IIA Netherlands

The Institute of Internal Auditors - Netherlands, is the only professional body in the Netherlands solely dedicated to the profession of internal auditing. We are part of the global Institute of Internal Auditors, which sets the International Professional Practice of Internal Auditing, and the Code of Ethics, which all members agree to follow. The IIA represents, promotes and develops the professional practice of internal auditing. We have more than 170,000 members in 165 countries worldwide, and 2,500 members in the Netherlands.

IN CONTROL & DISCLOSURE
THROUGH THE EYES OF THE INTERNAL AUDITOR

RESEARCH ON CURRENT PRACTICE IN THE NETHERLANDS AND INPUT FOR THE CORPORATE GOVERNANCE CODE MONITORING COMMITTEE
Annex 3 Reference to other research and guidance

The following list of other research material and guidance reports have been reviewed and referred to in this research:

7. IAARF: Internal Audit Capability Model for the Public Sector (2009)
10. Impact on governance; research on cooperation internal and external auditor - Nivra and IIA (2009)
11. ECIA - European Governance Magazine (2011)
Table of contents

Executive Summary 5

1. Introduction 6
   1.1 Background and objectives 6
   1.2 Research activities 6
   1.3 Overview of response [A] 6

2. In control & disclosure – research results 8
   2.1 Risk management and internal control systems (B) 8
      2.1.1 Summary of current practice 8
      2.1.2 Conclusions 12
   2.2 Disclosing risks and risk management and internal control systems (C) 13
      2.2.1 Summary of current practice 13
      2.2.2 Conclusions 13
   2.3 In control statement over financial reporting [D] 13
      2.3.1 Summary of current practice 13
      2.3.2 Conclusions 14
   2.4 Reporting alleged irregularities (E) 14
      2.4.1 Summary of current practice 14
      2.4.2 Conclusions 14

3. The role of the Internal Auditor 15
   3.1 The Internal Auditor in the Netherlands 15
   3.2 The role of IAF on ‘In control & disclosure’ 15
      3.2.1 Independence and reporting lines 15
      3.2.2 Scope of work 16
      3.2.3 Role on In-control statements and oversight 17
      3.2.4 Conclusions 17

4. Recommendations to the Monitoring Committee 18
   4.1 Risk Management and Control System 18
   4.2 The Internal Audit Function 18

Annex 1 Best practices from the Code 20
Annex 2 Detailed survey scope and results 21
Annex 3 Reference to other research and guidance 27
Foreword

Dear reader,

It is my pleasure to introduce this report that provides insight in to control & disclosure practices at companies in the Netherlands based on the requirements from the Dutch Corporate Governance Code. In particular we looked at best practices with regards to risk management, internal control and compliance frameworks and the level of embedding across the companies in scope of this research. The results being presented are considered from the perspective of the internal auditor and also include his own role.

Internal audit directors from 34 companies - most listed at the Amsterdam stock exchange - participated in the survey, which constitutes a response of 64%. The survey results have been validated and discussed in two round table sessions with the participants and a few others players in the field of governance. In these sessions best practices and conclusions in the areas being researched have been discussed, including the recommendations to the Corporate Governance Code Monitoring Committee.

I would like to thank all involved for their time and effort to participate in this research.

Michel Kee, RA
Board member IIA Netherlands & Project lead

Executive Summary

The purpose of the Dutch Corporate Governance Code is to protect the interests of the stakeholders; ‘Good entrepreneurship, including integrity and transparency of decision-making by the management board, and proper supervision thereof, including accountability for such supervision, are essential if the stakeholders are to have confidence in the management’. The Code is principle-based and includes best practices. Listed companies are required to implement these best practices or explain in their annual reports why they have not done so. The Corporate Governance Code (hereafter: Monitoring Committee) ensures that the Code is up-to-date and practicable and monitors compliance.

The internal audit function (IAF) has enhanced its professionalism and has evolved in the past two decades to become an essential and integral element of the governance framework of organisations. That perspective is further underpinned by this research conducted by the Institute of Internal Auditors (IIA) Netherlands. The objective of this research was to identify how companies are organised to meet the requirements from the Code on risk management and internal control systems including the disclosure thereof. Another goal was to provide clear recommendations to the Monitoring Committee. The research is conducted from the perspective of internal auditors and therefore called In control & disclosure - through the eyes of the internal auditor. In total 34 companies participated in this research, which constitutes a response of 64%.

In control & disclosure (chapter 2)
- Generally risk management and internal control systems have improved over the past few years and further enhancements are planned.
- Business management (1st line of defence) is broadly made accountable to manage risks and ensure effective controls, supported by a variety of specialised risk management, compliance and other control functions (2nd line of defence). It is essential that these lines of defence (including the IAF as 3rd line of defence) coordinate their work to ensure a coherent and efficient company-wide risk management and control framework.
- Different maturity levels of risk management exist across the companies included in the scope of the research. For instance, in several companies (outside the financial services sector) risk management is still perceived to be a requirement under the Code and not viewed as a management tool to support decision making. Risk appetite is not clearly defined or documented for 50% of the respondents.

