Verklaring Omtrent Risicobeheersing (VOR) – Opportunities for continuous improvement on good governance and risk management

November 2025

Introduction

In March 2025 the Dutch Corporate Governance Code (the Code) has been amended with the Verklaring Omtrent risicobeheersing (VOR) or in other words a “statement on risk management”. The main objective of the VOR lies not in the statement itself, but in the journey of reflection, dialogue, and transparency on risk management that precedes it.

As Rob van Wingerden[1] (Chair of the Monitoring Committee) emphasizes, the Code is intended as a source of inspiration for good governance and risk management, with open conversations about internal control and risk management at its core. Both the management board and audit committee are expected to take a leading role in this process and as a result have placed a renewed emphasis on the responsibilities of both the management board and the audit committee – in the area of risk management.

At the same time challenges arise due to the fact that the Code is principle-based and not overly prescriptive and therefore it leaves room for interpretation in several key areas:

- The Code applies the term “reasonable assurance” for financial reporting and “limited assurance” for sustainability reporting. For operational and compliance risks, the term “certainty” is applicable.
- Certainty and effectiveness: companies are free to define these terms within their own context. The Van Manen Working Group clarified that “certainty” does not equate to “assurance” as used in accountancy, nor does “effectiveness” refer to U.S. legislation such as the Sarbanes-Oxley Act (SOX).
- Operational and compliance risks: these are not explicitly defined in the Code, allowing companies to interpret them as appropriate.

This flexibility is beneficial, enabling organizations to tailor their internal risk management and control systems (IR&CS) to their unique context. This calls for an open dialogue within the organization, involving multiple disciplines and management layers. The process creates opportunities for continuous improvement and fosters a culture where risk awareness and transparency are paramount. This is exactly what the Monitoring Committee intended.

Building on our first publication[2] , this publication provides guidance and insights to support organizations, drawing on market experience, discussions with board members, and recent publications[3]. The aim is to help organizations achieve a VOR that not only meets the letter of the Code, but also its spirit: transparency, reflection, and ongoing improvement. It is structured around:

- Key insights gained in the market for the Code’s VOR-related provisions.
- The roles and responsibilities of stakeholders for risk management and the VOR, including the implications.
- Key questions that management may ask themselves in relation to risk management and the VOR.

[1] Managtementscope.nl (2025) Rob van Wingerden: ‘The code as source of inspiration again’
[2] KPMG (2024), ‘Considerations for the application of Verklaring Omtrent Risicobeheersing (VOR)’.
[3] NBA (2025), Brochure VOR-inspiratie-en-handvatten-voor-aib-en-ia.pdf, NBA (2025), Consultatie handreiking 1109

Key Insights

Many organizations have evaluated what the impact is of the changes to best practice provisions 1.4.2 and 1.4.3 and 1.5.3 for the IR&CS in their organization. As a result, valuable insights are emerging from these evaluations, and they may help other companies understand how to use the flexibility that the Code allows. These insights can guide others.

Provision 1.4.2 – Reporting on risk management

This provision requires companies to understand and articulate the risks associated with their strategy and their activities. It also mandates the application of one or more frameworks for IR&CS.

Our insights include:

- **Explicit risk appetite:** linking risk appetite to strategic objectives helps boards to assess whether risks are managed within acceptable boundaries.
- **Interconnected risks:** operational and compliance risks often overlap with strategic execution and should be assessed in the context of the business model and external environment.
- **Framework flexibility:** companies benefit from customizing their IR&CS based on maturity, sector-specific challenges, and governance culture.
- **Culture as a foundation:** a strong risk culture – reflected in leadership behavior, shared values, and employee engagement – enhances risk identification and mitigation.
- **Transparency:** stakeholders expect more clarity on risk identification, mitigation, monitoring, and escalation.
- **Governance:** The risk and control function takes responsibility for monitoring the effectiveness of IR&CS elements that are substantiating the VOR. Additionally, this function defines the guiding principles to ensure a consistent IR&CS structure across the organization.

