Considerations for the application of the Verklaring Omtrent Risicobeheersing (VOR)

KPMG Netherlands

November 2024

Introduction

In December 2023, the supporting parties[1], reached an agreement in the Van Manen Working Group on a proposal to amend the Dutch Corporate Governance Code (hereafter: the Code) by introducing the Verklaring Omtrent Risicobeheersing (VOR), or statement on risk management (unofficial translation).

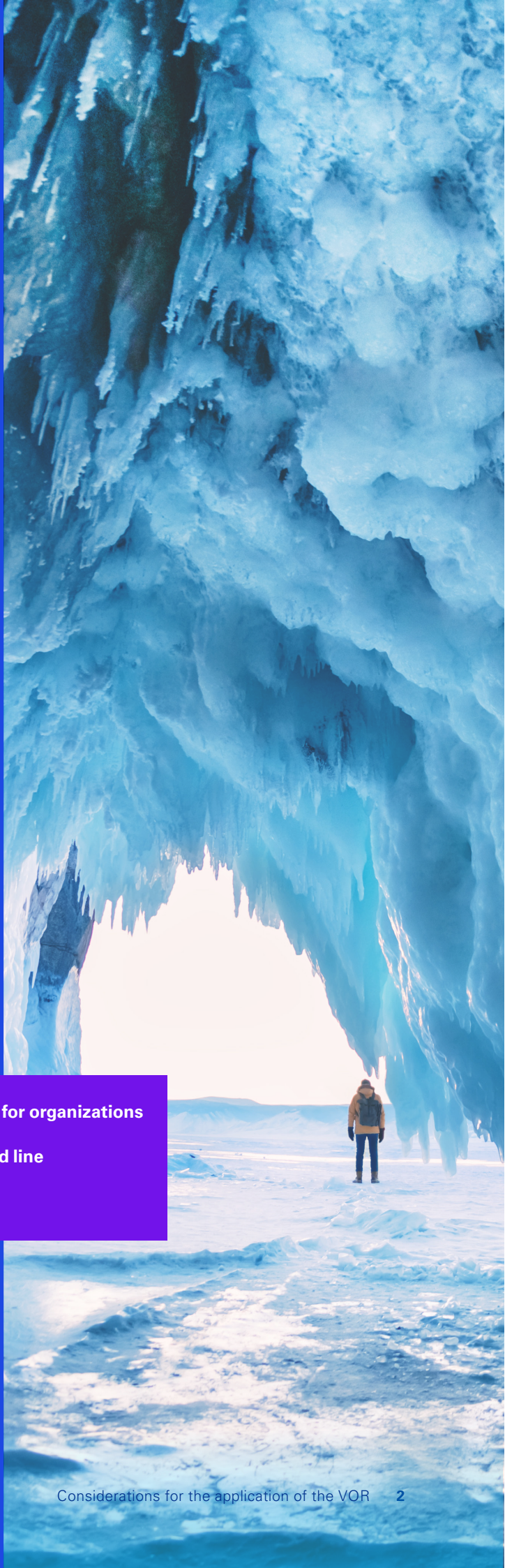
The proposed amendments aim to enhance the responsibilities of the management board, audit committee, and supervisory board in the area of risk management. Depending on the company's current risk management maturity additional steps need to be made in order to report on the VOR in the management board report. Directors and supervisory directors will be at the forefront of these efforts.

For some companies, the VOR will be a catalyst to reassess their risk management processes and internal controls, identifying whether adjustments are necessary to meet current standards. For others, it will drive further enhancements to risk management systems across various risk areas, ensuring that the company maintains in control. In certain cases, where strong controls are already in place, minimal adjustments may be needed.

However, the proposal is not prescriptive and lacks detailed guidelines, leading to uncertainty and an ongoing debate on how to apply the VOR effectively in practice. Regardless of the final outcome, these amendments offer an opportunity for directors to tailor their internal risk management and control systems to the specific needs of their companies.

This KPMG whitepaper outlines our considerations to apply the VOR. The paper is structured as follows:

1. **An overview of the proposed changes and key challenges for organizations**
2. **The roles and responsibilities of the first, second, and third line**
3. **Considerations to apply the VOR**



1 Eumedion, Euronext, the Dutch Trade Union Confederation (FNV), the National Federation of Christian Trade Unions in the Netherlands (CNV), the Netherlands Association of Stockholders (VEB), the Netherlands Association of Securities-Issuing Companies (VEUO) and the Confederation of Netherlands Industry and Employers (VNO-NCW) - and the NBA

1. An overview of the proposed changes

Introduction

The changes as proposed by the Working Group Van Manen to the Code, also referred to as the Verklaring Omtrent Risicobeheersing (VOR), emphasize the critical role of risk management in ensuring the company's long-term sustainable value creation. These changes will also strengthen the accountability chain for both financial and non-financial information.

The VOR highlights the responsibilities of the management board, audit committee, and supervisory board in overseeing risk management and reporting on these activities. As key figures in the governance structure, they are in the best position to ensure this happens effectively.

We expect that the introduction of the VOR will prompt management and supervisory directors to take more ownership over risk management and its external reporting. This will lead to a deeper engagement with the risk management processes and a more transparent communication on the effectiveness of risk management to stakeholders.

The proposed changes to the relevant the Code principles and best practice provisions are listed below, with key areas highlighted where applicable.

Best practice provision	
1.4.2	**In the management report, the management board should render account of:** I. the execution of the risk assessment, with a description of the principal risks facing the company in relation to its risk appetite, as referred to in best practice provision 1.2.1; II. the design and effectiveness of the internal risk management and control systems in the field of **operational, compliance and reporting risks** over last financial year and **which frameworks** were used; III. the assessment of the effectiveness of the internal risk management and control systems related to operational, compliance and reporting risks over the past financial year; IV. the sensitivity of the results of the company to material changes in external factors.

The main challenges related to the proposed changes

The management report must provide a clear overview of the company's risk assessment process, highlighting the key risks it faces in relation to its risk appetite, as outlined in best practice provision 1.2.1.
Best practice provision 1.4.2 aims to ensure that stakeholders fully understand the risks involved in the company's operations and strategic objectives. The two key changes that have been proposed under this principle, result in a few challenges.