Recommendations to the Monitoring Committee (chapter 4)
- Adjustments to the best practices II.1.3, II.1.4 and III.1.8 are proposed in order to bring these more in line with current practice and improve consistency between these.
- Generally research shows that the IAF has a strong independent assurance and advisory role on the company’s risk management and internal control systems. Consequently, and also inspired by the Banking and Insurance Codes, an adjusted principle and best practice provisions of the Code on the role of the IAF (V.3) are being proposed.
- Some of the research results raise new topics for further research (e.g. the audit committee agenda). The Institute of Internal Auditors Netherlands is committed to making a continued contribution.
1. Introduction

1.1 Background and objectives

The Dutch Corporate Governance Code requires that listed companies have a risk management and internal control system in place and provide disclosures regarding their systems in their annual reports, including an "in control" statement on financial reporting. The Monitoring Committee ensures that the Code is up-to-date and practicable and monitors compliance by listed Dutch companies.

The Institute of Internal Auditors (IIA) Netherlands conducted this research to identify how companies are organised to meet these requirements from the perspective of internal auditors. The purpose was to identify and share best practices and provide input to the Monitoring Committee. Special focus is given to the role of the Internal Audit Function (IAF) on these requirements.

Annex 1 provides reference to the best practices of the Code which have been most relevant to this research.

1.2 Research activities

Internal audit directors of all AEX funds, a selection of other listed companies, financial institutions and various other unlisted organisations that voluntarily comply with the Dutch Corporate Governance Code have been invited to participate in the survey. The IAF is mostly well-positioned to ensure compliance with, and/or contribute to, these corporate governance requirements. Please note that despite the independent and objective mindset of the internal auditor, the research results do not necessarily fully reflect the perceptions of the management of the company.

The survey included the following sections:
A. Company profile
B. Risk management and internal control systems
C. Disclosing risks and risk management and internal control systems
D. In control statement over financial reporting
E. Reporting alleged irregularities

For the body of the report we selected the most interesting responses. Annex 2 provides a detailed overview of the survey scope and all quantifiable results.

After the analysis of the survey results we held two roundtables with internal audit directors and other players in the field of governance to further discuss the results with the aim of identifying best practices in the area, being researched. The research provides clear opportunities for additional, more detailed research on specific areas. In Netherlands is committed to make a continued contribution.

In addition to the above we also conducted a review of relevant research and guidance reports (annex 3 provides a list of the relevant reports).

1.3 Overview of response (A)

1.3.1 Participating companies

In total 34 companies (64% of 53 companies approached) responded to the survey. The majority of the respondents (70%) are listed on the Amsterdam Stock Exchange. The Dutch Corporate Governance Code is applicable to these companies. Other companies (10 in total) agreed to comply with the Code voluntarily.

Table 1 below lists the respondents by type of listing (AEX, mid-caps, small-caps and companies that are not listed on the Amsterdam Stock Exchange). Most of the financial sector companies that responded are not listed.

1.3.2 Industries

Most of the participating companies are from the manufacturing/fast-moving consumer goods (FMCG) industry (10) and financial services sector (9). Diagram 1 shows a breakdown by industry.

1.3.3 Size of company

Half of the responding companies have more than 25,000 employees globally. From the responding companies, 18 (53%) operate in more than 25 countries, while 21 companies (62%) report having annual gross sales over € 5 billion.

1.3.4 Management philosophy

The majority of the respondents (68%) say that their company is mostly decentralized in structure. Of this group, 6 companies indicate that they are moving towards more centralisation, which affects the control environment.

Table: Management philosophy

<table>
<thead>
<tr>
<th>Philosophy</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fully centralized</td>
<td>5 (9%)</td>
</tr>
<tr>
<td>Mostly centralized</td>
<td>24 (26%)</td>
</tr>
<tr>
<td>Mostly decentralized</td>
<td>6 (23%)</td>
</tr>
</tbody>
</table>

Graph 1: Management philosophy

1.3.6 Relevant Corporate Governance Codes

All listed companies replied that the Dutch Corporate Governance Code is applicable. Most of the companies that are not listed voluntarily comply with the Code. In addition, requirements from foreign stock exchanges were mentioned, as well as other codes and regulations that are mandatory in the countries where the companies operate. These may provide different or stricter requirements compared to the Code.

Diagram 1: Respondents by industry
2. In control & disclosure - research results

2.1 Risk management and internal control systems (B)

2.1.1 Summary of current practice

Organisation and accountability (B.1)

The three lines of defence model - as illustrated in diagram 2 - is a useful tool to explain and demonstrate the roles in internal governance and the interaction between them.

Overall, the research shows support for the three lines of defence model. As a 1st line of defence, business management has ownership, responsibility and accountability for assessing, controlling and mitigating risks. A strong 1st line of defence in which business management proactively, transparently and continuously monitors risks and maintains sound internal controls and an ethical culture indicates the existence of a strongly embedded and mature control environment. Business management is made accountable for ensuring effective risk management and internal control at 91% of the participating companies, showing the need for improvements in 9% (3) of the cases. Management is supported by 2nd line of defence functions (e.g. business control, risk management, compliance, integrity and a variety of other functions; very different across the participating companies). These 2nd line functions are focused on supporting the internal governance process by means of policies and monitoring activities and facilitating the implementation of effective risk management practices by business management. As a 3rd line of defence, the IAF, using a risk-based approach, will provide independent assurance1 to senior management, executive board and audit committee on the adequacy of the design of the risk management and internal control processes and the effective operation of the 1st and 2nd lines of defence. This assurance task covers all elements of an organisation’s risk management, internal control and compliance framework. The IAF acts as a 3rd line of defence, as reported by 79% of the respondents. The external auditor might be considered as a 4th line of defence with respect to financial reporting.

