VEUO

Vereniging Effecten Uitgevende Ondernemingen

Memorandum

**Briefing Note: New Risk Management Statement (VOR)**

## 1 Introduction and executive summary

This briefing note outlines the new Risk Management Statement (*Verklaring Omtrent Risicobeheersing*, **VOR**) for Dutch listed companies, as provided for by the revised 2025 Dutch Corporate Governance Code.

For the financial year 2025 and onwards, the VOR introduces certain new risk declarations by the management board of a Dutch listed company on operational and compliance risks and on the company's sustainability reporting and the internal control systems and the effectiveness thereof.

The VOR has been included in the Dutch Code following a strong call for a broader *in control statement* by, among others, the professional body for auditors the NBA, shareholder representative organisations such as Eumedion and the VEB, and the Dutch House of Representatives. This included a call for a "declaration of effectiveness" on the risk management systems, where organisations as VEUO and VNO-NCW have pointed out that it is not possible to provide such a declaration due to inherent limitations in risk management systems. The new requirements are the result of an eventual compromise between the so-called constitutive parties to the Code and the NBA.

Dutch listed companies already disclose various risk management aspects in their annual reports, such as the key risks the company faces, their risk appetite, how their internal controls are designed, etc. Companies must evaluate how these disclosures align with the 2025 Code requirements. The addition of a statement on the certainty provided by the internal controls on the effective management of operational and compliance risks is expected to be the most significant change.

When we refer to the VOR, we are referring to the newly added elements in the 2025 Code (see Annex 2 for a comparison).

*This briefing note is provided for informational purposes only and does not constitute legal advice. It reflects the current state of play regarding the VOR and may be subject to change. For specific legal guidance, please consult your legal advisor. It might also be advisable to discuss the VOR with your external auditor.*

## 2 Background and context

At the conclusion of the 2022 review of the Dutch Corporate Governance Code (**Code**), some parties, including shareholder interest groups such as Eumedion and VEB, and the Dutch professional organisation for auditors the NBA, called for the inclusion of a broader so-called "in control statement" in the Code. Given the need for further evaluation and discussion with other constitutive parties to the Code, the Monitoring Committee decided to defer the matter to a subsequent committee.

Further, in 2023, the Dutch House of Representatives passed a motion urging the Minister of Finance to advocate for a Statement on Risk Management (VOR) in the Code, with potential legislative action if unsuccessful.

In response, the constitutive parties to the Code (including VEUO) established a working group, chaired by Jaap van Manen (Chair of the Monitoring Committee from 2013 tot 2018), to explore the feasibility of a VOR. As part of this process, various, and sometimes quite far-reaching, proposals were put forward, including a proposal for a statement by the management board that, to the best of its knowledge, the risk management and control systems were adequately designed and operated effectively during the reporting year, and as such these systems provided reasonable assurance that (i) the management board was continuously aware of the extent to which the organisation achieved its operational and strategic goals during the reporting year, (ii) the external reporting over the reporting year is reliable and (iii) the organisation acted in accordance with relevant laws and regulations during the reporting year.

Reference was also made to a comparable discussion in the United Kingdom, where the 2024 revision of the Corporate Governance Code requires a "declaration of effectiveness" of the material controls by the management board. Such a declaration of effectiveness could be interpreted as a "guarantee" on risk management and would therefore have resulted in a far-reaching VOR statement.

Organizations such as VEUO and VNO-NCW expressed concerns that issuing such a statement would be unfeasible. It is not possible to state that risks were managed effectively, due to inherent limitations to risk management systems, cost limitations and the fact that certain causes of risks sit outside the company's sphere of influence, for instance because they are caused or dependent on third parties or circumstances beyond the company's control.

Eventually in December 2023 the working group reached a compromise on the VOR and its scope. In March 2024, the Minister of Finance endorsed the Van Manen working group's proposal for the VOR, leaving the inclusion of the VOR in the Code up to the new Monitoring Committee.