Companies are required to explicitly define risks across three main areas: operations, compliance, and reporting. This reflects the assumption that the company's strategic risks filter down into these categories. As a result, companies are expected to adopt a more detailed and transparent approach to reporting, prompting them to thoroughly explore their risk profiles and disclose more comprehensive information. This additional requirement is intended

to boost stakeholder confidence by providing clearer and more detailed corporate disclosures.

In addition, management must select a specific framework for their internal risk management and control systems. The explanatory notes of the Code recommend the use of the COSO Internal Control Integrated Framework, which is widely regarded as a best practice due to its broad adoption and proven track record in the business world. For management, this means ensuring that the selected framework is implemented effectively, and that its principles are followed closely. It may require substantial effort to align current processes with the framework's requirements and to ensure comprehensive training and compliance across the company.

Best practice provision	
1.4.3	**The management board should state in the management report, with clear substantiation:** I. that the report provides sufficient insights into any failings in the effectiveness of the internal risk management and control systems with regard to the risks as referred to in best practice provision 1.2.1; II. that the aforementioned systems provide reasonable assurance that the financial reporting does not contain any material inaccuracies; III. **that these systems provide at least a limited assurance that the sustainability reporting does not contain any material inaccuracies;** IV. **what level of assurance these systems provide that the operational and compliance risks are managed effectively.**

The main challenges related to the proposed changes

Best practice provision 1.4.3 introduces two key changes. The first change requires internal risk management and control systems to provide limited assurance for sustainability reporting, while the second allows companies to determine the appropriate level of assurance for operational and compliance risks.

We expect that most companies will need to ivest in additional resources and efforts to ensure they can provide limited assurance over sustainability reporting; this will likely involve enhancing their existing sustainability reporting frameworks.

Furthermore, the changes allow companies to tailor assurance for operational and compliance risks to their specific contexts. Since these non-financial risks differ significantly from financial reporting risks, companies need to provide a clear and thorough explanation in their management report on how the level of assurance is defined and the company's approach to managing these risks in order to help stakeholders evaluate the effectiveness of the company's internal risk management and control system.

Additionally, defining material inaccuracies and major failings presents another challenge. The proposed changes lack detailed guidance on how management should define or report inaccuracies and failings. Therefore, it is essential for management to develop clear definitions and reporting frameworks to ensure transparent communication, to maintain stakeholder trust, and to comply with new reporting standards.

Overall, there is a strong need for clear communication with stakeholders regarding the interpretation of the VOR. Without clarity, stakeholders may misinterpret the scope or limitations of the internal risk management systems and, as a result, may not take well-informed decisions.

Best practice provision	
1.5.3	**The audit committee should report to the supervisory board on its deliberations and findings. This report must, at least, include the following information:** I. the methods used to assess the effectiveness of the design and operation of the internal risk management and control systems referred to in best practice provisions 1.2.1 to 1.2.3 inclusive; II. the methods used to assess the effectiveness of the internal and external audit processes; III. material considerations concerning financial and sustainability reporting; and the way in which the material risks and uncertainties, referred to in best practice provisions 1.4.2 and 1.4.3, have been analysed and discussed, along with a description of the most important findings of the audit committee **and the manner in which the statement as referred to in provision 1.4.3 is substantiated**.

The main challenges related to the proposed changes

This change increases the audit committee's responsibility for the audit committee to assess and report to the supervisory board on the substantiation of management's statements in best practice provision 1.4.3. This change aims to improve the depth and clarity of the audit committee's reporting, thereby strengthening overall corporate governance. The audit committee's report must include detailed information on several key areas.

First, it should outline the methods used to assess the effectiveness of the design and operation of the internal risk management and control systems, as referenced in best practice provisions 1.2.1 to 1.2.3. This includes a thorough evaluation of the structure and how well these systems function in practice. Additionally, the report must describe the methods used to assess the effectiveness of both internal and external audit processes, ensuring that issues are identified and resolved promptly through a rigorous assessment.

The report should also address considerations related to financial and sustainability reporting, including an analysis of material risks and uncertainties as outlined in best practice provisions 1.4.2 and 1.4.3. Furthermore, it must explain the most significant findings of the audit committee and describe how management's statement, as required by best practice provision 1.4.3, is substantiated.

One key challenge as a result from the proposed changes from best practice provision 1.5.3 to determine what additional information the audit committee needs and how to gather this information effectively. To address this,

the audit committee will need to develop a systematic approach to identify key areas of concern and collect comprehensive information, which may involve enhancing audit processes, seeking further input from internal and external auditors, and conducting a more detailed analysis of risk management and reporting practices.

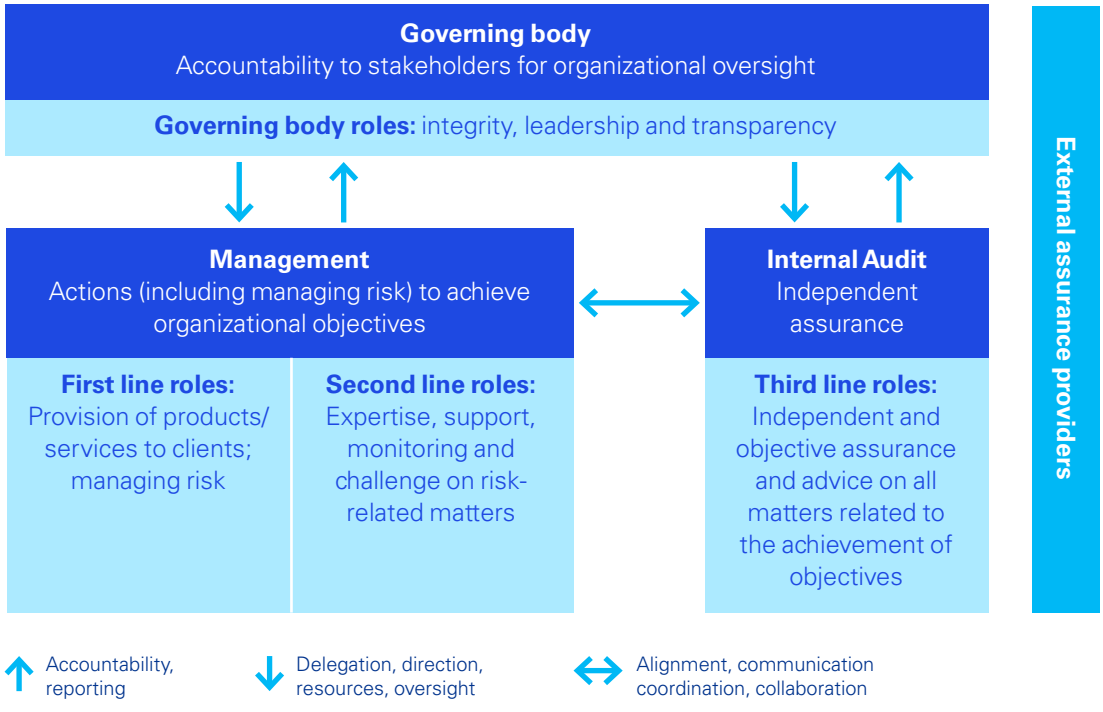
Additionally, the audit committee must ensure that its methods for evaluating the effectiveness of risk management and control systems are rigorous and well-documented. This will involve a thorough review of both the design and implementation of these systems, along with close collaboration with management, internal auditors and external auditors to fully understand the company's risk management practices.

