Discussion Paper

Risk management and internal control systems

NIVRA taskforce on Internal Control

Royal NIVRA

ISBN-13: 978-90-75103-46-5

Table of Contents

1 Foreword

In December 2003, the Corporate Governance Committee in the Netherlands, chaired by Mr Tabaksblat, published the Dutch Corporate Governance Code. This Code, which has been given statutory footing in the Netherlands Civil Code, lays down principles of good governance and best practice provisions.

One of the main principles of the Code is the management board 's responsibility to maintain adequate and effective internal risk management and control systems. Best practice provision II.1.4 of the Code stipulates that "the board of management shall declare in the annual report that the internal risk management and control systems are adequate and effective, and shall provide clear substantiation of this".

In its report of December 2005 the Monitoring Committee Corporate Governance Code concluded that the application of best practice provision II.1.4 required improvement, and provided additional guidance. In its second monitoring report, issued in December 2006, the Monitoring Committee concluded that the application of best practice provision II.1.4 had greatly improved, notwithstanding some remaining questions with respect to the application of the revised best practice provision II.1.4. and the absence of a generally accepted practice. In this respect the Monitoring Committee has confirmed its believe that the present system should be and remain principle-based, and that a generally accepted practice should be established in the market by the various parties concerned, in consultation among themselves.

This Discussion Paper is a first step towards such generally accepted practice. It takes into consideration the results of a roundtable session organised by the Netherlands Institute for Corporate Governance (NICG), in collaboration with the Royal Dutch Institute for Registeraccountants (NIVRA), on 1 November 2006. In this session, chaired by Mr Peters, CFO's and audit committee members of Dutch listed companies, in the presence of Mr Tabaksblat, discussed current practices and areas for improvement with regards to risk management and internal control systems, and the reporting thereon.

The participants of the NICG/NIVRA roundtable session expressed a strong preference for a full and consistent application of the UK approach to internal control and reporting thereon, and in particular the guidance provided by the Turnbull-Committee:

> *The board should, as a minimum, disclose that there is an ongoing process for identifying, evaluating and managing the significant risks faced by the company, that it has been in place for the year under review and up to the date of approval of the annual report and accounts, that it is regularly reviewed by the board and accords with the guidance provided by the FRC. In addition, the board should summarise the process it has applied in reviewing the effectiveness of the system of internal control and confirm that necessary actions have been or are being taken to remedy any significant failings or weaknesses identified from that review. It should also disclose the process it has applied to deal with material internal control aspects of any significant problems disclosed in the annual report and accounts.*

The UK approach does not include a requirement to provide a 'forward looking statement' Evidence gathered by the Turnbull Review Group demonstrates that the substantial improvements in internal control instigated by application of the Turnbull guidance, which was first issued in

1999, have been achieved without the need for detailed prescription as to how to implement the guidance. The principles-based approach has required boards to think seriously about control issues and enabled them to apply the principles in a way that appropriately dealt with the circumstances of their business. The evidence also supported the proposition that the companies which have derived most benefit from application of the guidance were those whose boards saw embedded risk management and internal control as an integral part of running the business.

The NIVRA taskforce on Internal Control concurs with the views of the roundtable participants, as it beliefs that the preferred approach to managing risks and reporting thereon is to consider all risk-categories equally, rather than differentiating between financial reporting risks and other risks. In addition the taskforce is of the opinion that management's declaration with regards to financial reporting risks, as currently required by the revised best practice provision II.1.4., may cause an expectation gap and leads to a 'rules based approach', as it resembles management's declaration required by section 404 of the Sarbanes Oxley Act in the US.

The UK approach is a truly principle based approach, in accordance with the Code as originally drafted. Accordingly, the taskforce strongly endorses adoption of the flexible, principles-based, Turnbull guidance, amended for the specifics of the business and legal environment in the Netherlands. Therefore, the guidance included in this Discussion Paper is largely based on the Revised Guidance for Directors on the Combined Code, which was published by the UK Financial Reporting Council (FRC) in the autumn of 2005.

The taskforce invites all parties concerned to reflect on the guidance included in this document and provide any relevant feedback that may support the development of a generally accepted practice for the application of best practice provision II.1.4 of the Code.