Provision 1.4.3 – Statement by the management board

This provision introduces the requirement for IR&CS to provide an appropriate level of certainty that operational and compliance risks are effectively managed.

Our insights include:

- **Definition:** the Code does not define certainty. It merely states that “certainty” does not equate to “assurance” as it is used in accountancy, so organizations themselves need to define certainty. It may be helpful to stay close to how assurance is defined, as this enables a common language between different stakeholders.
- **Certainty levels need to be explained:** boards should define the level of certainty, explain the definitions chosen and acknowledge inherent limitations.
- **Internal substantiation:** effective certainty can be reached in many ways, e.g. by mapping risks to controls, documenting control effectiveness, and/or involving internal audit or second-line functions.
- **Materiality and scope:** The management board is in the lead of a structured process of identifying key risks and controls associated with the strategy and the organization’s activities, regularly reviewing their impact, and ensuring alignment with risk appetite. The management board sets criteria, determines certainty, timeframes, and transparently communicates decisions to stakeholders.

Provision 1.5.3 – Audit committee report

This provision increases the audit committee’s responsibility to assess and report to the supervisory board on the substantiation of management board’s statements in provision 1.4.3.

Our insights include:

- **Strengthened dialogue:** the audit committee acts as a bridge between the management board and the supervisory board, encouraging a critical discussion of risk management and substantiation of the VOR.
- **Focus on continuous improvement:** the audit committee has now been enabled to identify opportunities in further professionalizing or integrating risk management.

The roles and responsibilities of stakeholders for the VOR, including the implications

With a leading role for the management board, the amendments to the Code serve as a catalyst for organizations to be open and to reassess the IR&CS, identifying whether adjustments and enhancements are necessary and result in improved good governance and strong risk management as intended by the Code, ensuring that the organization remains in control.

They also strengthen the definition and communication of the risk management function's roles and responsibilities within the organization. Particularly establishing a strong central oversight and reporting role for the IR&CS supporting the VOR is essential, given that risk management activities are often fragmented across departments. Additionally, the involvement of other stakeholders should be reviewed to ensure clarity and alignment. The table below outlines the roles and responsibilities of key stakeholders in relation to the VOR, along with the implications of their involvement.

Stakeholder	Responsibilities	Implications
Management board	• Draft the management report in accordance with Article 2:391 BW. • Ensure completeness, accuracy, and timeliness of governance-related disclosures. • Provide a substantiated explanation for any deviations from the Dutch Corporate Governance Code. • Issue the VOR – a statement on internal risk management and control systems. • Engage in dialogue with shareholders regarding governance practices and the VOR. • Creating and maintaining a sound risk culture.	• The management board determines the level of assurance or certainty that IR&CS provide for effectively managing financial, non-financial, operational and compliance risks, considering the organization's risk appetite and choices made in the system's design. • The board is free to define the concepts of 'certainty' and 'effectiveness', and to substantiate the VOR statement according to its own criteria.
Audit Committee	• Prepare decisions for the supervisory board regarding financial and sustainability reporting, including the effectiveness of risk management and internal control systems. • Review and discuss the VOR and its substantiation with the management board. • Report findings and deliberations to the full Supervisory Board.	• Oversight responsibilities expanded to IR&CS. • Requires technical expertise in risk and control frameworks. • Plays a key role in validating the VOR.

Risk Management & Internal Control	• Support the management board in:
	  • Identifying, evaluating, and managing risks.
	  • Setting up IR&CS.
	  • Actively driving the development and strengthening of the risk culture and associated behaviors throughout the organization.
		• Coordinator of the VOR and supporting processes.
		• Broader scope of oversight on operational and compliance risks.
		• Measure risk culture and behavior.

Internal Audit Function	• Assess the design and effectiveness of internal control systems. • May support the VOR process upon request from the board or Supervisory Board.	• Critical role in validating the IR&CS .

