function. This is a red flag. The first line owns and manages operational risks and must therefore ensure compliance in daily business.
	Policies and procedures			Nearly all participating companies have established a Code of Conduct which clearly communicates management expectations. The survey doesn't cover other specific policies and procedures, but KPMG's general observation is that policies and procedures tend to be in place, but not necessarily the operationalizing of these.
	Risk management			Risk management can be significantly improved in most companies as around 40% of the respondents do not agree that the company is conducting regular and systematic ethics/ESG compliance risk assessments. 92% agree that the management has a strong focus on mitigating governance risks and 69% agree that the management has a strong focus on mitigating environmental risks. Only 63% agree that the management has a strong focus on mitigating social/human- and labor rights risks. This survey shows that close to all participating companies include ethical requirements in their contracts with business partners. However, most companies are lacking a systematic approach to assess compliance with the ethical requirements.
	People and skills, communication and training			Around 30% of the respondents do not agree that the company has a risk-based ethics/ ESG compliance training program. This indicates that the respondents think that the training is "too general and "basic" and not adapted to the actual risk-exposure of the different roles in the company.
Detect and respond	Control activities, monitoring and testing			Close to 60% of the respondents agree that the company has effective controls in place to mitigate ethics/ESG compliance risk. On a general note, KPMG notes that many companies are struggling to define effective controls. Testing of the controls tends to be absent or performed sporadically.
	Issues management, whistleblower mechanism and investigations			In general Nordic companies have established whistleblowing mechanisms. 78% agree that employees trust that all whistleblowing reports will be followed-up professionally. 73% agree that business partners are encouraged to report identified concerns or misconduct through their whistleblowing channel.
	Reporting, consequences and learning			A large majority, 82%, agree that breaching the company Code of Conduct has appropriate consequences for involved employees. However only 61% agree that suppliers or other external parties that breach the company ethical requirements are sanctioned appropriately. Around 70% of the participants agree that the company takes efficient learning from the result of internal controls and other compliance findings.
	Technology and data analytics			Companies continue struggling to leverage technology tools. Only 34% of the respondents agree that they are leveraging necessary and effective technology tools to mitigate ESG-related risks. Only 25% of the respondents who have rated their maturity as high (maturity levels 4 and 5) agree to the statement.

The highest rated risk event - cybercrime and extortion - reflects recent trends in the Nordics, with cyberattacks hampering businesses across industries (see risk ratings on next page). The Norwegian Authority for Investigation and Prosecution of Economic and Environmental Crime's annual threat assessment for 2022 and other Nordic reports are pointing at areas within the field of cybercrime and consider it highly likely that there will be increased use of deepfake for CEO fraud, and such fraud attempts will be automated and increasingly adapted to the individual recipient.

Governance and environmental risks are dominating the Top 10 list. Around 70% of the respondents agree that their company is impacted by the new sanctions on Russia in 2022.

Despite stricter regulations and other factors such as the war in Ukraine and consequences of Covid on the supply chain contributing to increased inherent risks related to breaches of human-and labor rights, respondents do not seem to consider that there is any material risk of breaching human and labor rights. This may be due to the fact that the legal and financial consequences related to breaches of human and labor rights so far has been limited compared to breaches related to, for example, sanctions corruption, and money laundering.

The large majority

92 % of the respondents who have rated their maturity as high (maturity levels 4 and 5) agree that the company has been impacted by new regulations in 2022.

81 % agree that the customers have expressed increasing expectations to how the company manages ESG risks. In particular respondents from the "basic resources industry segment strongly agree".

73 % agree that the banks have expressed increasing expectations to how the company manages ESG risks.

Only

26 % disagree that the risks with respect to corruption and financial crime have increased during the last year.

30 % disagree that the risks with respect to human- and labor rights have increased during the last year.

How each risk event is on average considered across all respondents

Significant increase in risk level during the last year

Cybercrime and extortion

Sanctions

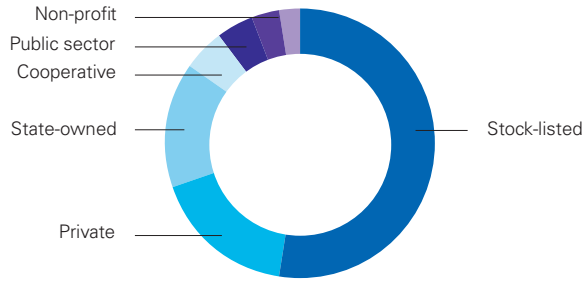
Sharing of sensitive information

Environmental risks

Respondents submitted what they assume to be their company's risk probability for the above listed events. Topics receiving recent attention, such as cybercrime and extortion, sanctions, sharing of sensitive information and environmental risks have had a significant increase in risk level in comparison to our 2021 survey.