2. The VOR in relation to the three lines model

In the previous chapter, we outlined the proposed changes to the Code and the key challenges that we foresee. These changes bring increased uncertainty and should be subject of further debate, requiring a more comprehensive and transparent approach to risk management and internal control. Companies will need to reassess and strengthen their risk management processes to ensure they can address all questions from the supervisory board and, more particularly, from the audit committee.

Clear roles and responsibilities across the three lines[2], supporting a cohesive approach towards risk management, becomes even more essential. Below, we outline the Three Lines Model and describe the roles and responsibilities of each line in relation to the VOR, along with the key activities they undertake.

Three lines Model



[2] https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-english.pdf

First line

The first line consists of operational management and employees responsible for delivering products and services to clients. This line has the primary responsibility for risk ownership and is directly involved in identifying, assessing and managing risks. The first line implements and maintains internal controls that are critical for mitigating risks, ensuring that day-to-day activities align with the organization's risk appetite and strategic objectives. In doing so, first-line management plays a vital role by providing performance data and insights that feed into the substantiation of the VOR.

Second line

The second line includes functions such as internal control, risk management, business control, legal and compliance, which support the first line by creating structured frameworks and processes for managing risk. They are responsible for setting policies and procedures ensuring the company's risk management strategy is comprehensive and aligned with regulatory requirements and industry best practices.

In addition to creating frameworks, the second line also oversees the evaluation of the effectiveness of processes and controls that relate to the VOR. They ensure that the company's risk management framework is regularly updated to respond to both internal and external challenges, remaining resilient in the face of evolving risks.

Third line

The third line, represented by the internal audit function (IAF), plays a crucial role by providing independent and objective assurance to management and the supervisory board on the overall effectiveness of the internal risk management and control systems. They evaluate the processes and controls established by the first and second lines to ensure these are aligned with the company's risk appetite and strategic objectives.

This could also include audits on the VOR itself, verifying that the management board statements are based on solid and reliable substantiation. The IAF does not only test the accuracy and completeness of risk management and internal control systems, but also ensures that these systems are adaptable to emerging risks and external challenges.

In this context the IAF should define an audit universe – a complete list of all areas within the organization that can be audited. The audit universe forms the basis for a risk-based audit plan, which prioritizes audits based on the company's most significant risks. By focusing on the areas that pose the greatest threats to the company's strategic objectives, the IAF can ensure that resources are allocated effectively.

Beyond its assurance role, the IAF can also serve as an advisor next to the second line. They can guide management in defining the company's risk appetite, ensuring it is integrated into both operational processes and strategic planning. They can support management by identifying risks that are most significant and should be disclosed in the management report. The IAF can provide training on internal risk management and control systems to ensure that these systems are aligned and understood throughout the organization.

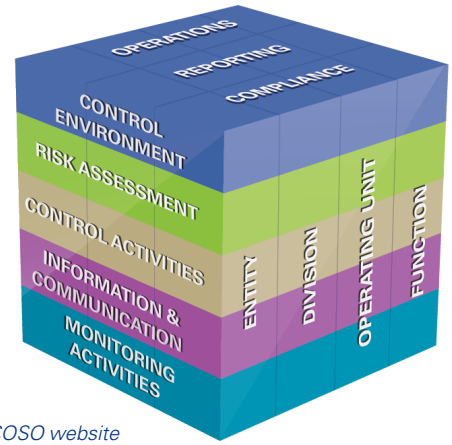
3. Considerations to operationalize the VOR

1. Considerations for the supporting framework

According to best practice provision 1.4.2, organizations are required to select a framework for their internal risk management and control system. This framework forms the foundation for a comprehensive and consistent approach to risk management across the organization. Research[3] shows that using such frameworks enhances an organization's ability to identify, assess, and mitigate risks, providing a solid structure for managing operational, financial, compliance, and strategic risks.

In practice we see that the COSO Internal Control Integrated Framework[4] (COSO IC) is the most widely used framework and, as such, the source of most experiences and best practices. Out of the 25 listed companies in the AEX (August 2024) already 19 make reference in their annual report to the COSO IC framework.

Typically, the COSO framework is already set up in such a way that it can be applied for the three VOR risk categories, including guidance on how to apply the COSO IC framework for ESG (COSO Internal Control over Sustainability Reporting[5]).



Source: COSO website

One of the key challenges when applying the COSO IC framework is ensuring and demonstrating that the 17 underlying principles are adequately addressed. To manage this, companies typically map these 17 principles to the relevant controls by using a mapping table. This table helps demonstrate how each principle is implemented within the organization's risk management and control systems. Below, an example of a mapping table is included, to illustrate how this process works.

#	Internal Control Action	CE				RA				CA				I&C			MA	
		P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16	P17
1	Management establishes integrity and ethical standards	X			X													
2	Regular risk assessments on emerging risks and threats			X														
3	Segretion of duties and authorization limits set					X												
4	Periodic reporting to the audit committee and stakeholders																	X
5	Continuous monitoring of key controls, with a feedback loop					X												

[3] Frigo, M. L., & Anderson, R. J. (2011). Strategic Risk Management: A Foundation for Improving Enterprise Risk Management and Governance. Journal of Corporate Accounting & Finance, 22(3), 81-88.
Beasley, M. S., Branson, B. C., & Hancock, B. V. (2009). COSO's 2013 Internal Control – Integrated Framework: Recommendations and Implications. Journal of Accountancy

[4] https://www.coso.org/guidance-on-ic

[5] https://www.coso.org/_files/ugd/719ba0_0b33989b84454d1682399ab5c71e49cb.pdf

2. Considerations for the level of assurance

The term 'assurance' appears frequently in the proposed amendments of the Code, particularly in best practice provision 1.4.3, which outlines the required levels of assurance per risk category:

- reasonable assurance for internal risk management and control systems related to financial reporting;
- limited assurance for internal risk management and control systems related to sustainability reporting;
- flexibility for compliance and operational risks, allowing management to define the appropriate level of assurance.