The new Monitoring Committee, that was installed early 2025, decided in March 2025 to include the proposal for the VOR in the Code. Given the broad support for the VOR, this was done without public consultation. Subject to certain technical legislative steps, Dutch listed companies will need to issue a VOR in their 2025 annual report.

## 3 The requirements of the VOR

### 3.1 What was already required by the Code?

Before 2025, the Code already required annual reports to include certain risk management statements, including whether the management report provides sufficient insight into failings in the effectiveness of internal risk management and control systems. The Code also required disclosures on risks to which the company is exposed, the design and operation of systems to mitigate those risks, and major failings in those systems observed during the reporting year. See annex 1 for these requirements.

While there is no specific statement required in the VOR on the management of strategic risks, strategic risks remain part of the scope of the Code (see for instance bpp 1.2.1).

### 3.2 What is new?

The 2025 Code maintains all statements and disclosures from the 2022 Code and adds the following.

- A description of how the management board has assessed the effectiveness of the internal risk management and control systems in relation to operational, compliance and reporting risks during the past financial year (see paragraph 3.3.1).
- A description of the frameworks that have been used in the design and operation of the internal risk management and control systems (see paragraph 3.3.2).
- A statement that these systems provide at least limited assurance that the sustainability reporting does not contain material inaccuracies (see paragraph 3.3.3).
- A statement on the level of certainty these systems provide that operational and compliance risks are effectively managed (see paragraph 3.3.4).
- An explanation in the audit committee's report to the supervisory board of how the VOR is substantiated (see paragraph 3.3.5).

See annex 2 for a comparison between disclosure requirements from the 2022 Code and the 2025 Code.

### 3.3 Complying with the VOR

A fundamental premise of the VOR is that it should be company-specific where possible. Both in the wording of the best practice provisions relating to the VOR and in the explanatory notes thereto this is emphasized. Companies can tailor their statements and descriptions to their own situation; there is no single prescribed way of complying with the VOR. We note that the best practice provisions and the explanatory notes should always be read in conjunction.

In paragraphs 3.3.1 to 3.3.5, below, we discuss the new requirements of the VOR. The descriptions and explanations provided in these paragraphs should also be read as examples that companies can tailor to their own situation.

### 3.3.1 Assessment of the effectiveness of the risk management systems

The first element of the VOR is *a description of how the management board has assessed the effectiveness of the internal risk management and control systems in relation to operational, compliance and reporting risks during the past financial year (bpp 1.4.2 (ii)).*

To be clear, this description does not have to be a separate section of the management report or even a separate section of the risk management paragraph. It is simply required that the annual report include a description of how the effectiveness of the internal risk management and control systems is assessed.

Such a description may include:

- Whether there is an internal audit function and, if so, how it is embedded in the organization
- Who within the company is responsible for assessing the effectiveness of the internal risk management and control systems
- How the effectiveness of these systems is monitored (e.g. (depending on the specific controls) is this real-time or retrospective; what is the frequency of retrospective monitoring, etc.)
- How the management board is informed of the results of this monitoring process
- How the management board discusses these findings internally
- How this assessment of effectiveness relates to the company's risk appetite
- How these findings are discussed with the supervisory board and/or the audit committee
- Whether these findings are discussed with the external auditor

The description should be tailored to include only those factors that are most pertinent to the company.

### 3.3.2 Description of frameworks used

The second element of the VOR, as laid down in bpp 1.4.2 (ii), is *a description of the frameworks used in the design and operation of the internal risk management and control systems.* The VOR does not prescribe a specific framework, nor does it prescribe to what extent any framework should be applied, such as which risk categories it should cover. Furthermore, other statements (for instance, on the level of certainty on the effective management of operational and compliance risks) do not have to be made with reference to this framework.

The overall framework for the design and operation of the company's internal risk management and control systems (e.g. COSO ERM) can be described, as can more specific frameworks for the management of certain types of risks (e.g. HACCP on food safety). Reference could also be made to relevant ISO standards, standards for the determination of maturity levels for cyber security risks, etc. When referencing a framework, it is important to clearly indicate how the framework has been utilized in the design and operation of the risk management systems. This could include whether the framework has been used as a blueprint for these systems or merely as a point of reference and/or a source of inspiration.