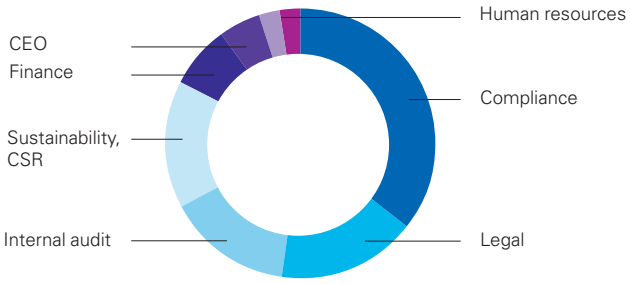
About the respondents

Ownership



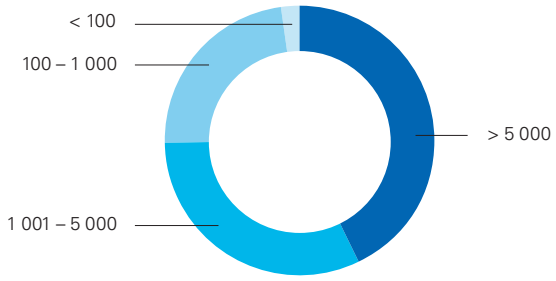
- The majority of the companies are stock listed or privately owned (not listed).
- State-owned companies are also in scope of the survey.

Function



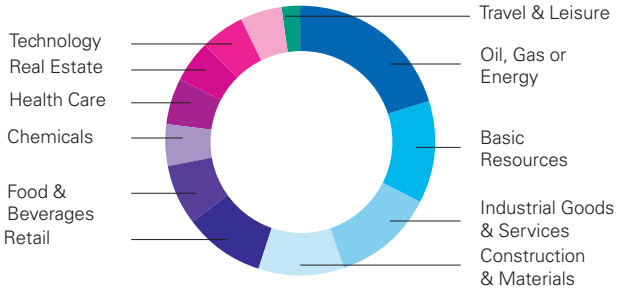
- Respondents are mainly placed in the 2nd line, within Compliance, Sustainability and Legal.
- Internal audit representatives are also participating.

Employees



- 73% of the companies have more than 1 000 employees globally, representing some of the biggest companies in the Nordics across industries.
- 40% of the companies have more than 5000 employees

Industries



- The survey represents companies across industries, including amongst other companies in Gas and oil, industrial goods and services, and basic resources.

The Ethics/ESG and Compliance Journey Survey 2022 includes responses from 49 Nordic companies, representing:

- Mature companies in the Nordics,
- International companies which operate globally, in a complex, international regulatory environment with local and international compliance obligations operating in 21 industries.

The compliance journey continues...

diving into the different elements of a robust compliance program

Tone and action from the top

It is imperative that the tone and action from the Board of Directors and Management is strong, visible and explicit. Management should create and foster a culture of ethics and compliance with the law, demonstrate exemplary conduct at the top with rigorous adherence, and clearly convey, in unambiguous terms, the firm's ethical standards, including consequences for misconduct. Indeed, the most important business decisions are taken by the top management. All managers and staff must be held accountable for compliance with ethical/ESG requirements, with known consequences as well as associated incentives.

Results

87 % agree that the tone and action of ethical behaviour is strong and explicit from top management. There are only small differences between ownership and industry segments.

However, **only 54%** of the same respondents that agree to this at the same time agree that the Line Management takes ownership of their respective risks within compliance. So, is the tone and action then truly explicit?

70 % agree that the Board of Directors annually reviews and approves the compliance program.

57 % agree that the company has implemented key performance indicators related to compliance.

85 % agree that the **management understands** the **actual** ethics/ESG risks the company is exposed to. There are only small differences between ownership and industry segments

35 % answer that they are "Neutral/do not know" to the statement "Our management has a high-risk tolerance" (degree of risk that the management is willing to take). As many as **50%** of the respondents who have rated their maturity as high (levels 4 and 5) disagree with the statement.

U.S. Department of Justice Criminal Division "Evaluation of Corporate Compliance Programs"

"The company's top leaders – the board of directors and executives – set the tone for the rest of the company. Prosecutors should examine the extent to which senior management have clearly articulated the company's ethical standards, conveyed and disseminated them in clear and unambiguous terms, and demonstrated rigorous adherence by example. Prosecutors should also examine how middle management, in turn, have reinforced those standards and encouraged employees to abide by them."