External Auditor	• Perform three key tests on the VOR:
	  - Whether it contains all the mandatory elements
	  - Whether it is consistent with the financial statements
	  - Whether in the light of the knowledge and understanding of the organization and its environment obtained during the audit (or limited assurance engagement on CSRD), it contains material misstatements
	• Communicate findings via:
	  - Management letter.
	  - Board report
	  - Auditor's report.
	  - General Meeting of Shareholders presentation.
		• Ensuring timely insight into the type of statement the management intends to issue. It is advisable that both the external auditor and management consult in advance on the wording of the proposed VOR.

Key questions when applying the VOR

Although all stakeholders have their own role in relation to the IR&CS and the VOR, the primary body responsible is the management board and the different management layers who act as the risk owners. In practice, we see many questions arising on how to properly address one's responsibilities regarding the VOR and how to provide accountability in the management board report and supervisory board report. Without being exhaustive, the following questions can support the organization in the process towards improved risk management and a substantiated VOR.

General

- Which guiding principles are defined in shaping the VOR, given its principle-based framework?
- Which framework(s) is (are) applied to design the effectiveness of the IR&CS for operational, compliance, and reporting risks? And are any guidelines applied for the design of the control (e.g., NIS2, or ISO standards)?
- How are the varying levels of assurance and certainty defined?
- How are material shortcomings in the IR&CS systems defined and assessed?
- To what extent does the organization evaluate whether staffing in first-, second-, and third-line control roles is adequate?
- What sort of internal reporting is available to the organization and the audit committee on risk management and the VOR?
- How does the audit committee verify that all material shortcomings, significant changes, and improvements have been identified and disclosed in the management report, including findings from internal and external auditors?

Risks

- Which Enterprise Risk Management framework (e.g., COSO ERM, ISO 31000) does the organization apply, and how is ensured that all principles of such a framework are applied?
- How is the link established between risks or risk profiles, risk appetites, and the VOR disclosure? (For example, a low-risk appetite may imply higher expectations regarding assurance or certainty over IR&CS)
- Which findings have been reported by the Internal Audit Function and by other functions that should be considered?
- Which topics are discussed and recorded in submissions, minutes of the management board, supervisory board, and relevant committees (e.g., risk or compliance committees)?
- What discussions have taken place regarding strategy, operations, compliance, performance, incidents, and reporting?
- Does the organization have sufficient oversight of operational and compliance risks within business operations, compared to financial and nonfinancial reporting risks?
- Which issues have been weighed considering correspondence with regulators?
- How do audit findings (internal and external) relating to financial and nonfinancial reporting align with the VOR disclosures? How are issues such as fraud, noncompliance, corrected and uncorrected findings, or internal control deficiencies incorporated into the reporting?

Assessing the design and effectiveness of the IR&CS

- Does the organization have an IR&CS for all areas to be covered by the VOR or is it in certain areas solely relying on the expertise of the external assurance providers (this shouldn't be the external auditor)?
- Is there an IR&CS for regulatory compliance ensuring that the most important requirements resulting from rules and regulations are translated into key risks and controls?
- Have the findings of internal and external auditors been considered to evaluate and enhance the IR&CS?
- Is the design of the IR&CS aligned with the defined risk appetite and assurance and certainty levels?
- What process is established to determine the design and effectiveness of the IR&CS, and how is this substantiated?
- What level of assurance is provided by Internal Audit?
- What is the approach to identify significant changes and improvements in the IR&CS systems?
- Is the IR&CS assessed continuously throughout the year, or only at year-end? Is this consistent with a "point-in-time" or "period-of-time" declaration?
- What level of substantiation is considered sufficient by the organization and the audit committee to assess the design and effectiveness of the IR&CS and substantiating the VOR?