NIVRA taskforce on Internal Control
5 October 2007

2 Introduction

The importance of risk management and internal control systems

1. A company's risk management and internal control systems have key roles in the management of risks that are significant to the fulfillment of its business objectives. A sound system of internal control contributes to safeguarding the shareholders' investment and the company's assets.

2. Enterprise risk management enables management to identify, assess, and manage risks in the face of uncertainty, and is integral to value creation and preservation. Enterprise risk management is most effective when these mechanisms are built into the entity's infrastructure and are part of the essence of the enterprise. By building in enterprise risk management, an entity can directly affect its ability to implement its strategy and achieve its mission[1].

3. Risk management and internal control systems are an integral part of enterprise risk management. This enterprise risk management framework encompasses internal control, forming a more robust conceptualization and tool for management.

4. Internal control (as referred to in paragraph 19 facilitates the effectiveness and efficiency of operations, helps ensure the reliability of internal and external reporting and assists compliance with laws and regulations.

5. Effective financial controls, including the maintenance of proper accounting records, are an important element of internal control. They help ensure that the company is not unnecessarily exposed to avoidable financial risks and that financial information used within the business and for publication is reliable. They also contribute to the safeguarding of assets, including the prevention and detection of fraud.

6. A company's objectives, its internal organisation and the environment in which it operates are continually evolving and, as a result, the risks it faces are continually changing. Sound risk management and internal control systems therefore depend on a thorough and regular evaluation of the nature and extent of the risks to which the company is exposed. Since profits are, in part, the reward for successful risk-taking in business, the purposes of risk management and internal control systems are to help manage and control risk appropriately rather than to eliminate it.

This guidance and its purpose

7. This guidance intends to:
   - reflect sound business practices whereby risk management and internal control systems are embedded in business processes by which a company pursues its strategic and operational objectives;
   - remain relevant over time in the continually evolving business environment; and

1 Many definitions included in this guidance are derived from the *Internal Control - Integrated Framework* (1992) and the *Enterprise Risk Management Framework* (2004) of the Committee of Sponsoring Organisations of the Treadway Commission (COSO). For purposes of readability detailed references are not included throughout this guidance.

- enable each company to apply this guidance in a manner which is suitable to it and takes company specific circumstances into account.

The guidance requires management and supervisory board members to exercise judgement regarding the companies' implementation of the Dutch Corporate Governance Code requirements related to risk management and internal control systems based on reviews and the reporting to shareholders by means of the annual report.

8. The guidance is based on the adoption of a risk based approach by a company's board to establishing sound risk management and internal control systems and to review its effectiveness. This should be incorporated by the company within its normal management and governance processes. It should not be treated as a separate exercise undertaken to meet regulatory requirements.

9. The Dutch Corporate Governance Committee (Tabaksblat Committee) has published the Dutch Corporate Governance Code in December 2003. The Code stipulates (Principle II.1) that the role of the management board is to manage the company, which means, among other things, that it is responsible for achieving the company's aims, strategy and policy, and results. The management board is accountable for this to the supervisory board and to the general meeting of shareholders. In discharging its role, the management board shall be guided by the interests of the company and its affiliated enterprise, taking into consideration the interests of the company's stakeholders. The management board shall provide the supervisory board in good time with all information necessary for the exercise of the duties of the supervisory board.

10. The management board is responsible for complying with all relevant legislation and regulations, for managing the risks associated with the company activities and for financing the company. The management board shall report related developments to and shall discuss the risk management and internal control systems with the supervisory board and its audit committee.

11. Best practice provision II.1.3 requires that the company shall have a risk management and internal control system that is suitable for the company. It shall, in any event, employ as instruments of the risk management and internal control system:
    a. risk analyses of the operational and financial objectives of the company;
    b. a code of conduct which should, in any event, be published on the company's website;
    c. guides for the layout of the financial reports and the procedures to be followed in drawing up the reports; and
    d. a system of monitoring and reporting.

12. In addition, best practice provision II.1.4 determines that the management board shall declare in the annual report that the risk management and internal control systems are adequate and effective and shall provide clear substantiation of this. In the annual report, the management board shall report on the operation of the risk management and internal control system during the year under review. In doing so, it shall describe any significant changes that have been made and any major improvements that are planned, and shall confirm that they have been discussed with the audit committee and the supervisory board.