### 3.3.3 Limited assurance on sustainability reporting

The European Corporate Sustainability Reporting Directive (CSRD), when is it is transposed into Dutch law, requires the external auditor to provide (at least) limited assurance on the sustainability reporting. The VOR adds in bpp 1.4.3 (iii) that also the management report should state *that there is at least limited assurance that the sustainability reporting does not contain material inaccuracies.* The explanatory notes to the VOR do not define this limited assurance, nor do they address how to interpret this in relation to the limited assurance on the sustainability report provided by the external auditor. If companies wish to do so, they can define "limited assurance" as meant in the statement required by bpp 1.4.3 (iii).

The explanatory notes imply that this statement only needs to be made if the company is required to publish a sustainability report under the CSRD. Of course, this depends on the CSRD implementation timetable and scope, which at this time is unclear due to the Omnibus developments. These developments also make uncertain whether the CSRD will require "reasonable assurance" in the future, as was originally planned.

In the statement, specific reference can be made (e.g. by mentioning the relevant pages or sections) to the sustainability section in the management report, to exclude possible statements on sustainability issues that are not included in this section.

### 3.3.4 Level of certainty on effective management of operational and compliance risks

The fourth element, the *statement on the level of certainty that the internal risk management and control systems provide on the effective management of operational and compliance risks* (bpp 1.4.3 (iv)) is arguably the core of the VOR.

The explanatory notes to the VOR provide that "certainty" in this respect does not have the same meaning as the technical audit term "assurance". Furthermore, there is no requirement to use a pre-defined framework or hierarchy of "levels of certainty" that the systems could provide. It is at the discretion of the company to define the terminology used, such as "level of certainty" or "effective management of risks". This can have consequences for the scope and nature of the statement.

A description of the purpose, scope and design of the internal risk management and control systems could be provided. In cases where these systems are not designed to provide (absolute) certainty on the effective management of operational and compliance risks, this can be explicitly stated in the statement under bpp 1.4.3 (iv).

Some guidelines regarding this statement are:

- The statement could set out the responsibilities of the management board with regard to risk management.
- The statement may make reference to
    - the company's strategy;
    - its risk appetite in relation to operational and compliance risks; and
    - risks faced by the company, which might include the risk that the company's internal risk management and control systems themselves did or do not function properly.
- Reference can be made to the operational and compliance risk factors as described in the risk paragraph of the management report, (if applicable) noting that these may not include all the risks that ultimately affect the company and explaining this.

- Reference can also be made to the explanation in the risk paragraph on how the company aims to control these risks.
- The statement could describe the scope, purpose and design of internal controls, including frameworks used.
- Inherent limitations of internal controls can be described, for instance (as the explanatory notes to the VOR point out by way of example) that in controlling compliance risks the company is reliant upon the conduct of its employees worldwide, which cannot reasonably be continuously controlled or monitored.

This description could be followed by a conclusion on the level of certainty the internal risk management and control systems provide on the effective management of compliance and operational risks.

#### 3.3.5 The role of the audit committee

It is important to note that the VOR is issued by the management board, and not by the supervisory board or the audit committee.

The role of the audit committee is to prepare the supervisory board's decision-making regarding the supervision of the integrity and the quality of the company's financial and sustainability reporting, and the effectiveness of the company's internal risk management and control systems.

According to the Code, the audit committee should report to the supervisory board on its deliberations and findings. This report must include the manner in which the statement referred to in bpp 1.4.3 is substantiated. Furthermore, the audit committee could include the VOR in the supervisory board report under the most important topics for the year as expected by bpp 2.3.5. It could also be advisable to update the rules of procedures of the supervisory board and/or audit committee to align with these new Code requirements, insofar as the current provisions are deemed not sufficient.

The internal audit function reports the essence of its audit results to the audit committee. These could include any flaws in the effectiveness of the internal risk management and control systems and any findings and observations with a material impact on the risk profile of the company.