Fraud

- Are the outcomes of the organization's fraud risk assessment consistent with the VOR?
- Is the organization's fraud risk assessment aligned with that of the external auditor, or are there material differences?
- Have control deficiencies regarding fraud been identified, and are findings from suspected fraud or related internal investigations incorporated?
- Is the management report consistent with the auditor's report concerning the effectiveness of fraud risk management?

Culture and behavior

- Are observations regarding culture and behavior consistent with the VOR?
- Is the board's disclosure (as required by best practice provision 2.5.4) consistent and aligned with the VOR? Check if it explains the following:
  - the organization's culture and any desired changes;
  - how culture, underlying values, and promoted behaviors contribute to sustainable long-term value creation; and what initiatives are taken to enhance this contribution;
  - the functioning and enforcement of the code of conduct.
- Are there observations on the implementation and enforcement of the code of conduct, and are they consistent with the VOR?
- Are deficiencies in internal controls that stem from culture and behavior adequately reflected in the VOR?

Deficiencies

- What thresholds (qualitative/quantitative) are applied to deficiencies? Are these consistent with Enterprise Risk Assessment criteria (or aligned with the SOx 404 definition of "Material Weakness")?
- Have all potential material shortcomings been discussed with the supervisory board and/or the audit committee?
- What considerations have led to not reporting certain material deficiencies that were discussed?
- Is there a rationale for not reporting on certain matters or material deficiencies (e.g., from a competitive standpoint)?
- Have all (material) findings of internal and external auditors been considered?

Monitoring by the audit committee and reporting to the supervisory board

- How does the audit committee monitor the VOR throughout the year?
- What role does the Internal Audit Function play in relation to the VOR?
- How does the audit committee assess the substantiation provided by management?
- How does management analyze deficiencies in the design and functioning of internal controls? And how does the audit committee evaluate these deficiencies?
- How does the audit committee report on the VOR to the supervisory board?

VOR and ESG

- For which sustainability disclosures is there material uncertainty regarding the interpretation of regulation?
- For what information are there significant concerns regarding the completeness and reliability of the IR&CS and underlying processes?
- How are such uncertainties and doubts disclosed in the management report?
- Are there operational or compliance risks that are partially described in the ESG section and partially elsewhere? How does reporting address overlapping or separated ESG and non-ESG risks, and is it possible for readers to obtain a complete picture?

Period-in-time vs. Point-in-time VOR

- Is a "period of-time" statement' (the statement that is envisaged by the Monitoring Committee) substantiated by evaluations conducted throughout the year?
- Is a "point-in-time" statement substantiated by an evaluation sufficiently close to year-end?
- How are deficiencies addressed that were identified later than their reporting period?

Enterprise risk assessment, double materiality, and the VOR

- Are all risks from the Enterprise Risk Assessment reflected in the management board report, and are their ratings consistent with the internal ERM profile?
- Are risks from the Enterprise Risk Assessment substantiated by the IR&CS?
- Is risk appetite defined for each identified risk, and is this consistent with the management board report?
- Is there consistency between the Double Materiality Assessment and the Enterprise Risk Assessment?

Conclusion

The amended Code - that includes the principles of the VOR - offers a great opportunity to start a journey of reflection, dialogue, and transparency to evaluate and enhance the way risk management is being performed by the organization.

While the Code allows for contextual interpretation, it demands a structured and substantiated approach to risk management. Organizations must ensure that their IR&CS are not only well-designed but also effectively monitored and reported.

Management plays a central role in shaping risk management and substantiating the VOR, supported by oversight from the audit committee. By addressing the questions and considerations outlined in this publication, organizations can enhance their readiness, foster a strong risk culture, and meet stakeholder expectations for accountability, assurance and certainty.

Contact

Huck Chuah
Partner
Chuah.Huck@kpmg.nl

Bart van Loon
Partner
VanLoon.Bart@kpmg.nl

Jeroen Bolt
Director
Bolt.Jeroen@kpmg.nl

Corine Tol
Associate Director
Tol.Corine@kpmg.nl

Home.kpmg

home.kpmg/socialmedia