The "tone and action from the top" should be a powerful demonstration of leadership and a hallmark of effective compliance programs. The Board plays a key role in promoting an organizational culture that encourages ethical conduct and a commitment to compliance. This is reinforced by the survey results, in which 70 % of the respondents' state that their Board today annually reviews and approves the compliance program. This is best practice, although I do think that the goal should be 100% considering the size and nature of the businesses represented by the respondents.

Erik Arvnes
Head of Investigation & compliance and Partner Forensic
KPMG Norway

Understanding the actual risks the company is exposed to is fundamental in order to design a robust compliance program. Equally important is having an agreed, common understanding of the level of risk appetite across the organization, starting with the top management and Board of Directors. When 35% answer that they do not know/or are neutral to the statement "Our management has a high-risk tolerance" this may indicate that the respondents, in majority compliance officers, do not have sufficient level in-depth discussions with the top management and Board of Directors regarding the risk appetite.

Beate Hvam-Axelsen
Head of Business Integrity & Compliance and Partner
KPMG Norway

There are several ways to improve a company's tone at the top, one being supportive to report misconduct. Employees should be able to report misconduct that occurs at the company, without fear of retaliation. Providing safe channel(s) for employees to report misconduct or unethical behavior helps companies to detect and prevent any undesirable behavior.

Martin Krüger
Head of Forensic, Risk & Compliance Consulting
KPMG Sweden

Important guidelines on compliance programs

- ISO 37301 Compliance management systems
- ISO 37001 Anti-Bribery management systems
- US. Department of Justice Criminal Division (DoJ) Guidance on corporate compliance programmes
- SFO Operational Handbook (evaluation of compliance programmes)
- ISO 26000 Social Responsibility
- IIA Guidelines for the Compliance Function
- OECD Due Diligence Guidance for Responsible Business Conduct
- Nordic regulatory guidance, e.g., Økokrims' checkpoints

ISO 37301 Compliance management systems

ISO 37301 was released 13 April 2021, replacing ISO 19600. It specifies requirements and provides guidelines for establishing, developing, implementing, evaluating, maintaining and improving an effective compliance management system within an organization. This document is applicable to all types of organizations regardless of the type, size and nature of the activity, as well as whether the organization is from the public, private or non-profit sector.

Quote from the US. Department of Justice Criminal Division (DoJ) Guidance on corporate compliance programmes

There are three fundamental questions a prosecutor should ask:

1. Is the corporation's compliance program well designed?
2. Is the program being applied earnestly and in good faith? In other words, is the program adequately resourced and empowered to function effectively?
3. Does the corporation's compliance program work in practice?

Roles and responsibilites

The Board of Directors (BoD) has an overall oversight responsibility for compliance, internal control environment and risk management of the company. External guidelines impose expressed responsibility of the Board to know how the compliance program works and to oversee its implementation. While guidelines do not specify how Boards should meet these obligations, the oversight function is often assigned to the Board Committee (e.g., Audit Committee). Regardless of how the Board's oversight is organized, BoD should review and approve key elements of the Compliance program and exercise regular and visible oversight. The three-line model provides a high-level overview of the roles and responsibilities for risk ownership (management), risk control (compliance, risk management) and risk assurance (internal audit) and distinguishes between three internal groups (or lines) that are involved in the processes. The first line owns and manages operational risk and must therefore ensure compliance in daily business transactions and the adequacy of internal control performed by employees in this line, e.g., sales, procurement, export, clerical staff and other such functions. Good practice is that the Compliance function / Compliance officer has autonomy and independence, in other words direct and independent access to the CEO and top management and a formalized independent reporting to the Board (or subcommittee).

Results

50 % agree that **line management (1st line – operational units)** takes responsibility for compliance. 45% of the respondents with > 5000 employees (40% of the respondents) agree. There are only small differences between type of ownership and industry segments.

82,5 % agree the compliance function established is independent from type of ownership. It is however particularly common for Norwegian listed companies where 90% have an established compliance function. 80% of the respondents with > 5000 employees have a dedicated compliance function.

78 % State owned and partly state-owned companies have established an internal audit function (3rd line). 95% of the respondents with > 5000 employees have a dedicated internal audit function.