Based on these reports, the audit committee could form a position on the effectiveness of the design and operation of the internal risk management and control systems, and report to the supervisory board. This position could include an analysis on whether these findings correspond with the proposed VOR statement in the management report.

### 3.4 Interpretation

Companies can explain and define the terminology used in the VOR – for instance "level of certainty" and "effective management of risks".

Furthermore, specific disclaimers can be included in the VOR, for instance that:

- Certain risks, by their nature, cannot be effectively managed, nor is this always feasible due to high costs and dependence on the actions of people the company employs or otherwise engages or is reliant upon.

- Risk management and control systems have inherent limitations and cannot provide absolute certainty on the effective management of risks.
- Certain causes of risks sit outside the sphere of influence of the company, for instance because they are caused by or dependent on third parties or circumstances beyond the company's control.

Companies with a listing in the US could specify that the VOR statement should not be construed as a statement in response to the requirements of the US Sarbanes-Oxley Act of 2002. This is also explicitly mentioned in the explanatory notes to the VOR.

### 3.5 The role of the external auditor

The external auditor does not have an explicit role in relation to the VOR. Consequently, the external auditor does not provide assurance on the VOR. Naturally, a company can request an auditor to provide assurance on (elements of) the VOR.

The role of the external auditor is the same as for other elements of the management report, namely to assess (i) whether it contains all the mandatory elements, (ii) whether it is consistent with the financial statements, and (iii) whether, in the light of the knowledge and understanding of the organisation and its environment obtained during the audit of the financial statements, it contains no material misstatements. The NBA has further specified these assessments by the auditor in its Practice Note 1109, which is currently being updated by an internal working group of the NBA to reflect the changes in the 2025 Code.

In the context of this assessment, it is advisable to discuss the VOR with the external auditor, both in terms of the processes leading up to the VOR and the final statement in the management report.

## 4 Next steps

### 4.1 Evaluate current disclosures

Annual reports by listed companies already contain a number of disclosures on risks and risk management, including disclosures on risk appetite, the risks undertaken and faced by the company, and the internal controls and risk management systems the company has in place. Companies will need to assess the extent to which these disclosures meet the requirements of the 2025 Code.

Many annual reports do not currently include a statement on the level of certainty provided by the internal controls and risk management systems on the effective management of operational and compliance risks. This is likely to be the most impactful addition to the Code.

### 4.2 Evaluate internal processes and internal controls

Companies may evaluate their current internal processes and internal controls, for instance relating to the following topics.

- Who within the company is responsible for enterprise risk management? What is the role of the board of management, the supervisory board and the audit committee?
  - Including the role of business management (1st line), internal control (2nd line) and internal audit (3rd line).
- Which frameworks are used (for instance COSO ERM)?

- What is the company's risk appetite with regard to reporting, operational, compliance and strategic risks?
- What is the ambition level regarding these risks (for instance, for financial reporting risks the ambition level might be no misstatements within a predefined materiality, for operational risks the ambition level may be a downtime of lower than a certain threshold, etc.)?
- Which mitigating measures are in place, including, but not limited to internal control frameworks? These may also include soft controls, policies and codes, etc.
- How is design, implementation and operating effectiveness of internal controls evaluated?
- What are the conclusions of these evaluations (for instance have there been major failings)?
- How is the above discussed with the external auditor?

### 4.3 Timeline

The 2025 Code mandates that the first VOR will need be issued for the 2025 financial year. Consequently, preparations for the VOR will need to take place during this financial year.

Under the Dutch Civil Code, listed companies are required to report on their compliance with the Code on a "comply or explain" basis. The government plans to amend the relevant Decree to extend this "comply or explain" obligation to the VOR as well. This amendment is expected to take effect in the summer of 2025. As a result, companies will need to report on their adherence to the VOR using the same "comply or explain" framework. The Monitoring Committee has indicated it will closely monitor how companies implement the VOR.