Diagram 2: Three lines of defence model

“IT is not the ship so much as the skilful sailing that assures the prosperous voyage”

George William Curtis

Generally, as illustrated in the graphs below, risks and responsibilities of risk, compliance and assurance functions are clearly defined and formally documented. 50% of the respondents, however, indicate that certain improvements can be made: cooperation between the various functions can be further optimised at 31% of the participating companies.

2.2 Risk Management (B.2)

In order to provide some perspective to the research results, first some general comments on risk management are made:

Enterprise risk management is a process, effected by an entity’s board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

Risk maturity of the organisation can be qualified in 5 categories: (1) Risk naïve, (2) Risk aware, (3) Risk defined, (4) Risk managed and (5) Risk enabled.

Over the last few years, the importance of managing risk as part of strong corporate governance has been increasingly acknowledged. Organisations are under pressure to identify the significant business risks they face - social, ethical, and environmental as well as strategic, financial, and operational - and to explain how they manage them. The use of enterprise-wide risk management frameworks has expanded as organisations recognise the advantages of coordinated approaches to risk management.

All respondents reported that responsibility for the risk management function’s activities of the company lies with (a member of) the management board.

The survey shows that 79% of respondents have a structured company-wide risk management process in place to continuously evaluate and mitigate strategic, operational, financial (reporting), compliance and project risks. A key driver for making risks explicit rather than implicit (managing risks has always been part of business) is the increasing and evolving company risk profile due to amongst others - business expansion, growing business complexity, continuous organisational changes, evolving business partnerships and technology, and increasing legislation. Managing risks is a core business activity in the financial services sector and therefore generally embedded in a structured way.

The risk management process is embedded in the regular management cycle for 82% of the respondents, as opposed to being organised as a separate/disconnected process.

For 59% of the respondents, the risk management process is perceived as a management tool, while 41% of the respondents (all outside financial services sector) and reflecting a higher level for non-AEX) indicate that it is perceived as a corporate governance requirement, thus implying a risk of them over substance2. The Monitoring Committee wishes to ensure that corporate governance does not become a box-ticking exercise, in which strict adherence to the letter of the provisions becomes more important than acting in the spirit of the Code.

Risks and responsibilities of risk, compliance and assurance functions are clearly defined and formally documented

Graph 3: Risks and responsibilities of risk, compliance and assurance functions are clearly defined and formally documented

Graph 4: Coordination of activities of the risk, compliance and assurance functions is optimised

Risk appetite is defined as the level of risk that is acceptable to the board or management. This may be set in relation to the organisation as a whole, for different groups of risks or at an individual risk level3.

The risk appetite is effectively defined and documented, as indicated by only 50% of the respondents. As a rule the financial services sector has defined (quantified) and documented the company risk appetite; as this is also required by the Banking and Insurance Codes. A non-financial services company reported that its financing and credit rating strategy indicates its risk appetite from a financial perspective. Others mention that their risk appetite is mostly of a qualitative nature, like managing the balance between growth through acquisitions and the sound integration of such acquisitions.

Graph 5: Risk appetite is clearly defined and documented

Risk comes from not knowing what you’re doing

Warren Buffett

The survey shows that 79% of respondents have a structured company-wide risk management process in place to continuously evaluate and mitigate strategic, operational, financial (reporting), compliance and project risks. A key driver for making risks explicit rather than implicit (managing risks has always been part of business) is the increasing and evolving company risk profile due to amongst others - business expansion, growing business complexity, continuous organisational changes, evolving business partnerships and technology, and increasing legislation. Managing risks is a core business activity in the financial services sector and therefore generally embedded in a structured way.

The risk management process is embedded in the regular management cycle for 82% of the respondents, as opposed to being organised as a separate/disconnected process.
“If everything seems under control, you’re just not going fast enough”

Mario Andretti

When internal control frameworks are in place, these are derived from the COSO® framework, as reported by 91% of the respondents. Business management owns these frameworks, as reported by 94% of the respondents. Design and operating effectiveness of internal control frameworks are periodically reviewed and continuous improvement is fostered, as reported by 91% of the respondents. These reviews are mostly a joint effort between management and internal control specialists, as illustrated in the graphs below. A clear best practice is not indicated; generally, however, there is room for extending the use of risk and control self-assessments by business management. In general, the role of management on assessing controls is stronger at the AXA funds compared to the other companies.

“Laws control the lesser man… Right conduct controls the greater one”

Mark Twain

The code of conduct is periodically reviewed and updated, as reported by 91% of the respondents. The graphs below indicate that most companies can further improve on keeping the code actively alive through management representation (B6). As illustrated in the graphs below, generally there is room for improvement in making policies clearer, easier assessable and up-to-date and in monitoring compliance with policies.

