

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.

Explanation

The risks to be identified and managed in the context of Principle 1.2 include both internal and external risks that the company may face.

The internal risk management and control systems must be tailored to the company. This provides smaller listed companies the opportunity to comply using 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 for the measures put in place to manage and control the risks.

Explanation

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 in the areas of cybersecurity, supplier and supply chain dependencies, data protection and risks associated with new technologies and changing business models, such as in the area of ethically responsible application of new technologies (e.g. Responsible AI)).

With regard to strategic risks, a distinction can be made between the decision-making process on the strategy and its implementation. The risk management and control systems do not oversee the decision-making on the strategy. Risks associated with the implementation of the strategy translate into operational, compliance and reporting risks. Without prejudice to the necessary robustness of the strategy determination, many strategic risks cannot be managed 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 operating effectiveness

The management board should monitor the design and operating effectiveness of the internal risk management and control systems and should carry out a systematic assessment of their design and operating effectiveness 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 report on both design and the operating effectiveness of the internal risk management and control systems.

Explanation

The Board is responsible for continuous monitoring of the design and operating effectiveness of the internal risk management and control systems and assesses their effectiveness at least once a year, reporting on it in the management report. In view of the inherent practical limitations associated with internal risk management and control systems, the determination of the design and operating effectiveness of these systems will not be able to provide absolute assurance that all possible risks have been fully identified and mitigated at all times. The Board's statement on risk management therefore does not provide absolute assurance, but declares about management of material risks in line with the board's strategy and risk appetite.

1.4.1 Accountability to the supervisory board

The management board should discuss the design and operating effectiveness 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 report on it to the supervisory board.

1.4.2 Reporting on risk management

In the management report, the management board reports on:

- i. the execution of the risk assessment, with a description of the main risks facing the company in relation to its risk appetite, as referred to in best practice provision 1.2.1;
- ii. the design and operating effectiveness of the internal risk management and control systems during the past financial year and which frameworks were used;
- iii. its assessment of the effectiveness of the internal risk management and control systems in relation to operational, compliance and reporting risks for the past financial year;
- iv. any major deficiency in the internal risk management and control systems 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.

Explanation

Based on best practice provision 1.4.2, the management board describes in the management report the design, operating effectiveness and the assessment of the effectiveness of the internal risk management and control systems. Pursuant to part i, the company includes in its annual report a description of the main risks with which it faces in the performance of its tasks. The description does not only cover reporting risks, but also all types of risks referred to in best practice provision 1.2.1. This is not so much an exhaustive explanation of all potential risks, but a description of the main risks the company faces. The description of main risks in section i is in line with the risk section prescribed in Section 2:391 of the Dutch Civil Code (hereinafter: the Dutch Civil Code) and with the description of material risks in the context of Section 5:25c of the Financial Supervision Act.

With regard to best practice provision 1.4.2, part ii, it is expected that the management board indicates, in the reporting on the design and operating effectiveness of the internal risk management and control systems, which reference or standards framework (e.g. the COSO framework for internal control) has been used. It is also expected that the management board clearly explains how it has assessed the operating effectiveness 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 deficiency 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 sustainability reporting is free from material misstatements;
- 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 includes material risks, as referred to in best practice provision 1.2.1, as well as uncertainties, to the extent that they are relevant for the company's continuity for a period of twelve months after the preparation of the report.

Explanation

Based on best practice provision 1.4.3, the management board declares that it has provided sufficient insight into the operational, compliance and reporting risks as referred to in best practice provision 1.2.1 ~~also looking forward to~~ the risks relevant to the continuity of the company ~~as referred to in best practice provision 1.2.1~~. This concerns both identified material shortcomings

and material risks and uncertainties that can reasonably be foreseen at the time the statement is given, as well as the impact of these material risks and uncertainties on the company. Parts i and vi of the management board's statement are not limited to financial reporting risks. This is in line with the internal risk management and control systems, also not limited to financial reporting risks.

With regards to part iii, it is obvious to seek connection with the introduction of the CSRD. The CSRD and the associated European Sustainability Reporting Standards (ESRS) contain a comprehensive framework of standards and a detailed timeline for their implementation. It is obvious that the reporting about the internal risk management and control systems with regard to sustainability reporting risks in line with the CSRD, for the time being assumes the provision of limited assurance. A management board is free to indicate that the internal risk management and control systems with regard to sustainability information provide reasonable assurance that the sustainability reporting does not contain any material misstatements.

Part iv is about the management board self-indicating the level of certainty that the risk management and internal control systems provide about effectively managing the operational and compliance risks, considering the company's risk appetite and the choice made in designing the internal risk management and control systems. In this context, the word 'certainty' is not to be read as the term 'assurance' used in auditing, nor is it intended that companies should apply a fixed framework for this. Nor is 'effectiveness' connected to the similar wording in American legislation (i.e. the Sarbanes-Oxley Act). Companies can explain the terminology used in their statement or in the explanation thereof.

It is possible that the management board will conclude that certain risks cannot be effectively managed by their nature, or that the effectiveness of the aforementioned systems cannot be determined. An example is compliance with laws and regulations, where the company is partly dependent on the behaviour of its employees worldwide, while their behaviour cannot reasonably be continuously controlled or fully embedded in procedures. To comply with this provision, the management board can declare this and explain.

As noted in the explanatory note to Principle 1.4, internal risk management and control systems are inextricably restricted. It is therefore logical that the statement that the management board also includes in the management reporting based on best practice provision 1.4.3: (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.

Principle 1.5 Role of the supervisory board

The supervisory board should oversee 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 inclusive as well as 1.4.1 to 1.4.3 inclusive. It focuses among other things on the supervision of the management board with regard to:

- i. connecting with, implementation and follow up on recommendations 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.

Explanation

Most of the tasks assigned to the audit committee already stem from legislation and have not been repeated in the Code. Specific reference is made to Article 39 of European Audit Directive 2006/43/EC. This article is implemented in Dutch legislation: Article 2, paragraph 2 of the Decree of 26 July 2008. Requirements for the composition and available expertise with regard to the preparation and audit of the annual accounts, are also included in Article 2 of the aforementioned Decree.

In some cases, especially in the case of companies active in the financial sector, a risk committee has been set up in addition to an audit committee. Article 39(4) of the aforementioned Directive states that the management report must include information about another body being appointed to carry out the tasks of the audit committee, and about the composition of that body.

In the meantime, several companies set up a committee, in addition to the audit committee, to oversee sustainability issues relating to the company. Such a committee is often called a sustainability committee or corporate responsibility committee. If a company has set up such a committee, the preparation of the decision-making in the context of the supervision of integrity and quality of sustainability reporting, can be carried out by this 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 reports 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 design and operating effectiveness 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, were analysed and discussed, along with a description of the most important findings of the audit committee, and the way if substantiating the statement meant in provision 1.4.3.

Explanation

In case the company has established a separate committee to oversee the company's sustainability issues, this committee may report to the supervisory board on the committee's deliberations and findings and the material considerations regarding sustainability reporting, instead of the audit committee.

1.5.4 Supervisory board

The supervisory board discusses the reporting by the audit committee, done on the basis of best practice provision 1.5.3.