To support companies in this transition, VEUO organized a symposium featuring presentations from legal experts, internal control specialists, auditors, and audit committee members. Following the symposium, several working sessions were held to discuss VOR preparations and potential statements.

We remain committed to working closely with our members as they prepare for VOR implementation. In the coming months, we will conduct a review of our members’ VOR preparations, including an evaluation of any draft statements companies intend to issue. This review will be followed by opportunities for members to engage in discussions and share insights.

* * *

**Annex 1 – Disclosures on risk management in the 2022 Code**

Below is a list of the statements that were already required from the management board under the 2022 Code:

- The statement that the management report provides sufficient insights into failings in the effectiveness of the internal risk management and control systems with regard to strategic, operational, compliance and reporting risks (bpp 1.4.3 (i)).
- The statement that these systems provide reasonable assurance that the financial reporting does not contain any material inaccuracies (bpp 1.4.3 (ii)).
- The statement that, based on the current state of affairs, it is justified that the financial reporting is prepared on a going concern basis (bpp 1.4.3 (iii)).
- The statement that the report states the material strategic, operational, compliance and reporting risks and uncertainties to the extent that they are relevant to the expectation of the company's continuity for the period of twelve months after the preparation of the report (bpp 1.4.3 (iv)).

In addition, the 2022 Code required the management board to explain in the management report the design and operation of the risk management systems and the strategic, operational, compliance and reporting risks to which the company is exposed. At a minimum, the following elements should be discussed.

- The execution of the risk assessment, including a description of the principle strategic, operational, compliance and reporting risks in relation to the company's risk appetite (bpp 1.4.2 (i)).
- The design and operation of the internal risk management and control systems during the past financial year (bpp 1.4.2 (ii)).
- Any major failings in the internal risk management and control systems which have been observed in the financial year, any significant changes made to these systems and any major improvements planned, along with a confirmation that these issues have been discussed with the audit committee and the supervisory board (bpp 1.4.2 (iii)).
- The sensitivity of the results of the company to material changes in external factors (bpp 1.4.2 (iv)).

Vereniging Effecten Uitgevende Ondernemingen

**Annex 2 – Changes of 2025 Code compared to 2022 Code**

### 1.4 Risk management accountability

The management board should render account of the effectiveness of the design and the operation of the internal risk management and control systems.

| |
|---|
| **Explanatory note**<br>The management board is responsible for ongoing monitoring of the design and operation of the internal risk management and control systems, and should assess their effectiveness at least once a year and account for this in the management report. Given the inherent practical limitations associated with internal risk management and control systems, determining the effectiveness of the design and operation of these systems cannot provide absolute certainty that all potential risks have been fully identified and mitigated at all times. Accordingly, the Board's risk management statement does not provide absolute certainty, but rather provides control of the material risks appropriate to the strategy and risk appetite. |

### 1.4.1 Accountability to the supervisory board

The management board should discuss 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 with the audit committee, and render account of this to the supervisory board

### 1.4.2 Reporting on risk management

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 operation of the internal risk management and control systems in terms of operational, compliance and reporting risks during the past financial year and what frameworks were used for that purpose;
iii. its assessment of the effectiveness of the internal risk management and control systems with respect to the operational, compliance and reporting risks during the past financial year;
iv. any major failings in the internal risk management and control systems which have been observed in the financial year, any significant changes made to these systems and any major improvements planned, along with a confirmation that these issues have been discussed with the audit committee and the supervisory board; and
v. the sensitivity of the results of the company to material changes in external factors

| |
|---|
| **Explanatory note**<br>On the basis of best practice provision 1.4.2, the management board should describe, in the management report, the design ~~and the~~, operation and assessment of the effectiveness of the internal risk management and control systems. Pursuant to section i, the company's annual report should include a description of the main risks it encounters in carrying out its tasks. The description should relate not only to reporting risks, but to all types of risks as referred to in |

best practice provision 1.2.1. Rather than providing an exhaustive list of all possible risks, the company should identify the main risks it faces. The description of the main risks in section i is in keeping with the risk section prescribed in Article 2:391 of the Dutch Civil Code and the description of the essential risks under Section 5:25(c) of the Financial Supervision Act.