“Those who look only to the past or present are certain to miss the future”

John F. Kennedy

The LOR is standard text with a limited number of specific disclosures, as indicated by 94% of the respondents. The frequency of the LOR is - depending on applicable governance legislation - varied across the spectrum of participating companies: 26% on a quarterly basis, 29% depending on applicable governance legislation. In 5 cases (15%) no structured program w.Is/was in place to implement the code of conduct, including awareness sessions, training, defining roles and responsibilities.

““You have to learn the rules of the game. And then you have to play better than anyone else”

Albert Einstein

The LOR is standard text with a limited number of specific disclosures, as indicated by 94% of the respondents. The frequency of the LOR is - depending on applicable governance legislation - varied across the spectrum of participating companies: 26% on a quarterly basis, 29% twice a year and 41% annually.

The graph below shows that as a rule companies can improve on having documented guidelines in place to support reviewing internal control frameworks in a structured and consistent manner.

Graph 11: Documented guidelines support reviewing internal control frameworks.

Code of conduct (B4)

With only a few exceptions, companies have established a code of conduct defining expected behaviour of employees. These codes are approved by the management board and available on the companies’ websites. In 5 cases (15%) no structured program w.Is/was in place to implement the code of conduct, including awareness sessions, training, defining roles and responsibilities.

Policies (B5)

Companies have a structured document in place to establish, update, review, approve and communicate policies, as indicated by 62% of the respondents. Policies are approved and communicated by the management board at 94% of the participating companies. As illustrated in the graphs below, generally there is room for improvement in making policies clearer, easier assessable and up-to-date and in monitoring compliance with policies.
In the absence of an audit committee, this is the responsibility of the entire supervisory board and the effectiveness of the company-wide risk management and control systems are somewhat inconsistent and might overall be too high.

Graph 19: The supervisory board/audit committee is effectively overseeing the effectiveness of the company-wide risk management and internal control systems. It is discussed with the management board and supervisory board/audit committee.

Overview (R)\(^l\)

Regular meetings/oversight bodies (in addition to the audit committee) are in place to oversee results from the risk, compliance and audit activities, according to 94% of the respondents. All meetings/oversight bodies are attended by the internal auditor at 91% of the participating companies, while the external auditor attested in 68% of the cases. The graph below shows that cascading of such meetings/oversight bodies to lower management levels to enable accountability could generally be improved.

Graph 17: Oversight meetings/oversight bodies are cascaded to lower management to enable accountability

“A good decision is based on knowledge and not on numbers”  
Plato

The graph below shows that follow-up and monitoring of reported non-compliance/issues could be improved at 35% of the participating companies.

\(^l\)Section B7 and B8 are included in chapter 3

\(^{11}\)In the absence of an audit committee, this is the responsibility of the entire supervisory board

2.3 In control statement on financial reporting (D)

2.3.1 Summary of current practice

The function/manager responsible for coordinating the preparation of the in control statement on financial reporting differs per participating company. The CFO is mentioned by 53% of the respondents or else this task has been delegated to risk management (29%) or IF (15%).

Companies have a clear framework and guidelines in place for evaluating the effectiveness of internal control on financial reporting, as reported by 91% of the respondents (see also 2.1.1 - Internal Control Frameworks). The use of management self-testing can broadly be expanded. Most of the respondents indicate that the in control statement goes beyond financial reporting (66%).

“You don’t concentrate on risks, you concentrate on results. No risk is too great to prevent the necessary job from getting done”  
Chuck Yeager

The table below summarizes the activities which are most relevant in supporting the in control statement.

<table>
<thead>
<tr>
<th>Performance analysis/review</th>
<th>Fully agree</th>
<th>Mostly agree</th>
<th>Mostly disagree</th>
<th>Fully disagree</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance</td>
<td>0%</td>
<td>6.5%</td>
<td>22.3%</td>
<td>70.7%</td>
<td></td>
</tr>
<tr>
<td>Regular supervision</td>
<td>0%</td>
<td>2.1%</td>
<td>28.8%</td>
<td>70.3%</td>
<td></td>
</tr>
<tr>
<td>Formal control framework</td>
<td>0%</td>
<td>5.1%</td>
<td>20.4%</td>
<td>72.6%</td>
<td></td>
</tr>
<tr>
<td>Formal management selftesting</td>
<td>5.6%</td>
<td>17.4%</td>
<td>26.5%</td>
<td>50.4%</td>
<td></td>
</tr>
<tr>
<td>Letter of representation</td>
<td>2.9%</td>
<td>5.9%</td>
<td>41.8%</td>
<td>50.4%</td>
<td></td>
</tr>
<tr>
<td>Audits</td>
<td>2.9%</td>
<td>5.9%</td>
<td>24.7%</td>
<td>76.5%</td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td>20%</td>
<td>11.4%</td>
<td>25.3%</td>
<td>42.9%</td>
<td></td>
</tr>
</tbody>
</table>

Table 3: Activities supporting the in control statement

2.3.2 Conclusion

As management is responsible for the design and effectiveness of the internal control system, formal self-testing should be seen as a good practice to substantiate the reported conclusion in the in control statement, in addition to internal and external audits.
2.4 Reporting alleged irregularities (E)

2.4.1 Summary of current practice

All participating companies have a whistle-blowing procedure in place to allow employees to report irregularities and wrongdoing. At 91% of these companies this can also be done anonymously. Maintaining employee awareness is crucial. Internal audit may assist management with providing training to the employees. Whistle-blowing cases are generally investigated independently in timely fashion and effectively, although IAFs reported room for improvement. As illustrated in the graph below, a cross-functional committee (e.g. ethics or integrity committee) is broadly in place to oversee effectiveness of the code of conduct and whistleblowing. At 26% of the participating companies, however, such a formal committee has not been established.