13. The Code does not provide a prescribed lay-out or content for the statement stipulating how these principles and best practice provisions should be applied. The intention of the Code is that companies should be free to explain their risk management and internal control systems

policies based on the principles, but in a way that suits them, and is justified by the special circumstances which have led the organisation to adopt a particular approach.

14. The direction offered by this document should be considered as a practical guidance for management and supervisory board members that assists them in the application of best practice provisions II.1.3 and II.1.4 of the Code.

15. For the purpose of this guidance, internal controls considered by the management board, should include all types of controls; including those of a strategic, operational and compliance nature, as well as internal financial controls

Groups of companies

16. Throughout this guidance, where reference is made to 'company' it should be taken, where applicable, as referring to the group of which the reporting company is the parent company. For groups of companies, the review of effectiveness of internal control and the report to the shareholders should be from the perspective of the group as a whole.

Appendix

17. The Appendix to this document contains questions which management boards may wish to consider in applying this guidance..

3 Maintaining sound risk management and internal control systems

Definition of enterprise risk management and internal control

18. Enterprise risk management is a process, ongoing and flowing through an entity, and is effected by an entity's management board and other personnel. It is applied in strategy setting and applied across the enterprise, at every level and unit, and includes taking an entity level portfolio view of risk. Enterprise risk management is designed to identify potential events that, if they occur, will affect the entity and to manage risk within its risk appetite. Enterprise risk management is able to provide reasonable assurance regarding the achievement of entity objectives to an entity's management board, geared to achievement of objectives in one or more separate but overlapping categories.
    Enterprise risk management, no matter how well designed and operated, cannot provide a guarantee regarding achievement of an entity's objectives. Reasonable assurance reflects the notion that uncertainty and risk relate to the future, which no one can predict with precision. The Monitoring Committee takes 'reasonable assurance' to mean a degree of certainty that would be satisfactory for a prudent manager in the management of his affairs in the given circumstances.

19. The universally used definition of Internal control is defined in the COSO enterprise risk management framework. Internal control is:
    A process, affected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:
    - Strategic - high-level goals, aligned with and supporting its mission
    - Operations - effective and efficient use of its resources
    - Reporting - reliability of reporting
    - Compliance - compliance with applicable laws and regulations

    Enterprise risk management has certain limitations. The limitations relate to the limits of human judgment, resource constraints, and the need to consider the cost of controls in relation to expected benefits, the reality that breakdowns can occur, and the possibility of management override and collusion.

20. In considering limitations of enterprise risk management, three distinct concepts must be recognized:
    - First, risk relates to the future, which is inherently uncertain.
    - Second, enterprise risk management - even effective enterprise risk management - operates at different levels with respect to different objectives. For strategic and operations objectives, enterprise risk management can help ensure that management, and the board in its oversight role, is aware, in a timely manner, only of the extent to which the entity is moving towards achievement of these objectives. But it cannot provide even reasonable assurance that the objectives themselves will be achieved.
    - Third, enterprise risk management cannot provide absolute assurance with respect to any of the objective categories.

Elements of a sound system of internal control

21. An internal control system encompasses the policies, processes, tasks, behaviours and other aspects of a company that, taken together:
    - facilitate its effective and efficient operation by enabling it to respond appropriately to significant business, operational, financial, compliance and other risks to achieving the company's objectives. This includes the safeguarding of assets from inappropriate use or from loss and fraud and ensuring that liabilities are identified and managed;
    - help ensure the quality of internal and external reporting. This requires the maintenance of proper records and processes that generate a flow of timely, relevant and reliable information form within and outside the organization;
    - help ensure compliance with applicable laws and regulations, and also with internal policies with respect to the conduct of business.

    A company's system of internal control will reflect its control environment which encompasses its organizational structure. The system will furthermore include:
    - risk assessment;
    - control activities;
    - information and communications processes; and
    - processes for monitoring the continuing effectiveness of the system of internal control.

22. The system of internal control should:
    - be embedded in the operations of the company and form part of its culture;
    - be capable of responding quickly to evolving risks to the business arising from factors within the company and to changes in the business environment; and
    - include procedures for reporting immediately to appropriate levels of management any significant control failings or weaknesses that are identified together with details of corrective action being undertaken.