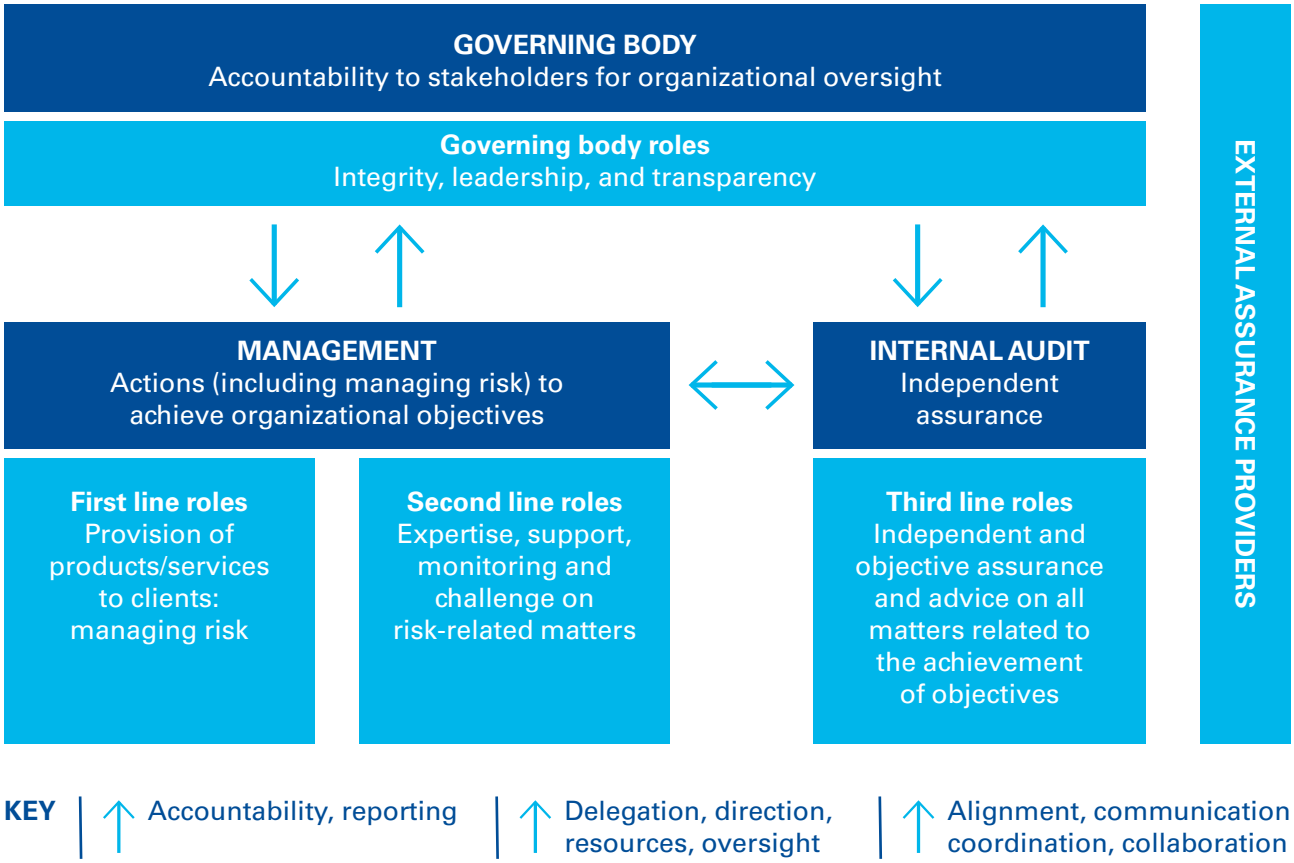
68 % privately owned companies (both listed and not listed) have established an internal audit function (3rd line). Note that all Finnish companies participating in the survey have established this function, while it is varying in the rest of the Nordics.

60 % Agree to the statement that the 3 lines – "the operational units (1st line), compliance resources (2nd line) and the internal audit (3rd line) operate in "silos" – the activities are not integrated"

Interestingly, **42%** of the respondents who have rated their maturity as high (maturity levels 4 and 5) agree with the statement, only **33%** disagree, and the remaining answer neutral/do not know.

From an internal audit perspective I see a red flag that 40% of the respondents' state that the company does not have effective controls in place to mitigate ethics/ESG compliance risk. However, this is in line with what we observe in the market, where risk and climate/ESG are not sufficiently integrated into the corporate governance system. The Norwegian Financial Authority has from autumn 2019 stated that climate and ESG risks should be integrated into strategy, pricing, product development and risk management.

Kenneth Hansen
Head of Internal Audit services
KPMG Norway



IIA's Three Lines Model

Policies and procedures

The maturity and sophistication of a company's internal policies and procedures within business ethics/ESG and compliance, such as anti-bribery, corruption, and human rights is a strong indicator for overall corporate governance. Policies and procedures should aim to reduce risk identified through risk assessments and to give content and effect to ethical norms, including the organization's code of conduct, by incorporating the organization's culture of compliance into day-to-day operations. Policies and procedures should be communicated to all employees and relevant third parties (e.g., suppliers, agents, JV partners), and any linguistic or other barriers to foreign employee access should be addressed.