“Respect for right conduct is felt by every body”
Jane Austen

<table>
<thead>
<tr>
<th>Fully disagree</th>
<th>Mostly disagree</th>
<th>Mostly agree</th>
<th>Fully agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>17,6%</td>
<td>8,8%</td>
<td>26,9%</td>
<td>47,1%</td>
</tr>
</tbody>
</table>

Graph 22: A formal cross-functional committee (e.g. ethics or integrity committee) exists to oversee effectiveness of code of conduct and whistleblowing

Results from whistle-blowing/fraud cases are, as a rule periodically reported to the management board and supervisory board/advisory committee, with some room for improvement reported by 1 out of 7 respondents.

2.4.2 Conclusions

In general, whistle-blowing procedures exist; maintaining employee awareness is crucial.

Results on investigated cases are reported in timely fashion to the appropriate levels of management.

A cross functional ethics or integrity committee is considered good practice from the research. It brings various disciplines and areas of expertise together to have oversight on the integrity program. It monitors investigations of reported cases and draws conclusions on the business ethics in a broader sense.

3. The role of the Internal Auditor

3.1 The Internal Auditor in the Netherlands

Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization’s operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.1

- Definition The Institute of Internal Auditors1

Internal audit advisory role is not always clear to the stakeholders. Traditionally, the IAF has mainly fulfilled an assurance role through its independent audits. Currently the IAF more often acts as a subject matter expert advising on the design of internal control frameworks. Other activities may include, facilitating risk workshops and assisting in the implementation of control measures. Obviously, internal audit independence and objectivity must remain intact. After all, these are key drivers of the IAF’s added value. The schedule below identifies IAF’s audit key responsibilities, possible advisory roles it may assume, and tasks that they should not perform.

Key role of IAF Permitted advisory projects of IAF based on sufficient guarantees*

- Provide assurance on risk management systems, including compliance
- Provide assurance on the control of major risks
- Evaluate in control statements and risk reports
- Provide assurance on the reliability of financial and other management information
- Provide assurance on compliance with laws and regulations
- Advise on the design of risk management
- Assist with implementation of control systems
- Facilitate risk control self-assessment
- Assist in preparing control for approved by management
- Participate in projects as subject expert
- Determine objectives of organisation and risk appetite
- Ongoing monitoring of realisation of objectives and mitigation of risks
- Advise on follow up recommendation from audit reports
- Issue in control statements for external risk takers
- Carry responsibility for the quality of control systems

Tasks of directors and line management not to be performed by IAF

Table 4: Role of the IAF

* To maintain its objectivity IAF should not accept management responsibility. IAF may advise but line management is ultimately responsible for the design and effectiveness of risk management and Internal control systems. It is good practice to have a formal confirmation on the scope of the work, the role and responsibilities of both IAF and management in these types of advisory work. Assurance on a project is needed a reasonable amount of time should be taken this account (e.g. one year) if the same person would do the audit. As leader of risk control off assessment the auditor should make it very clear that he/she is not part of the discussion, but just acts as a mediator. The auditor is not responsible for the outcome of the assessment. Another option is to subsume certain assurance assignments.

Size of the IAF

Respondents from the survey total small to large IAF. An overview of the size of IAF across the 34 participating companies is shown below. All IAF’s with a staff up to 10 FTE are from outside the financial services sector, while 5 out of 7 IAF’s with a capacity above 100 FTE are from the financial services sector. Two respondents out of 34 say that the IAF has not yet been fully established in their company.

3.2 The role of IAF on ‘In control & disclosure’

The sections in the survey on ‘In control & disclosure’ included the current role of the IAF on the areas researched, which is summarised in this chapter.

3.2.1 Independence and reporting lines

The IAF acts independently and objectively as the 3rd line of defence in their companies, as indicated by 94% of the respondents. The table below shows the IAF mostly has multiple reporting lines, hierarchical reporting line is mostly to the CEO (60%). Double hierarchical reporting lines are indicated by 5 respondents. Double functional reporting lines exist at most of the participating companies. Hierarchical reporting to the CEO added to functional reporting to the CFO and audit committee is considered best practice.

“Change before you have to”
Jack Welch

LEVEL 5 Optimising
LEVEL 4 Managed
LEVEL 3 Integrated
LEVEL 2 Infrastructure
LEVEL 1 Initial

Diagram 3: Internal audit capability model

<table>
<thead>
<tr>
<th>Size of IAF</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 – 5 FTE</td>
</tr>
<tr>
<td>6 – 10 FTE</td>
</tr>
<tr>
<td>11 – 20</td>
</tr>
<tr>
<td>21 – 100</td>
</tr>
<tr>
<td>More than 100</td>
</tr>
</tbody>
</table>

Graph 23: Number of FTEs in the IAF

Maturity levels of the IAF

Some of the respondents are in an early phase of introducing the concept of internal auditing in their company. Other IAF’s have existed for more than 50 years. The diagram below shows the IAF maturity levels through the capability model that the Research Foundation of the IIA developed.