23. A sound system of internal control reduces, but cannot eliminate, the possibility of poor judgement in decision-making; human error; control processes being deliberately circumvented by employees and others; management overriding controls; and the occurrence of unforeseeable circumstances.

24. A sound system of internal control therefore provides reasonable, but not absolute, assurance that a company will not be hindered in achieving its business objectives, or in the orderly and legitimate conduct of its business, by circumstances which may reasonably be foreseen.

25. A system of internal control cannot, however, provide protection with certainty against a company failing to meet its business objectives or all material errors, losses, fraud, or breaches of laws or regulations.

Responsibilities of the management board in maintaining sound risk management and internal control systems

26. The management board is responsible for the company's system of internal control. It should set appropriate policies on internal control and seek regular assurance that will enable it to satisfy itself that the system is functioning effectively. The management board must further ensure that the system of internal control is effective in managing those risks in the manner which it has approved.

27. The Dutch Corporate Governance Code states in the additional information provided with regard to the board's statement on internal control (best practice provision II.1.4) that: it would be logical for the management board to indicate in the declaration on the risk management and internal control systems what framework or system of standards (for example the COSO Internal Control - Integrated Framework) it has used in evaluating the risk management and internal control systems. Therefore the establishment and the employment of an internal control framework, which functions as a guideline for internal control evaluation falls under the responsibility of the management board.

28. In determining its policies with regard to internal control, and thereby assessing what constitutes sound risk management and internal control systems in the particular circumstances of the company, the management board's deliberations should include consideration of the following factors:
    - the nature and extent of the risks facing the company;
    - the extent and categories of risk which it regards as acceptable for the company to bear;
    - the likelihood of the risk concerned materializing;
    - the company's ability to reduce the incidence and impact on the business of risks that do materialize; and
    - the costs of operating particular controls relative to the benefit thereby obtained in managing the related risks.

29. It is the role of the management board to implement policies on risk and control. In fulfilling its responsibilities the management board should identify and evaluate the risks faced by the company for consideration and design, operate and monitor a suitable system of internal control which implements the policies adopted by the management board.

Responsibilities of the employees in maintaining sound risk management and internal control systems

30. All employees have some responsibility for internal control as part of their accountability for achieving objectives. They, collectively, should have the necessary knowledge, skills, information, and authority to establish, operate and monitor the system of internal control. This will require an understanding of the company, its objectives, the industries and markets in which it operates, and the risks it faces.

4 Reviewing the effectiveness of risk management and internal control systems

Responsibilities of the management board

31. Dutch Corporate Governance Code advocates that the management board takes responsibility for the disclosure on internal control in the annual report. Best practice provision II.1.4 of the Dutch Corporate Governance Code, regarding the board's statement on internal control, is applicable to the management board and states that the management board shall annually declare that the risk management and internal control systems are adequate and effective and shall provide clear substantiation of this. Furthermore the Code states that the management board shall report related developments too and shall discuss the risk management and internal control systems with the supervisory board and its audit committee (Principle II.1).

32. Reviewing the effectiveness of internal control is an essential part of the management's board's responsibilities. The management board will need to form its own view on effectiveness based on the information and assurances provided to it, exercising the standard of care generally applicable to directors in the exercise of their duties. Management is accountable to the management board for monitoring the system of internal control and for providing assurance to the management board that it has done so.

Responsibilities of the supervisory board

33. The supervision of the management board by the supervisory board shall include the structure and operation of the risk management and internal control systems. (best practice provision III.1.6(c))

34. The supervisory board - or the audit committee as subcommittee of the supervisory board - shall in any event focus on supervising the activities of the management board with respect to the operation of the risk management and internal control systems, including supervision of the enforcement of the relevant legislation and regulations, and supervising the operation of codes of conduct. (best practice provision III.5.4)

35. The supervisory board shall discuss at least once a year the risks of the business and the result of the assessment by the management board of the structure and operation of the risk management and internal control systems, as well as any significant changes thereto. (best practice provision III.1.8)

36. The supervisory board and its individual members each have their own responsibility for obtaining all information from the management board and the external auditor that the supervisory board needs in order to be able to carry out its duties properly as a supervisory organ. If the supervisory board considers it necessary, it may obtain information from officers and external advisers of the company. The company shall provide the necessary means for this purpose. The supervisory board may require that certain officers and external advisers attend its meetings. (best practice provision III.1.9)

Responsibilities of internal auditing

37. Internal auditing typically operates in two capacities. First, internal auditors provide independent, objective assessments to provide assurance on the appropriateness of the organization's governance structure and the operating effectiveness of specific governance activities. Second, they act as catalysts for change, advising or advocating improvements to enhance the organization's governance structure and practices.