Results

95 % agree that the company has established code of conduct which clearly communicates management expectations.

We note that 92% of the respondents who have rated their maturity as high (maturity levels 4 and 5) agree.

Example: Document hierarchy

Code of Conduct (Board of Directors)

Policies (Board of Directors/Management)

Manuals/Procedures (Policy-owners)

» Mandatory governing documents for all employees
» Regular reviews and updates

Other guiding documents

Routines within units etc.

» Must be consistent with corporate governing documents above

U.S. Department of Justice Criminal Division "Evaluation of Corporate Compliance Programs"

"Any well-designed compliance program entails policies and procedures that give both content and effect to ethical norms and that address and aim to reduce risks identified by the company as part of its risk assessment process. "

As many as 95% of the companies participating in the survey have established a Code of Conduct. A Code of Conduct is an overarching document and a communications tool to make the internal framework of rules accessible and understandable to the relevant stakeholders. However, we see that companies are struggling in pushing compliance accountability to the operational units as only 50% confirm that the 1st line takes responsibility for compliance. It is important to establish policies and procedures which clearly define the responsibilities of all roles in the organization with regards to compliance activities such as risk assessments, controls, reporting, training and awareness initiatives to further enhance accountability in in the 1st line.

Ingve Rasmussen
Compliance advisory and transformation consultant
KPMG Norway

Risk management

Understanding a company's risk exposure is critical to ensure that accurate actions are defined to mitigate the risk. Good practice in the industry today is to align and integrate the ethics/ESG compliance risk assessment process with the company's end-to-end strategy and risk assessment process. Ethics/ESG compliance risk assessments should be done bottom-up, involving employees in risk exposed positions. Companies must engage in ongoing monitoring of the third-party relationships through updated due diligence, training, audits, and/or annual compliance certifications. Contracting should include ESG related provisions and audit rights.

Results

65 % agree that the company conducts regular and systematic ESG related risk assessments covering internal and external risks. 70% of the respondents with >5000 employees agree. There are only small differences between ownership and industry segments. Interestingly, as many as 25% of the companies who have rated their maturity as high (levels 4 and 5) disagree, indicating in particular need for improvement with respect to the supply chain risk management.

92 % agree that the management has a strong focus on mitigating **governance risks**

69 % agree that the management has a strong focus on mitigating **environmental risks**

63 % agree that the management has a strong focus on mitigating **social/ human– and labor rights risks**

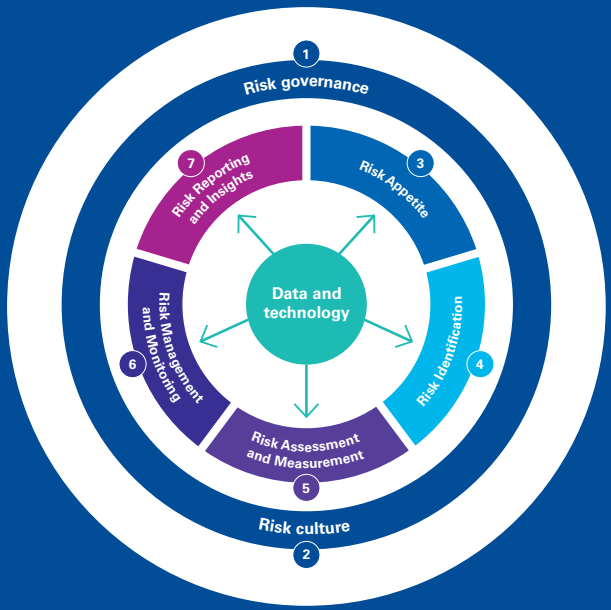
90 % agree that the company includes ethical requirements (e.g., Supplier Code of Conduct) in contracts with suppliers.

80 % agree that the top risks are prevalent due to potential misconduct in the Company's supply chain.

60 % agree that the top risks are prevalent due to potential misconduct by the Company's own employees.

40 % agree that the top risks are prevalent due to potential misconduct by the Company's contracted in-staff.

30 % agree that the top risks are prevalent due to potential misconduct by agents/intermediaries acting on the Company's behalf.



Our clients have moved beyond traditional integrity due diligence in their efforts to understand the reputational risk associated with their third parties – now their due diligence embraces all aspects of an ESG perspective. So over time, I expect that the 69% of respondents who agree that management has a strong focus on mitigating environmental risks and the 63% of respondents who agree that management has a strong focus on mitigating social/ human/labor rights risks will increase to be more aligned with the 92% who agree that management has a strong focus on mitigating governance risks. The survey results also reflect the importance of clear communication around ethics with not just the largest third parties but all the way down the supply chain.