“Change before you have to”
Jack Welch

LEVEL 5 Optimising
LEVEL 4 Managed
LEVEL 3 Integrated
LEVEL 2 Infrastructure
LEVEL 1 Initial

Diagram 3: Internal audit capability model

The role of the IAF on ‘In control & disclosure’

The sections in the survey on ‘In control & disclosure’ included the current role of the IAF on the areas researched, which is summarised in this chapter.

3.2.1 Independence and reporting lines

The IAF acts independently and objectively as the 3rd line of defence in their companies, as indicated by 94% of the respondents. The table below shows the IAF mostly has multiple reporting lines, hierarchical reporting line is mostly to the CEO (60%). Double hierarchical reporting lines are indicated by 5 respondents. Double functional reporting lines exist at most of the participating companies. Hierarchical reporting to the CEO added to functional reporting to the CFO and audit committee is considered best practice.
The IAF is mostly equally positioned, involved, aligned and rewarded compared to other direct reports of the management board, which confirms the development the function risk underpins.

3.2.2 Scope of work

Overview

As illustrated in the diagram below, the IAF - on average - spend most of their time on operational audits (43%), while IT and financial audits add up to 28%. Audits in the areas of risk management and compliance take in total 17% of the available resources.

Risk management and internal control systems

The IAF is the catalyst in forming risk management and provides proactive advice on management practices, as reported by 77% of the respondents.23 The IAF contributes to the facilitation of the identification and evaluation of key risks at 62% of the participating companies, as illustrated below.

If you can dream it, you can do it

Walter Elias (Walt) Disney

The IAF is making a strong contribution to the effectiveness, evaluation and improvement of the company-wide risk management and control systems, as reported by 91% of respondents. The IAF has effective oversight over the 2nd line assurance functions, as reported by 88% of the respondents.24

Compliance

Most of the IAFs (74%) are involved in whistle-blowing and fraud investigations, covering the management of the investigations, requiring specific competencies, to partly or wholly. The IAF directs 21% (62%) act as a trusted person in the follow-up of whistle-blowing cases, which is not considered best practice. Those who do not have such a role refer to other functions, such as integrity, compliance or human resources. If an ethics or integrity committee exists, the IAF director is a member in 68% of the cases.

Role of the external auditor

The external auditor is reviewing and reporting on the company-wide risk management and internal control systems within the scope of the regular financial audit assignment, as indicated by 91% of the respondents. As 32% of the participating companies the external auditor is also assigned to review parts of risk management and control systems beyond the regular financial reporting assignment. This is generally considered the domain of the IAF.

The external auditor, within the boarders of the financial audit assignment, can generally improve the reliance on the work performed by the IAF, as illustrated below:25

Conclusions

- The IAF generally plays a key role in Corporate Governance, as does the external auditor, both supporting the management board and the audit committee in their oversight responsibilities.
- Direct reporting line to CEO and functionally to CFO and audit committee is considered best practice to ensure an independent position of the IAF in the companies.
- Depending on the size and risk maturity level of the company, the IAF may play different roles, from providing advice to independent assurance. The perception of the external auditor is that the IAF acts as the main catalyst in forming risk management and facilitates the identification and evaluation of key risks.
- Overall, the IAF is well-positioned and appropriately staffed to evaluate the design and effectiveness of risk management and internal control systems.

The policy of being too cautious is the greatest risk of all

Jawaharlal Nehru

- Almost 60% of audits are spent on operational and IT audits.
- Most companies do not ask their external auditor to review (parts of) the risk management and control systems beyond the financial reporting assignment. It is broadly the domain of the IAF to provide assurance in these areas.
- Generally speaking, external auditors can improve on placing reliance on the work performed by the IAF in these areas.
- The role of the IAF in the LOD process and the quality of the disclosure on risks and the system of risk management and internal controls could be further expanded.
4. Recommendations to the Monitoring Committee

The focus of the Monitoring Committee in last year’s report was on the shareholders and the supervisory board and its composition. There may be an opportunity for the current year to provide further guidance on best practices as they relate to risk management and internal control. The chapter provides recommendations for adjusting some of the applicable best practice provisions, if appropriate, or for providing further guidance by the Monitoring Committee, including concerning the role of the IF. Based on the results of this research.

4.1 Risk Management and Control System

Best practice II.1.3

The company shall have an internal risk management and control system that is suitable for the company. It shall, in any event, employ as instruments of the internal risk management and control system: a) risk analyses of the strategic, operational, compliance and financial objectives of the company and effective risk responses; by a code of conduct which should be kept alive and published on the company’s website.

The recommendation is to widen the scope of risk assessment: a) also to strategic and compliance risk, which is considered best practice and consistent with the requirements of best practices II.1.4 and II.1.8. Concerning the code of conduct, the recommendation is to add that, in order to maintain a sound ethical culture, the code needs to be kept alive (e.g., continuous awareness training, employee induction programs, oversight and monitoring). Research shows that this is considered best practice.