    In an organization, management and the board establish and monitor companywide systems for effective governance. Internal auditors can support and improve these actions. In addition, although internal auditors should remain independent, they may participate in the establishment of governance processes. By providing assurance on the organization's risk management, internal control, and governance processes, internal auditing becomes a key cornerstone for effective organizational governance.

    Which capacity is most relevant for internal auditing is highly influenced by the maturity level of the organization's governance processes and structure, and the organizational role. In an organization with a less mature governance structure and process, the internal audit function may be focused more on advice regarding optimal structure and practices. In organizations with more structured and mature governance practices, internal auditors could focus more on:

    - Evaluating whether companywide governance components work together as expected.
    - Analyzing the level of reporting transparency among parts of the governance structure.
    - Comparing governance best practices.
    - Identifying compliance with recognized and applicable governance codes.

Responsibilities of the external auditor

38. The report of the external auditor pursuant to article 2:393, paragraph 4, Civil Code shall contain the matters which the external auditor wishes to bring to the attention of the management board and the supervisory board in relation to his audit of the annual accounts and the related audits. Best practice provision V.3.4 mentions that for example the external auditor might include the following matters with regard to the audit and risk management and internal control systems: :
    - information about the course of events during the audit and cooperation with internal auditors and/or any other external auditors, matters for discussion with the management board, a list of corrections that have not been made, etc.
    - the reliability and continuity of automated data processing
    - the quality of the internal provision of information:
    - points for improvement, gaps and quality assessments;
    - comments about threats and risks to the company and the manner in which they should be reported in the particulars to be published;
    - compliance with articles of association, instructions, regulations, loan covenants, requirements of external supervisors, etc.

The effectiveness of risk management and internal control systems

39. Determining whether enterprise risk management is "effective" is a judgment resulting from an assessment of whether the five components have been, and still are, present and functioning effectively. Thus, the components are also criteria for effective enterprise risk

management and internal control systems. For the components to be present and functioning properly there can be no material weaknesses, and risk needs to have been brought within the entity's risk appetite.

40. When enterprise risk management is determined to be effective in each of the four categories of objectives, respectively, the management board and directors have reasonable assurance that:
    - They understand the extent to which the entity's strategic objectives are being achieved
    - They understand the extent to which the entity's operations objectives are being achieved
    - The entity's reporting is reliable
    - Applicable laws and regulations are being complied with

The process for reviewing effectiveness of risk management and internal control systems

41. Ongoing monitoring activities of an enterprise, including managerial activities and everyday supervision of employees, generate insights from those who are directly involved in the entity's activities. These insights are gained in real time and can provide quick identification of deficiencies. Other sources of deficiencies are the separate evaluations of enterprise risk management. Evaluations performed by management, internal auditors, or other functions can highlight areas in need of improvement. External parties frequently provide important information on the functioning of an entity's enterprise risk management. These include customers, vendors and others doing business with the entity, external auditors, and regulators. Reports from external sources should be carefully considered for their implications for enterprise risk management, and appropriate corrective actions should be taken.

42. Effective monitoring on a continuous basis is an essential component of sound risk management and internal control systems. The management board cannot, however, rely solely on the embedded monitoring processes within the company to discharge its responsibilities. It should regularly receive and review reports on internal control. In addition, the management board should undertake an annual assessment for the purposes of making its public statement on risk management and internal control systems to ensure that it has considered all significant aspects of internal control for the company for the year under review and up to the date of approval of the annual report.

43. The management board should define the process to be adopted for its review of the effectiveness of risk management and internal control systems. This should encompass both the scope and frequency of the reports it receives and reviews during the year, and also the process for its annual assessment, such that it will be provided with sound, appropriately documented, support for its statement on internal control in the company's annual report.