With regard to best practice provision 1.4.2, section ii, it would be logical for the management board to indicate in the description of the design ~~and the~~, operation and assessment of the effectiveness of the internal risk management and control systems what framework or criteria (e.g. the COSO framework for internal control) have been used. It also makes sense for the board to make clear in the description how it has assessed the effective functioning of ~~in assessing~~ the internal risk management and control systems.

### 1.4.3 Statement by the management board

The management board should state in the management report, with clear substantiation~~, that~~:

- 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 these ~~the aforementioned~~ systems provide reasonable assurance that the financial reporting does not contain any material inaccuracies;
- iii. that these systems provide at least limited assurance that the sustainability reporting does not contain material inaccuracies;
- iv. what level of certainty these systems provide that operational and compliance risks are effectively managed;
- v. that, based on the current state of affairs, it is justified that the financial reporting is prepared on a going concern basis; and
- vi. that the report states the material risks, as referred to in best practice provision 1.2.1, and the uncertainties, to the extent that they are relevant to the expectation of the company's continuity for the period of twelve months after the preparation of the report

**Explanatory note**

Pursuant to best practice provision 1.4.3, the management board should make a statement confirming that it has provided sufficient insight into the operational, compliance and reporting risks ~~as referred to in best practice provision 1.2.1~~ and also looking ahead to the risks that will be relevant to the continuity of the company ~~as referred to in best practice provision 1.2.1~~. This includes both material shortcomings that have been identified and material risks and uncertainties that can reasonably be foreseen at the time at which the statement is issued and the broad impact of these material risks and uncertainties on the company. Sections i and vi ~~iv~~ of the management board's statement are not limited to financial reporting risks. The statement is therefore in line with the internal risk management and control systems, which are similarly not limited to financial reporting risks.

With regard to part iii, the obvious choice is to align with the introduction of the Corporate Sustainability Reporting Directive (CSRD). The CSRD and the associated European Sustainability Reporting Standards (ESRS) contain an extensive framework of standards and a detailed timeline for their implementation. It is obvious that the statement on internal risk management and control systems related to sustainability reporting risks should, in line with the CSRD, be based on providing a limited degree of assurance for the time being. A management board is free to indicate that its internal risk management and control systems with respect to sustainability information provide a reasonable degree of assurance that the sustainability reporting does not contain material inaccuracies.

In part iv, the relevant issue is that the management board, also in light of the company's risk appetite and the choice it has made in designing its internal risk management and control systems, should indicate itself what level of certainty these systems provide that operational and compliance risks are effectively controlled. The word 'certainty' in this context should not be read to mean the same as the term 'assurance' used in accountancy, nor is it intended that companies should have a set framework for determining that certainty. Nor is the term 'effectiveness' meant to be aligned with the concept used in US legislation (in this case, the Sarbanes-Oxley Act). Companies can further explain the terminology they use in their statement or the accompanying notes.

The management board may come to the conclusion that certain risks by their nature cannot be controlled effectively, or that the effectiveness of the systems mentioned above cannot be determined. An example of this is compliance with laws and regulations, where the company partly depends on the conduct of its employees worldwide, while their conduct cannot reasonably be controlled continuously or be fully embedded in procedures. To comply with this provision, the management board can declare and explain this.

As noted in the explanation to Principle 1.4, internal risk management and control systems are inextricably bound by limitations. It therefore makes sense that the statement which the management board includes in the management report on the basis of best practice provision 1.4.3 should also at least reflect on: (a) the responsibilities of the management board with regard to the internal risk management and control systems, (b) the objectives of these systems, (c) the characteristics of these systems, and (d) the inherent limitations of these systems.
~~Sections ii and iii are limited to the financial reporting risks. It should be noted, however, that this theme is currently developing and that integrated reporting (in which no distinction is any longer made between financial reporting and sustainability reporting) is on the rise. Companies are therefore encouraged to monitor and anticipate developments in integrated reporting.~~