Christy Lorgen
Head of Corporate Intelligence
KPMG EMEA

Organizations are facing a changing geopolitical and regulatory environment related to sanctions, corruption, and human rights. This highlights the need for organizations to proactively update its risk assessments and monitor those risks to ensure responsible business conduct.

Gard Heggelund
Compliance advisory and transformation consultant
KPMG Norway

The Transparency Act introduced this year in Norway triggered business and human rights attention, generated important compliance discussions, and already caused amendment across industries. Similar legislation has been proposed in other countries and the EU, changing the game for those businesses ignoring actual or potential human rights violations and compliance in their operations and supply chains. As a result of increased legislation we expect good practices to further develop, creating market opportunities for businesses with robust ESG compliance frameworks in place.

Eivind Pytte Ødegaard
Head of Responsible Supply Chain
KPMG Norway

People and skills, communication and training

Good practice is to establish a mandatory training program covering the Code of Ethics for all employees and hired-in personnel. The trainings should be conducted at onboarding and repeated annually. It is important to keep records of participants in the training in line with expectations in DoJ/ISO/IIA. In addition to the general Code of Ethics training, organizations should establish mandatory tailored compliance training for roles with high exposure to compliance risks, such as general managers including the members of the Board of Directors, finance and procurement personnel.

Results

57 % agree that the company has a risk-based ethics and compliance training program tailored to different roles in the company. There are only small differences between ownership and industry segments.

Many companies have today implemented basic Ethics/Code of Conduct trainings – for example eLearning programs – which are mandatory for all employees. However, all training is not relevant for all and the different roles in a company are exposed to different types of ethics/compliance risks.

U.S. Department of Justice Criminal Division "Evaluation of Corporate Compliance Programs"

"Prosecutors should assess the steps taken by the company to ensure that policies and procedures have been integrated into the organization, including through periodic training and certification for all directors, officers, relevant employees, and, where appropriate, agents and business partners."

Having employees meet a standard of compliance training ensures that an organization has secured legal accountability. If, however, employees see that the leadership of their company is not following the compliance training, then they will not either. Engagement from the top or "practice what you preach" is crucial.

Olesya Brodin
Risk & Compliance Consultant
KPMG Sweden

It is important to have training programs that are adapted to the different employees in addition to an overall program. As mentioned in the report, it is very important that this is followed up on a regular basis. Many of today's firms/companies only have some written rules around ethics and morality, (preferably together with the employment contract) without further follow-up.

Frode Løkken
Human- and labor rights consultant
Responsible supply chain
KPMG Norway

Training programs should not only measure the completion of training, but also the training effectiveness. Measurement and evaluation helps the organization towards a more risk-based ethics and compliance training program as it gives us the information we need to improve program design and to eliminate ineffective or unnecessary programs. New technology has significantly enhanced our ability to collect training data and measure success.

Fabian Bævre Larsen
Compliance advisory and transformation consultant
KPMG Norway

Control activities, monitoring, and testing

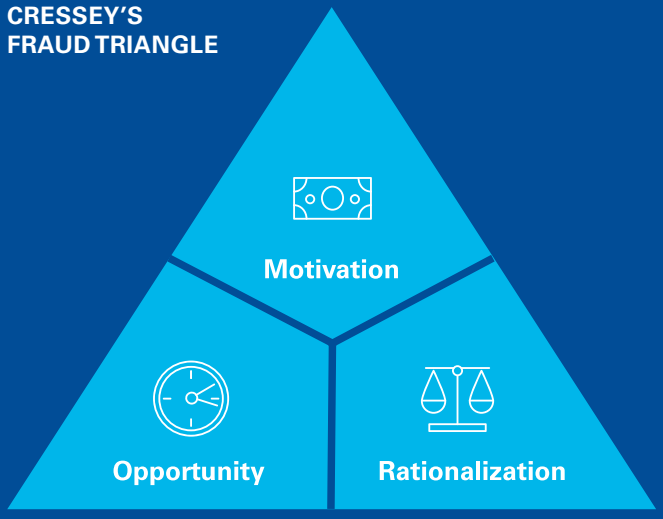
The Board of Directors is overall responsible for ensuring that the Company has implemented effective systems of monitoring activities, review procedures, and testing for effectiveness. All locations should be included in the organization's ongoing monitoring. It is the responsibility of the management to ensure that the company has effective controls in place to mitigate the ethics/ESG compliance risks, based upon the risk assessments in the organization. Good practice is that the company carries out risk-based controls (data analysis), accounting reports are reviewed for warning signs of fraud and unusual trends, and post transactional reviews are performed to check for fraud or red flags. The expectations for control and monitoring activities of ESG risks related to external third parties, in particular the supply chain, is increasing.