44. The reports from management to the management board should, in relation to the areas covered by them, provide a balanced assessment of the significant risks and the effectiveness of risk management and internal control systems in managing those risks. Any significant control failings or weaknesses identified should be discussed in the reports, including the impact that they have had, could have had, or may have, on the company and the actions being taken to rectify them. It is essential that there be openness of communication by management with the management board on matters relating to risk and control.

45. When reviewing reports during the year, the management board should:
    - consider what are the significant risks and assess how they have been identified, evaluated and managed;
    - assess the effectiveness of the related system of internal control in managing the significant risks, having regard in particular to any significant failings or weaknesses in internal control that have been reported;
    - consider whether necessary actions are being taken promptly to remedy any significant failings or weaknesses; and
    - consider whether the findings indicate a need for more extensive monitoring of the system of internal control.

46. Additionally, the management board should undertake an annual assessment for the purpose of making its public statement on risk management and internal control systems. The assessment should consider issues dealt with in reports reviewed by it during the year together with any additional information necessary to ensure that the management board has taken account of all significant aspects of risk management and internal control systems for the company for the year under review and up to the date of approval of the annual report

47. The management board's annual assessment should, in particular, consider:
    - the changes since the last annual assessment in the nature and extent of significant risks, and the company's ability to respond to changes in its business and the external environment;
    - the scope and quality of management's ongoing monitoring of risks and of the system of internal control, and, where applicable, the work of its internal audit function and other providers of assurance;
    - the extent and frequency of the communication of the results of the monitoring to the management board which enables it to build up a cumulative assessment of the state of control in the company and the effectiveness with which risk is being managed;
    - the incidence of significant control failings or weaknesses that have been identified at any time during the period and the extent to which they have resulted in unforeseen outcomes or contingencies that have had, could have had, or may in the future have, a material impact on the company's financial performance or condition; and
    - the effectiveness of the company's public reporting processes.

48. The frequency of separate evaluations necessary for management to have reasonable assurance about the effectiveness of enterprise risk management is a matter of management's judgment. In making that determination, consideration is given to the nature and degree of changes occurring and their associated risks, the competence and experience of the personnel implementing risk responses and related controls, and the results of ongoing monitoring. Usually, some combination of ongoing monitoring and separate evaluations will ensure that enterprise risk management maintains its effectiveness over time.

49. Should the management board become aware at any time of a significant failing or weakness in internal control, it should determine how the failing or weakness arose and reassess the effectiveness of management's ongoing processes for designing, operating and monitoring the system of internal control.

5 The management board's disclosures and statement on risk management and internal control systems

Recommendations for declaration in annual report regarding internal control[2]

50. The annual report and accounts should include such meaningful, high-level information as the management board considers necessary to assist shareholders' understanding of the main features of the company's risk management processes and system of internal control, and should not give a misleading impression.

51. In its narrative statement in the annual report of how the company has applied best practice provision II.1.4, the management board should, as a minimum, disclose that there is an ongoing process for identifying, evaluating and managing the identified significant operational, strategic,financial, legislative, regulatory and financial reporting risks faced by the company, that it has been in place for the year under review and up to the date of approval of the annual report and accounts, that it is regularly reviewed by the management board and supervisory board and accords with the guidance in this document.

52. The disclosures relating to the application of best practice provision II.1.4 should include an acknowledgement by the management board that it is responsible for the company's system of internal control and for reviewing its effectiveness. Relating to best practice provision III.1.8 the disclosures should also state that the evaluation of the design and operational effectiveness of the risk management and internal control system is being discussed with the Supervisory Board / Audit Committee. It should also explain that such a system is designed to manage rather than eliminate the risk of failure to achieve business objectives, and can only provide reasonable and not absolute assurance against material misstatement or loss.

53. In relation to best practice provision II.1.4, the management board should summarise the process it has applied in reviewing the effectiveness of the system of internal control and confirm that necessary actions have been or are being taken to remedy any significant failings or weaknesses identified from that review. It should also disclose the process it has applied to deal with material internal control aspects of any significant problems disclosed in the annual report and accounts.