However, the proposed amendments do not include a sufficiently specific definition or guidance for the term 'assurance' in this context. It only clarifies what assurance is not, stating: *"The word 'assurance' in this context should not be interpreted as in external audit, nor does it imply that companies must follow a fixed framework."*

This ambiguity gives companies the flexibility to define assurance based on their unique situations. As a result, users of the VOR should be able to:

- assess the added value of the VOR and make informed decisions based on this information provided;
- compare companies based on the level of assurance they provide.

In practice, companies find it challenging to define assurance for their specific circumstances. Although the Code suggests not interpreting assurance in the same way as in external audits, applying similar concepts can help both management and users of the VOR establish a common understanding. Therefore, it is crucial to understand the difference between limited assurance and reasonable assurance, as used in external audits, to provide clarity to stakeholders:

- Reasonable assurance, in the context of the VOR, is comparable to an audit opinion on financial reporting. This opinion provides stakeholders with confidence that the company's financial statements are properly prepared, materially accurate, and reasonably stated. In the context of the VOR, reasonable assurance involves a comprehensive setup and evaluation of the company's internal culture, the testing of internal controls, and a thorough evaluation of risks. This leads to a well-substantiated conclusion, offering stakeholders a high level of confidence in the accuracy and completeness of the VOR.
- Limited assurance, while following similar procedures, is carried out with a reduced scope and intensity, leading to a lower level of confidence. This form of assurance demonstrates that the company has met the necessary preconditions, such as implementing adequate controls, processes, and frameworks. However, it provides less depth of validation, offering a more general level of confidence in the company's risk management and internal control systems.

While management may consider the extremes of 'no assurance' or 'full assurance', neither is generally practical. No assurance would not inspire confidence among stakeholders, and full assurance is nearly impossible in a dynamic risk environment.

Limited Assurance	
Negatively formulated conclusion	Ways to obtain comfort to make this statement are amongst others, among other things (but not limited):
Example of statement: ***"We have not noted anything to conclude that the subject matter does not conform in all material respects with the identified criteria."***	• Reviewing management documentation • Inquiry & observation • Analytical procedures • Limited number of site visits, coverage through data analysis with limited underlying evidence

Reasonable Assurance	
Positively formulated conclusion	Ways to obtain comfort to make this statement are, among other things (but not limited):
Example of statement: *"We conclude that the subject matter conforms in all material respects with the identified criteria."*	• Controls testing (if applicable) • Sampling procedures • Higher number of site visits, coverage through sample testing • Data analysis with detailed requests for underlying evidence

3. Considerations for risk appetite

Another critical element to consider is the company's risk appetite – the amount and type of risk the company is willing to take to achieve its strategic objectives. A lower risk appetite means the company is more sensitive to risks materializing, which can lead to a faster classification of an incident as a major failure.

The threshold for what constitutes as a major failure in these areas can vary significantly depending on the company's risk appetite and should be clearly defined. For example, a compliance breach may be classified as a major failure in an organization with a low-risk appetite, while in case of a company with a high risk appetite, the same breach might be viewed as acceptable.

Limited Assurance	Impact on the internal risk management and control system
Very high	• The company is very risk taking and accepts these risks to materialize with a very high likelihood and/or impact. • The number of controls and the cost of control to mitigate the risks are minimal. • There is limited monitoring by management.
High	• The company is risk taking and accepts these risks to materialize with a high likelihood and/or impact. • There are a limited number of controls in place, which are more detective in nature. • Management only monitors occasionally.
Medium	• The company accepts these risks to materialize with a medium likelihood and/or impact. • There are controls in place to manage these risks on both the preventive and detective side. • Management monitors these risks on a periodic basis.
Low	• The company accepts these risks to materialize with a very low likelihood and/or low impact. • There are adequate controls in place to both prevent and detect these risks. • Management regularly monitors these risks.
Very low	• The company has (almost) no appetite for these risks to materialize. • There are adequate controls in place to prevent the risk from occurring and detective controls are in place to be able to take action when necessary. • Management is continuously monitoring these risks.

Additionally, it's important to consider material inaccuracies when assessing risk appetite. Material inaccuracies refer to errors or omissions that could have a significant impact on the company's decision-making processes or undermine stakeholder trust. While there is substantial guidance on materiality in the area of financial reporting, the understanding of material inaccuracies in compliance and operational risks is more subjective and less well-documented and can vary – based on the industry, regulatory expectations, and the organization's risk appetite.

In financial reporting, frameworks like IFRS and GAAP define material inaccuracies as errors or omissions that could influence economic decisions, often using both quantitative thresholds and qualitative factors. In the context of compliance and operational risks, materiality is more subjective, focusing on regulatory breaches, significant operational disruptions, or reputational damage.

4. Considerations on the required efforts of the company

To provide confidence that management can make a VOR statement, they need to evaluate the assurance-related processes and activities in place. A tool that can assist management in this evaluation – though it should not be the only tool – is the so-called assurance map[6]. An assurance map offers a structured overview of how the three lines (including external service providers, when relevant) provide assurance over the company's key risks.

It visualizes which departments or functions are responsible for assurance-related activities for specific risks. This allows management to assess the overall coverage of assurance efforts across the company. Once the assurance map is defined, management, in collaboration with the supervisory board, can decide whether the existing assurance activities provide sufficient confidence to compose a formal VOR statement, or whether additional assurance efforts are required. In some cases, it may even be decided that fewer assurance efforts are also sufficient to substantiate the VOR.

An example of an assurance map is provided below to illustrate how this tool can be applied.

Risk	Risk appetite	1st line		2nd line			3nd line	4th line
		Management	Project	Risk & I/C	Compliance	Health & Safety	internal Audit	External Audit
Risk 1	High							
Risk 2	Very low							
Risk 3	Low							
Risk 4	Medium							
Risk X	X							

high level of assurance related activities

medium level of assurance related activities

no assurance related activities

The example of the assurance map above demonstrates how the level of engagement and oversight is tailored to each risk, ensuring that the organization's risk appetite aligns with its control environment and assurance activities. Each risk is treated individually, based on its associated risk appetite, with the involvement of management, compliance, internal audit, and external audit varying accordingly.