Results

60 % agree that the company has effective controls in place to mitigate compliance risks. There are only small differences between ownership and industry segments.

We note that 92% of the respondents who have rated their maturity as high (maturity levels 4 and 5) agree.

CRESSEY'S FRAUD TRIANGLE



Designing and implementing key controls and ensuring their operational effectiveness are vital to ensuring compliance risks are mitigated to an acceptable level. Mature organizations have either established manual plans for control activities, monitoring and testing or implemented real-time monitoring systems to obtain assurance that controls are working effectively. Implementation of such systems affects the motivation and opportunity aspect of the fraud triangle in a positive way reducing the probability of fraud or untoward incidents to take place.

Teejay Srai
Head of investigation and major projects team
KPMG Norway

Organizations can benefit greatly by defining control activities in relation to their main compliance risks and the front runners will aim to establish a comprehensive control repository providing a clear link between risks and controls.

Mikael Flod
Risk and Compliance consultant
KPMG Sweden

It is almost impossible to ensure compliance with all applicable laws and regulations by means of manual processes and detective controls. The most effective way to ensure compliance with sometimes complex and challenging regulatory requirements is to automate repetitive processes and to integrate appropriate preventive controls.

Andreas Halvarsson
Partner, Risk & Compliance Consulting
KPMG Sweden

Issue management, whistleblower mechanism, and investigation

Having a professional whistleblowing mechanism in place is an ethical backbone for responsible business. Investigations of reports of misconduct in the company require neutral and professional assessments of factual grounds. KPMG notes that several companies lack procedures for securing electronic evidence and review of employee email as well as procedures to manage media/ shareholders/other stakeholders in the event of irregularities. Equally important is insight and understanding of the human challenges all affected parties are exposed to. The EU Directive on whistleblower protection makes it safer to express concerns and offers management an efficient tool for compliance.

Investigations of any allegations or suspicions of misconduct by the organization, its employees, or agents should be conducted in a timely and thorough manner, with established procedures for documenting the organization's response, including disciplinary or remediation measures taken. The company should conduct a root cause analysis, including the extent, seriousness and pervasiveness of misconduct and give due consideration to why the controls failed, the vendor selection (if appropriate), prior indicators of control failures or allegations of misconduct, and management accountability and the remedial actions taken. Good practice is that the Company has a policy to ensure that the board is informed of severe irregularities.

Results

78 % agree that employees trust that all whistleblowing reports will be followed-up professionally. 3% of the respondents disagree, the remaining are neutral. There are only small differences between ownership and industry segments.

Worth noting, **92%** of the respondents who have rated their maturity as high (maturity levels 4 and 5) agree to the statement.

73 % agree that business partners are encouraged to report identified concerns or misconduct through our whistleblowing channel. There are only small differences between ownership and industry segments.

Interestingly, **100%** of the respondents who have rated their maturity as high (maturity levels 4 and 5) agree to the statement.

73 % agree that the company takes efficient learning from the results of internal controls and other compliance findings. There are only small differences between ownership and industry segments.

U.S. Department of Justice Criminal Division "Evaluation of Corporate Compliance Programs"

"Properly Scoped Investigation by Qualified Personnel – How has the company ensured that the investigations have been properly scoped, and were independent, objective, appropriately conducted, and properly documented?

Response to Investigations – Have the company's investigations been used to identify root causes, system vulnerabilities, and accountability lapses, including among supervisory managers and senior executives? What has been the process for responding to investigative findings? How high up in the company do investigative findings go?"

Every investigation of misconduct is also a learning opportunity, which enables you to safeguard your employees and bottom line.

Timo Piroinen
Head of Forensics
KPMG Finland

It is interesting to observe that this significant proportion of the respondents agree that business partners are encouraged to report through the whistleblower mechanism. This may indicate that the threshold for such «external whistleblowing» is lowered, which is good.

Tor Henning Rustan
Head of Legal Forensic and Partner
KPMG Norway

The results are more convincing than what I expected and might reflect an increased awareness on the importance of ethical business conduct. Has the implementation of the EU Directive contributed to increased awareness? Previous Norwegian research, however, indicates less trust among employees on the employer's ability to handle reported concerns professionally. Corporations must always acknowledge that maintaining such trust among its employees is a never-ending process.