“The secret to success is to own nothing, but control everything”

Jack Welch

Best practice II.1.4

In the annual report the management board shall provide:

a) a description of main risks related to the strategy and operations of the company and the mitigating responses;

b) a description of the design and effectiveness of the internal risk management and control systems during the financial year;

Recommendation is to bring best practice II.1.4 [a/b] in line with the proposed adjusted best practice II.1.3 [a].

Best practice III.1.8

The supervisory board shall discuss at least once a year the corporate strategy, the risk appetite and the main risks of the business, the result of the assessment by the management board of the design and effectiveness of the internal risk management and control systems, as well as any significant changes therein. Reference to those discussions shall be made in the report of the supervisory board. The research shows that risk appetite is not effectively defined and communicated by the management board.

when the risk appetite is clearly defined (can also be qualitative) and effectively communicated by the management board.

4.2 The Internal Audit Function (IAF)

Generally, the research shows that the IAF has a strong assurance and advisory role on the company’s risk management and internal control systems. This is very different across the range of participating companies dependent on the stage of development of embedding sound risk management and internal control practices.

For the next version of the Dutch Corporate Governance Code, the recommendations are to change the principle and best practice provisions concerning the IAF, also inspired by the Banking Code 2010 and the Insurance Code

The following revised principle and best practice provisions are recommended.

Principle: The management board shall ensure that an IAF is established and have been designed properly, are in place and are effectively monitored and properly working. The internal auditor shall report his findings and recommendations for improvement to the management board and the audit committee.

V.3.1 The internal auditor, management board, external auditor and audit committee shall consult periodically, including as regards the risk analysis, the IAF in conjunction with internal and external audit plans and the outcome of the audits performed by internal and external auditors. Current V.3.1 included

V.3.2 The internal auditor shall have unrestricted access to the chairman of the audit committee. Current V.3.2 slightly adjusted

...
Annex 1 Best practice provisions from the Code

The following existing best practice provisions from the Dutch Corporate Governance Code have been referred to in this research.

Best practice II.1.3
The company shall have an internal risk management and control system that is suitable for the company. It shall, in any event, employ an instrument of the internal risk management and control system:

a) risk analyses of the operational and financial objectives of the company;

b) a code of conduct which should 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.

Best practice II.1.4
In the annual report the management board shall provide:

a) a description of main risks related to the strategy of the company;

b) a description of the design and effectiveness of the internal risk management and control systems for the main risks during the financial year; and

c) a description of any major failings in the internal risk management and control systems which have been discovered in the financial year, any significant changes made to these systems and any major improvements planned, and a confirmation that these issues have been discussed with the audit committee and the supervisory board.

Best practice II.1.5
As regards financial reporting risks the management board states in the annual report that the internal risk management and control systems provide a reasonable assurance that the financial reporting does not contain any errors of material importance and that the risk management and control systems worked properly in the year under review. The management board shall provide clear substantiation of this.

Best practice II.1.7
The management board shall ensure that employees have the possibility of reporting alleged irregularities of a general, operational and financial nature within the company to the chairman of the management board or to an official designated by him, without jeopardising their legal position. Alleged irregularities concerning the functioning of management board members shall be reported to the chairman of the supervisory board. The arrangements for whistleblowers shall be posted on the company’s website.

Best practice III.1.8
The supervisory board shall discuss at least once a year the corporate strategy and the main risks of the business, the result of the assessment by the management board of the design and effectiveness of the internal risk management and control systems, as well as any significant changes thereto. Reference to these discussions shall be made in the report of the supervisory board.

Annex 2 Detailed survey scope and results

The annex provides a detailed overview of the questions included in the survey and the results except for the answers to the open-end questions. The questions not based on fully/mostly agree/disagree have been marked with an (*) and explained in italic text.

A. Company profile

<table>
<thead>
<tr>
<th>Question</th>
<th>Disagree</th>
<th>Mostly Agree</th>
<th>Mostly Disagree</th>
<th>Agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.1</td>
<td>What is the name of your company</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A.2</td>
<td>What type of industry fits best your organisation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A.3</td>
<td>Total number of employees at the end of 2010</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A.4</td>
<td>Gross sales level (Annual Report 2010 in Euros)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A.5</td>
<td>Number of countries the company operates in</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A.6</td>
<td>Management philosophy respectively: fully centralised, mostly centralised, mostly decentralised, fully decentralised</td>
<td>2 9 23 0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A.7</td>
<td>What is the overall company risk profile respectively: low, moderate high, very high</td>
<td>8 21 5 0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

B. Risk management and internal control system

Best practice II.1.3
The company shall have an internal risk management and control system that is suitable for the company. It shall, in any event, employ an instrument of the internal risk management and control system:

a) risk analyses of the operational and financial objectives of the company;

b) a code of conduct which should 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.