For example, Risk 1, with a high-risk appetite, involves a medium level of assurance activities from management (represented in orange), with additional collaboration with Risk / Internal Control (IC), Internal Audit and External Audit to manage the risk appropriately. In contrast, Risk 2, with a very low risk appetite, requires a much higher level of assurance activities (represented in green) across all lines, ensuring strong controls are in place.

The assurance map supports the principle of combined assurance[7], where various assurance activities are coordinated to provide a holistic view of risk management. The South African Corporate Governance Code (King IV) also emphasizes the importance of integrated assurance to align with the strategic objectives of a company, ensuring all significant risks are effectively managed and reported to the governing body. The assurance map plays a critical role here in meeting these governance requirements, facilitating better decision-making and accountability.

[5] The IIA Global – *The Three Lines Model: An Update of the Three Lines of Defense*
[6] See also South Africa's King IV Report on Corporate Governance.

By regularly updating and reviewing the assurance map, companies can respond to changes in the risk environment and business strategies, maintaining alignment with their risk appetite and governance frameworks. The map also serves as a communication tool, providing the board with a clear and concise overview of the company's risk management efforts. This enables the board to fulfil its oversight responsibilities effectively, ensuring the company remains resilient and well-governed. Risk management efforts, particularly assurance activities, are essential to mitigating and addressing risks at all levels of the company.

For each of the company's three lines in the assurance map, different assurance-related activities can be performed. Below is an overview of these activities (though not exhaustive).

1

The first line conducts activities to ensure that risks are identified and controlled at the operational level such as:

Control self-assessments: Managers and employees periodically assess the effectiveness of the controls in place within their own areas of responsibility. This self-review process helps identify gaps and areas for improvement.

Management reviews: Regular reviews by management of operational performance, compliance with policies, and risk exposure. This might include financial performance reviews, safety checks, or compliance with internal policies.

Incident reporting: Immediate reporting and investigation of any operational incidents (e.g., data breaches, safety incidents) to understand the underlying causes and prevent recurrence.

Letters of representation: Management provides formal attestations about the accuracy and completeness of information related to risk and control in their area of responsibility. This often serves as an internal control confirmation for higher management.

2

The second line performs activities to provide oversight and ensure adherence to internal and external regulations like:

Compliance monitoring: Regular monitoring and testing of compliance with regulatory standards, such as environmental laws, data protection laws, or industry-specific regulations. This could involve checking processes against legal requirements or performing mock inspections.

Risk assessments: Corporate, project, compliance and operational risk assessments are carried out by risk management to identify and evaluate the potential risks faced by the company. Control owners are appointed to assess and treat the risks accordingly.

Site visits: Risk officers conduct site visits to check on the physical implementation of controls, such as safety protocols or environmental compliance. For example, a health and safety officer may visit construction sites to ensure adherence to safety standards.

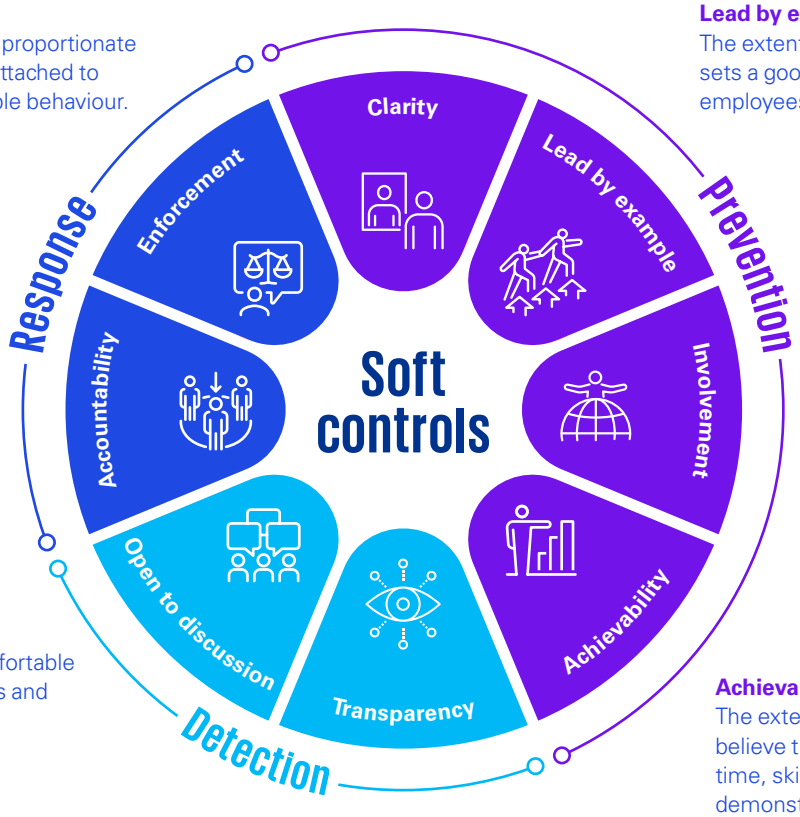
Data analytics: Leveraging data analytics to continuously monitor transactional data for anomalies or trends that indicate emerging risks or control failures. For example, monitoring financial transactions for signs of fraud or reviewing operational data for indications of potential risks.

Measuring quality of the soft controls: Assessing non-tangible factors, such as leadership behaviour, corporate culture, employee ethics, and communication effectiveness that influence risk management and control effectiveness (see figure below)

Clarity
The extent to which rules and procedures included in the policy are known to employees and they understand what is expected with regard to dealing with rules, procedures and guidelines.

Enforcement
The extent to which proportionate consequences are attached to desired or undesirable behaviour.

Lead by example
The extent to which management sets a good example to its employees.



Accountability
The extent to which employees feel comfortable addressing each other about undesirable behaviour.

Involvement
The extent to which there is motivation among employees to exhibit desired behaviour.

Open to discussion
The extent to which employees feel comfortable discussing dilemmas and doubts.

Achievability
The extent to which employees believe that they have sufficient time, skills and knowledge to demonstrate desired behaviour with regard to controlled business operations.

Transparency
The extent to which employee behaviour and its effects are visible to others.