54. Where a management board cannot make one or more of these disclosures, it should state this fact and provide an explanation.

55. Where material joint ventures and associates have not been dealt with as part of the group for the purposes of applying this guidance, this should be disclosed.

---

2 The proposed declaration deviates from best practice provision II.1.4 which states that: The management board shall declare in the annual report that the internal risk management and control systems are adequate and effective and shall provide clear substantiation of this. In the annual report, the management board shall report on the operation of the internal risk management and control system during the year under review. In doing so, it shall describe any significant changes that have been made and any major improvements that are planned, and shall confirm that they have been discussed with the audit committee and the supervisory board.

6 Appendix

Assessing the effectiveness of the company's risk management and internal control systems

Some questions which the management board may wish to consider and discuss with management when regularly reviewing reports on internal control and when carrying out its annual assessment are set out below. The questions are not intended to be exhaustive and will need to be tailored to the particular circumstances of the company.

This Appendix should be read in conjunction with the guidance set out in this document.

Risk assessment

- Does the company have clear objectives and have they been communicated so as to provide effective direction to employees on risk assessment and control issues? For example, do objectives and related plans include measurable performance targets and indicators?
- Are the significant internal and external operational, financial, compliance and other risks identified and assessed on an ongoing basis?
- Is there a clear understanding by management and others within the company of what risks are acceptable to the management board?

Control environment and control activities

- Does the management board have clear strategies for dealing with the significant risks that have been identified? Is there a policy on how to manage these risks?
- Do the company's culture, code of conduct, human resource policies and performance reward systems support the business objectives and risk management and internal control system?
- Does senior management demonstrate, through its actions as well as it policies, the necessary commitment to competence, integrity and fostering a climate of trust within the company?
- Are authority, responsibility and accountability defined clearly such that decisions are made and actions taken by the appropriate people? Are the decisions and actions of different parts of the company appropriately co-ordinated?
- Does the company communicate to its employees what is expected of them and the scope of their freedom to act? This may apply to areas such as customer relations; service levels for both internal and outsourced activities; health, safety and environmental protection; security of tangible and intangible assets; business continuity issues; expenditure matters; accounting; and financial and other reporting.
- Do people in the company (and in its providers of outsourced services) have the knowledge, skills and tools to support the achievement of the company's objectives and to manage effectively risks to their achievement?
- How are processes/controls adjusted to reflect new or changing risks, or operational deficiencies?

Information and communication

- Do management and the management board receive timely, relevant and reliable reports on progress against business objectives and the related risks that provide them with the

information, from inside and outside the company, needed for decision-making and management review purposes? This could include performance reports and indicators of change, together with qualitative information such as on customer satisfaction, employee attitudes etc.
- Are information needs and related information systems reassessed as objectives and related risks change or as reporting deficiencies are identified?
- Are periodic reporting procedures, including half-yearly and annual reporting, effective in communicating a balanced and understandable account of the company's position and prospects?
- Are there established channels of communication for individuals to report suspected breaches of law or regulations or other improprieties?

Monitoring

- Are there ongoing processes embedded within the company's overall business operations, and addressed by senior management, which monitor the effective application of the policies, processes and activities related to internal control and risk management? (Such processes may include control self-assessment, confirmation by personnel of compliance with policies and codes of conduct, internal audit reviews or other management reviews).
- Do these processes monitor the company's ability to re-evaluate risks and adjust controls effectively in response to changes in its objectives, its business, and its external environment?
- Are there effective follow-up procedures to ensure that appropriate change or action occurs in response to changes in risk and control assessments?
- Is there appropriate communication to the management board (or board committees) on the effectiveness of the ongoing monitoring processes on risk and control matters? This should include reporting any significant failings or weaknesses on a timely basis.
- Are there specific arrangements for management monitoring and reporting to the management board on risk and control matters of particular importance? These could include, for example, actual or suspected fraud and other illegal or irregular acts, or matters that could adversely affect the company's reputation or financial position.

Royal NIVRA

A.J. Ernststraat 55
P.O Box 7984
1008 AD Amsterdam
The Netherlands
T +31 (0)20 301 03 01
F +31 (0)20 301 03 02
E nivra@nivra.nl
I www.nivra.nl