HOUTHOFF

Amendments to the Dutch Corporate Governance Code regarding the risk management statement*

Amendments to the Code are in red and underlined.

Principle 1.2 Risk management

The company should have adequate internal risk management and control systems in place. The management board is responsible for identifying and managing the risks associated with the company's strategy and activities.

Explanatory note

The risks to be identified and managed under principle 1.2 comprise both internal and external risks which the company may face.

The internal risk management and control systems should be tailored to the company in question. This allows smaller listed companies to use less extensive procedures.

1.2.1 Risk assessment

The management board should identify and analyse the risks associated with the strategy and activities of the company and its affiliated enterprise. The identification and analysis should cover in any case the strategic, operational, compliance and reporting risks. The management board is responsible for establishing the risk appetite, and also the measures that are put in place in order to counter the risks being taken.

Explanatory note

Examples of strategic, operational, compliance and reporting risks include risks such as climate change, social inequality, tax risks, fraud risks, money laundering risks and information and communication technology risks (including cybersecurity, supplier and supply chain dependencies, data protection and risks associated with new technologies and changing business models, as in the ethically responsible use of new technologies (e.g. Responsible AI)).

In terms of strategic risks, a distinction can be made between decision-making and the implementation of the strategy. Risk management systems do not govern decision-making about strategy. The risks associated with the implementation of the strategy are operational, compliance and reporting risks. Without compromising the necessary robustness of the strategy policy, many strategic risks are not suitable for risk management because they are wholly or partly outside the company's sphere of influence.

1.2.2 Implementation

Based on the risk assessment, as referred to in best practice provision 1.2.1, the management board should design, implement and maintain adequate internal risk management and control systems. To the extent relevant, these systems should be integrated into the work processes within the company and its affiliated enterprise, and should be familiar to those whose work they are relevant to.

1.2.3 Monitoring of design and operation

The management board should monitor the design and operation of the internal risk management and control systems and should carry out a systematic assessment of their design and operation at least once a year. Attention should be paid to observed weaknesses, instances of misconduct and irregularities, indications from whistleblowers, lessons learned and findings from the internal audit function and the external auditor. Where necessary, improvements should be made to internal risk management and control systems.

Principle 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***
>
> *The management board is responsible for the ongoing monitoring of the design and operation of the internal risk management and control systems, and assesses their effectiveness at least once a year and accounts 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 will not provide absolute assurance that all risks have been fully identified and mitigated at all times. Therefore, the management board's risk management statement does not provide absolute assurance but rather appropriate control of material risks that align with 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 the areas of operational, compliance and reporting risks over the past financial year, and the frameworks used for this purpose;

iii. its assessment of the effectiveness of internal risk management and control systems concerning 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

On the basis of best practice provision 1.4.2, the management board should describe, in the management report, the design, 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, 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 in assessing the internal risk management and control system. Furthermore, it would be logical for the management board to clarify in the description how it has assessed the effective functioning of 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:

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 limited assurance that the sustainability reporting does not contain material inaccuracies;

iv. the level of assurance these systems provide in effectively managing operational and compliance risks;

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 uncertain- ties, 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~~, including 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 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.*

Regarding section iii, the obvious way to proceed is to align the statement on the internal risk management and control systems with the introduction of the CSRD. The CSRD and the accompanying ESRS provide an extensive framework of standards and a detailed timeline for their implementation. It is expected that the statement on internal risk management and control systems with regard to sustainability reporting risks in line with the CSRD will assume limited assurance for the time being. A management board has discretion to state that the internal risk management and control systems regarding sustainability information provide reasonable assurance that the sustainability reporting does not contain any material inaccuracies.

Section iv stipulates that the management board, partly considering the company's risk appetite and the choice it has made in designing its internal risk management and control systems, indicates the level of assurance these systems provide in effectively managing operational and compliance risks. The word 'assurance' should in this context not be read as the term 'assurance' used in accountancy, nor is it intended that companies should have a set framework for this. In addition, 'effectiveness' is not meant to be linked with the equivalent concept in US legislation (in this case, the Sarbanes-Oxley Act). Companies may further explain the terminology they use in their statement or accompanying notes.

The management board may conclude that certain risks, by their very nature, cannot be effectively managed, or that the effectiveness of the aforementioned systems cannot be established. An example 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 on an ongoing basis or fully embedded in procedures. To comply with this provision, the management board may clarify and explain this.

As indicated in the explanatory note to Principle 1.4, internal risk management and control systems are inextricably subject to limitations. It is therefore logical that the statement which the management board includes in the management report on the basis of best practice provision 1.4.3. also addresses at least: (a) the responsibilities of the management board regarding 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.

Principe 1.5 Role of the supervisory board

The supervisory board should supervise the policies carried out by the management board and the general affairs of the company and its affiliated enterprise. In so doing, the supervisory board should also focus on the effectiveness of the company's internal risk management and control systems and the integrity and quality of the financial and sustainability reporting.

1.5.1 Duties and responsibilities of the audit committee

The audit committee undertakes preparatory work for the supervisory board's decision-making regarding the supervision of the integrity and quality of the company's financial and sustainability reporting and the effectiveness of the company's internal risk management and control systems, as referred to in best practice provisions 1.2.1 to 1.2.3, and 1.4.1 to 1.4.3. It focuses among other things on the supervision of the management board with regard to:

i. relations with, and compliance with, recommendations and follow-up of comments by the internal and external auditors and any other external party involved in auditing the sustainability reporting;
ii. the funding of the company; and
iii. the company's tax policy.

Explanatory note

The majority of the audit committee's duties already arise out of the relevant legislation and are not repeated in the Code. Specific reference is made to Article 39 of the EU Statutory Audits Directive (Directive 2006/43/EC). This article has been implemented in Dutch legislation: Article 2(2) of the Decree of 26 July 2008. The requirements for the composition and available expertise in relation to the preparation and auditing of the financial statements are also included in Article 2 of this decree.

In some cases, especially in companies operating in the financial sector, a risk committee is established in addition to the audit committee. Article 39(4) of the above directive stipulates that, if another body has been designated to perform the functions of the audit committee, the management report must state which body carries out those functions and how that body is composed.

Various companies have set up a committee in addition to the audit committee to deal with sustainability issues relating to the company. Such a committee is often referred to as a sustainability committee or corporate responsibility committee. If a company has established such a committee, the preparation of the decision-making for the supervision of the integrity and quality of the sustainability reporting can also be carried out by such a committee instead of the audit committee.

1.5.2 Attendance of the management board, internal auditor and external auditor at audit committee consultations

The chief financial officer, the internal auditor and the external auditor should attend the audit committee meetings, unless the audit committee determines otherwise. The audit committee should decide whether and, if so, when the chairman of the management board should attend its meetings.

1.5.3 Audit committee report

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
iv. 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 how the statement referred to in provision 1.4.3 has been substantiated.

Explanatory note

If the company has established a separate committee that deals with sustainability issues relating to the company, this committee may, instead of the audit committee, report to the supervisory board on the committee's deliberations and findings and the material considerations with regard to sustainability reporting.

1.5.4 Supervisory board

The supervisory board should discuss the items reported on by the audit committee on the basis of best practice provision 1.5.3.

**No English translation of the Dutch Code has been made available by the monitoring committee as of yet. This translation is provided by Houthoff for informational purposes only and may deviate from the English translation to be published by the monitoring committee.*