3

The third line provides risk-based assurance to senior management and the board and conducts the following audits:

Internal Audits: Audits to review the audit object and to provide an independent opinion about the effectiveness of the controls or whether the object present a true and fair view of the company's performance.

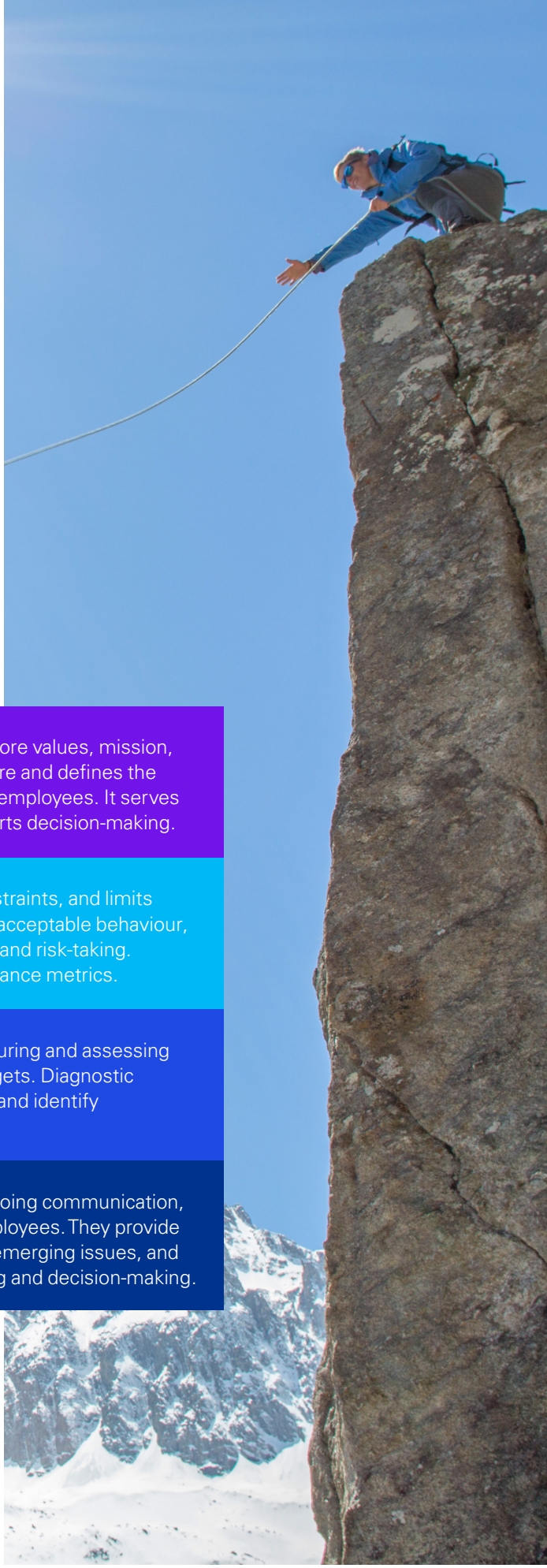
Follow-up audits: Re-assessing findings from previous audits to provide an independent opinion about the effectiveness of the remediation plans created during the initial audit.

The fourth line – external audit – provides an additional layer of assurance by conducting audits on both financial and non-financial reporting, performing regulatory compliance reviews, and issuing third-party certifications (such as SOC I Type 1 or Type 2). These activities collectively contribute to comprehensive oversight and strong controls throughout the company.

5. Considerations for internal controls

The foundation of the VOR lies in the company's internal risk management and control system, which is built on a framework of internal controls. Management should note, as outlined in the explanatory notes below, that the VOR should not be treated the same as the internal control statement required under US Sarbanes-Oxley legislation.

A theoretical concept that could be applied is the Levers of Control model introduced by R. Simons[8]. This framework focuses on the organizational systems and mechanisms that guide employee behaviour and manage risks. The model identifies four primary levers of control, each playing a distinct role in managing risks and organizational performance:



Belief systems: These encompass the company's core values, mission, and vision. This lever shapes the organizational culture and defines the fundamental principles and expected behaviours of employees. It serves as a foundation for shared understanding and supports decision-making.

Boundary systems: These establish the rules, constraints, and limits within the company. They define acceptable and unacceptable behaviour, setting the boundaries of authority, responsibilities, and risk-taking. Examples include policies, procedures, and performance metrics.

Diagnostic control systems: These focus on measuring and assessing performance against established objectives and targets. Diagnostic systems monitor key performance indicators (KPIs) and identify deviations that require corrective action.