Petter Amland
Head of Investigation Team
KPMG Norway

Reporting, consequences and learning

The company should convey that unethical conduct will not be tolerated, and the compliance program should have disciplinary procedures in place to address misconduct, as well as failures to take steps to prevent or detect misconduct. Disciplinary measures should be enforced consistently across the organization and be commensurate with the violations. The company must engage in meaningful efforts to review the compliance program and ensure it is up to date, and to promote improvement and sustainability. Reviews should include gap analyses to determine if particular areas of risk are not sufficiently addressed in the policies, controls, or training.

Results

73 % agree that the company takes efficient learning from the results of internal controls and other compliance findings. We note that 100% of the respondents who have rated their maturity as high (maturity levels 4 and 5) agree.

82 % agree that breaching the company Code of Conduct has appropriate consequences for involved employees.

61 % agree that Suppliers or other external parties who breach the company code of conduct are sanctioned appropriately. We note that 27% are "neutral or do not know" which may indicate that the respondents (in majority dedicated compliance and internal audit personnel) do not have a close interaction with line management/procurement on this topic.

U.S. Department of Justice Criminal Division "Evaluation of Corporate Compliance Programs"

"Prosecutors should assess whether the company has clear disciplinary procedures in place, enforces them consistently across the organization, and ensures that the procedures are commensurate with the violations. Prosecutors should also assess the extent to which the company's communications convey to its employees that unethical conduct will not be tolerated and will bring swift consequences, regardless of the position or title of the employee who engages in the conduct."

It may be rather optimistic that 73 % of the companies take efficient learning from results. Unfortunately, too often we find that the learning is restricted to a small group, and that companies struggle to implement their findings throughout all their departments.

Kristine Aasgård
Responsible supply chain consultant
Human- and labor rights expert
KPMG Norway

Technology and data analytics – the digital transformation journey

The amount of compliance-relevant data to analyze, as well as the increased expectations for traceability, openness, and transparency, lead to increased need for efficient digital tools. Digitalization of compliance controls offers the possibility of continuous monitoring of data sources. Digital tools also enable sharing of data across the organization while taking care of the safety aspects and protection of sensitive data. One of the success factors related to technology is to procure systems which can be integrated with the company's existing systems. For instance, if you want a third-party database assessing compliance risks, it should be integrated with the company's master data to ensure completeness of the third-party universe. If compliance ends up utilizing their own system, in silos from all other systems, there is a risk that it won't be properly implemented in the organization.

Results

34 % agree that the company has necessary and effective technology tools to mitigate ESG-related risks. Interestingly, only **25%** of the respondents who have rated their maturity as high (maturity levels 4 and 5) agree to the statement.

Companies continue struggling to leverage technology tools. Results from the Compliance Journey Survey 2021 showed that companies tend to struggle to effectively leverage on technology tools. 41 % of the respondents agreed that their compliance program sufficiently leveraged technology. In 2022, only 34 % of the respondents agree that they are leveraging necessary and effective technology tools to mitigate ESG-related risks.

U.S. Department of Justice Criminal Division "Evaluation of Corporate Compliance Programs"

"Do compliance and control personnel have sufficient direct or indirect access to relevant sources of data to allow for timely and effective monitoring and/or testing of policies, controls, and transactions? Do any impediments exist that limit access to relevant sources of data and, if so, what is the company doing to address the impediments?"

Industry leaders are starting to move away from traditional 'compliance only' solutions by implementing emerging technologies, allowing for a greater degree of flexibility aimed at integrating with business operations tailored to the business end user.

Esther Amalie Voktor Borgen
Head of Compliance Advisory and Transformation
KPMG Norway

Conclusion

Key drivers for the evolution

- Wave of regulations, including increased social-related requirements with the Norwegian transparency act coming into force. The EU is looking at implementing similar legislation
- Still increased expectations from external stakeholders, such as customers and banks
- Cyberthreats constantly evolving
- Geopolitical uncertainties in Europe following the war in Ukraine affecting commodity prices

Main challenges ahead

- Making the first line responsible and accountable for compliance; empowerment and accountability hand-in-hand
- Establish effective controls and conduct regular testing of effectiveness
- Follow up of third parties throughout the lifecycle, not only focusing on pre-engagement screening

PAST	TODAY	TOMORROW
» Unclear requirements » Unclear roles and responsibilites » Fragmented pieces of compliance activities » Main focus on anti-corruption and sanctions	» Requirements are better documented and understood » Compliance functions and programs in place » Focus extended to cover ESG, data protection and security » Compliance not yet an integrated part of daily operations (1st line) » Mainly manual processes in data analysis, documentation and reporting	» Compliance risks integrated into daily operational work » ESG focus with proactive responsible supply chain activities » Digitalization enables data-driven, efficient and agile data analysis » Whistleblowing creates an ethical backbone for responsible business

kpmg.no | kpmg.fi | kpmg.se | kpmg.dk