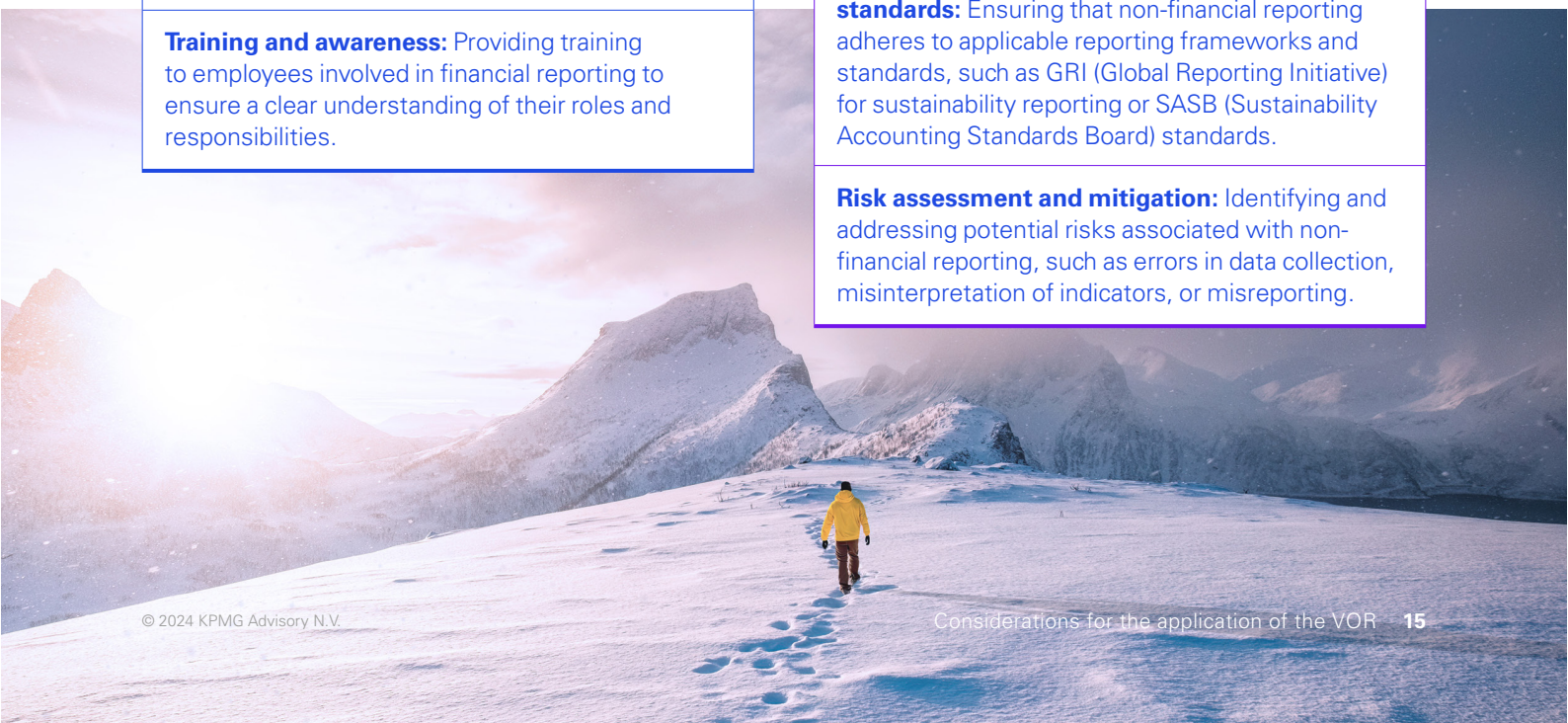
Interactive control systems: These encourage ongoing communication, dialogue, and feedback between managers and employees. They provide a platform for discussing uncertainties, addressing emerging issues, and fostering a collaborative approach to problem-solving and decision-making.

When considering the different risk categories that the VOR addresses, it is important to think about the types of controls that could be applied. Below is an overview of potential controls for each category (though not exhaustive). The level of detail in these controls should align with the level of assurance that management has defined – for example, reasonable assurance requires a more detailed set of controls compared to limited assurance.

[8] Simons, R. (1994). Levers of control: How managers use innovative control systems to drive strategic renewal. Harvard Business Press

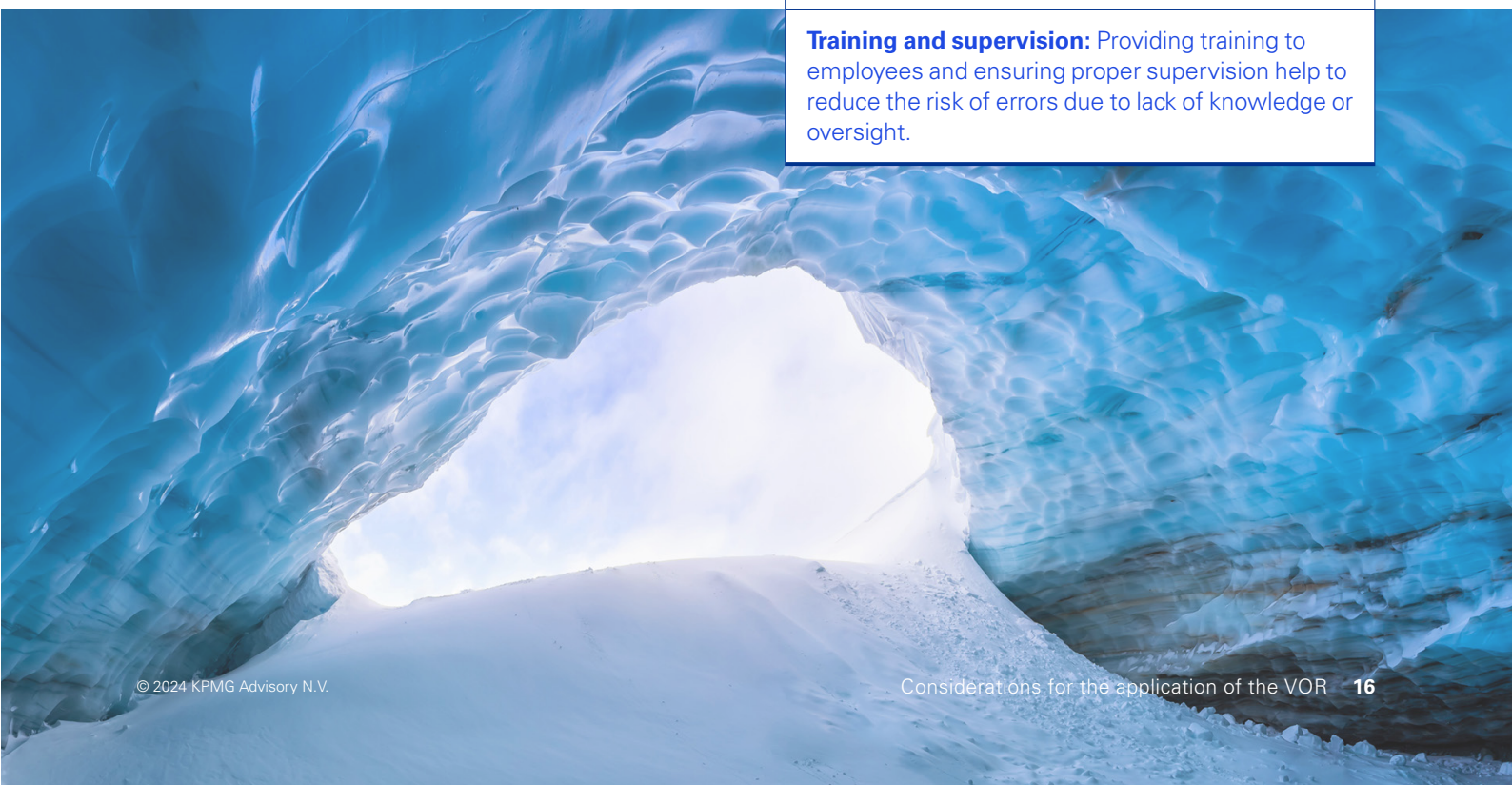
What type of internal controls are applicable for financial reporting risks?
Segregation of duties: Separating responsibilities for financial reporting processes, such as authorization, custody, and recording of transactions, to reduce the risk of errors and fraud.
Review and approval processes: Implementing a system of review and approval for financial transactions and reporting to ensure accuracy and completeness.
Periodic reconciliations: Regular reconciliations of key accounts, such as bank accounts, accounts receivable, and accounts payable, to detect and rectify any discrepancies.
Documentation and record-keeping: Maintaining complete and accurate documentation of all financial transactions and events to support the integrity of financial reports.
Internal and external audits: Conducting regular internal audits and engaging external auditors to independently review the accuracy and completeness of financial statements.
Compliance with accounting standards and regulations: Ensuring that financial reporting adheres to applicable accounting standards (e.g., GAAP, IFRS) and regulatory requirements (e.g., SEC regulations).
Management review and oversight: Active involvement of management in the financial reporting process, including review and approval of financial statements and reports.
Training and awareness: Providing training to employees involved in financial reporting to ensure a clear understanding of their roles and responsibilities.

What type of internal controls are applicable for non-financial reporting risks?
Data integrity controls: Implementing measures to ensure the accuracy, completeness, and reliability of non-financial data, such as operational metrics, sustainability indicators, and key performance indicators.
Documented procedures and policies: Establishing clear procedures and policies for collecting, validating, and reporting non-financial information to ensure consistency and accuracy.
Training and awareness programs: Providing training to employees responsible for non-financial reporting to ensure they understand the reporting requirements, data collection methods, and the importance of accuracy.
Quality assurance processes: Implementing review and validation processes to verify the accuracy and completeness of non-financial data before it is reported.
Management oversight and review: Involvement of management in the oversight and review of non-financial reporting activities to ensure the accuracy and reliability of the reported information.
Independent verification and assurance: Engaging external parties to provide independent verification and assurance of non-financial information, such as environmental impact assessments, social responsibility reports, and sustainability disclosures.
Compliance with reporting frameworks and standards: Ensuring that non-financial reporting adheres to applicable reporting frameworks and standards, such as GRI (Global Reporting Initiative) for sustainability reporting or SASB (Sustainability Accounting Standards Board) standards.
Risk assessment and mitigation: Identifying and addressing potential risks associated with non-financial reporting, such as errors in data collection, misinterpretation of indicators, or misreporting.



What type of internal controls are applicable for compliance risks?
Segregation of duties: This ensures that no single individual has the ability to initiate, approve, and complete a transaction or process, reducing the risk of fraud or error.
Regular monitoring and auditing: Regular reviews and audits of processes and transactions help to identify and address any non-compliance issues.
Written policies and procedures: Clearly documented policies and procedures help to ensure that employees understand what is expected of them in terms of compliance.
Management oversight: Oversight and review of compliance-related activities by management helps to ensure that the company remains in compliance with relevant laws and regulations.
Training and awareness programs: Training and awareness programs for employees help to ensure that they understand their compliance obligations and can identify and address potential compliance issues.
Reporting mechanisms: Establishing mechanisms for employees to report potential compliance issues or violations helps to ensure that non-compliance can be identified and addressed promptly.

What type of internal controls are applicable for operational risks?
Segregation of duties: Separating responsibilities within a process to prevent errors or fraud. For example, the individual who authorizes a transaction should be different from the individual who records the transaction.
Documentation and record keeping: Maintaining accurate and complete records of transactions, processes, and activities helps to ensure that operations are conducted in a controlled and consistent manner.
Physical controls: Implementing physical safeguards, such as locks, security measures, and limited access to assets, to protect against theft, damage, or unauthorized use.
Reconciliation and review: Regular reconciliation of accounts, inventory, and other records helps to identify discrepancies or errors in a timely manner.
Performance indicators and benchmarks: Establishing key performance indicators (KPIs) and benchmarks helps to monitor and evaluate operational performance, allowing for early identification of potential issues.
Contingency planning: Developing plans for potential operational disruptions, such as natural disasters or system failures, helps to minimize the impact on operations.
Training and supervision: Providing training to employees and ensuring proper supervision help to reduce the risk of errors due to lack of knowledge or oversight.



4. Considerations with other regulations

In addition, it is crucial to consider how the VOR aligns with existing EU regulations, such as the Prospectus Regulation and other legal frameworks. While the VOR aims to enhance transparency and improve risk management disclosures, companies must ensure these new requirements do not conflict with their broader obligations under EU law.

For instance, the Prospectus Regulation establishes specific rules for disclosures when offering securities to the public in the EU, including requirements related to risk factors. There is a potential risk that the VOR's disclosure obligations, especially those concerning risk management and control systems, could overlap or contradict these rules. This could result in increased regulatory complexity, particularly for companies operating both in the Dutch market and across Europe.

To minimize such risks, companies should implement the VOR with a clear understanding of how it fits within the broader framework of EU regulations. This requires a comprehensive review of how the VOR's reporting obligations interact with EU directives such as the Corporate Sustainability Reporting Directive (CSRD) and the European Sustainability Reporting Standards (ESRS), which address both financial and non-financial risks, including environmental and social factors.

Aligning the VOR with these EU regulations is essential for not only avoiding legal conflicts, but also ensuring consistency in corporate governance practices across borders. Companies should strive to implement the VOR in a way that complements their existing compliance frameworks, improving transparency both nationally and at the European level. This alignment will help ensure the VOR strengthens the company's risk management and reporting processes, rather than adding unnecessary complexity.

Supervisory boards and audit committees have a key role in overseeing this alignment, ensuring that the VOR complies with the Code and remains fully in line with applicable EU regulations according to the comply or explain principle. Taking a proactive approach will help avoid conflicts, enhance legal certainty, and further the company's commitment to transparency and stakeholder trust.

Contact

Jeroen Bolt
Bolt.Jeroen@kpmg.nl
+31 6 513 673 05

Bart van Loon
VanLoon.Bart@kpmg.nl
+31 6 532 493 28

Huck Chuah
Chuah.Huck@kpmg.nl
+31 6 4636 60 13

Peter Paul Brouwers
Brouwers.PeterPaul@kpmg.nl
+31 6 532 597 60

Reda Mizab
Mizab.Reda@kpmg.nl
+31 6 517 837 77

Alex Graafmans
Graafmans.Alex@kpmg.nl
+31 6 394 895 53

KPMG.nl