B.1.1 Organisation and accountability

<table>
<thead>
<tr>
<th>Question</th>
<th>Disagree</th>
<th>Mostly Agree</th>
<th>Mostly Disagree</th>
<th>Agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>B.1.1</td>
<td>Business management is accountable to ensure effective risk management and control systems</td>
<td>2 1 5 26</td>
<td></td>
<td></td>
</tr>
<tr>
<td>B.1.2</td>
<td>Which assurance/compliance functions are in place supporting the risk management and control systems</td>
<td>Open-end question</td>
<td></td>
<td></td>
</tr>
<tr>
<td>B.1.3</td>
<td>Roles and responsibilities of these assurance/compliance functions are clearly defined and formally documented</td>
<td>1 2 14 17</td>
<td></td>
<td></td>
</tr>
<tr>
<td>B.1.4</td>
<td>The coordination of activities of these assurance/compliance functions is optimised ensuring no overlaps and gaps in approach</td>
<td>0 2 22 10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>B.1.5</td>
<td>The AE has an effective oversight over the (second-line) assurance functions</td>
<td>1 3 16 14</td>
<td></td>
<td></td>
</tr>
<tr>
<td>B.1.6</td>
<td>Which member of the management board is responsible for the risk management function/activities of the company</td>
<td>Open-end question</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

B.2 Risk management

<table>
<thead>
<tr>
<th>Question</th>
<th>Disagree</th>
<th>Mostly Agree</th>
<th>Mostly Disagree</th>
<th>Agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>B.2.1</td>
<td>The company has defined and documented its risk appetite in an understandable, usable and consistent manner, resulting in quantitative output</td>
<td>5 12 12 5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>B.2.2</td>
<td>The company has a structured company-wide risk management process in place to continuously evaluate and mitigate strategic, operational, financial (reporting), compliance and project risks</td>
<td>2 5 18 9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>B.2.3</td>
<td>The risk management process is supported by detailed guidelines (definitions, criteria, steps) and templates</td>
<td>3 8 12 13</td>
<td></td>
<td></td>
</tr>
<tr>
<td>B.2.4</td>
<td>The risk management process is embedded in the regular management cycle</td>
<td>2 4 12 16</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
B.4.2 The code of conduct includes … *

B.4.1 A code of conduct to define expected behaviour of employees is established and available on the company's website.

B.3.9 The IAF independently reviews the design and operating effectiveness of internal control frameworks.

B.3.8 Operating effectiveness of internal control frameworks are periodically reviewed and continuous improvement is fostered.

B.3.7 Internal control frameworks are owned by management.

B.3.6 The company has a formalised and structured company-wide internal control framework in place for …

B.2.13 The IAF regularly reviews the effectiveness of the company-wide risk management process.

B.2.12 The IAF aligns its audit plan to company risk assessments and provides assurance on mitigation strategies concerning selected key risks.

B.2.11 The IAF facilitates the identification and evaluation of key risks.

B.2.10 The effectiveness of the risk management process is evaluated and continuous improvement is fostered.

B.2.9 Risk assessments contribute to management decision making.

B.2.8 Structured risk assessments are performed on the level of …

B.2.7 The IAF independently reviews the design and operating effectiveness of internal control frameworks.

B.2.6 The risk management process is perceived to be … respectively … fully/mostly corporate governance requirement, fully/mostly management only, fully/mostly management and control systems.

B.2.5 Management board.

B.2.4 Regional/divisional management.

B.2.3 Operating units management.

B.2.2 Corporate functions.

B.2.1 Business processes.

B.1.2 Tax.

B.1.1 Compliance with financial policies.

B.1.0 Compliance with other policies.

B.0.9 Reporting controls.

B.0.8 Reporting disclosures.

B.0.7 Fraud and irregularities.

B.0.6 Financial reporting.

B.0.5 Corporate functions.

B.0.4 Operating unit management.

B.0.3 Regional/divisional level.

B.0.2 Business controls.

B.0.1 Design of internal control frameworks are owned by management.

B.0.0 Design of internal control frameworks are owned by management.

B.3.3 Internal control frameworks are periodically reviewed and updated/documented.

B.3.2 These internal control frameworks are based on or derived from COSO.

B.3.1 The company has a formalised and structured company-wide internal control framework in place for financial reporting.

B.2.14 The IAF is making a strong contribution to oversee overall effectiveness of the company-wide risk management.

B.2.13 The IAF is making a strong contribution to continuously evaluate and improve the company-wide risk management.

B.2.12 The IAF is making a strong contribution to provide assurance on mitigation strategies concerning selected key risks.

B.2.11 The IAF is making a strong contribution to the identification and evaluation of key risks.

B.2.10 The effectiveness of the risk management process is evaluated and continuous improvement is fostered.

B.2.9 Risk assessments contribute to management decision making.

B.2.8 Structured risk assessments are performed on the level of …

B.2.7 The IAF independently reviews the design and operating effectiveness of internal control frameworks.

B.2.6 The risk management process is perceived to be … respectively … fully/mostly corporate governance requirement, fully/mostly management only, fully/mostly management and control systems.

B.2.5 Management board.

B.2.4 Regional/divisional management.

B.2.3 Operating units management.

B.2.2 Corporate functions.

B.2.1 Business processes.

B.1.2 Tax.

B.1.1 Compliance with financial policies.

B.1.0 Compliance with other policies.

B.0.9 Reporting controls.

B.0.8 Reporting disclosures.

B.0.7 Fraud and irregularities.

B.0.6 Financial reporting.

B.0.5 Corporate functions.

B.0.4 Operating unit management.

B.0.3 Regional/divisional level.

B.0.2 Business controls.

B.0.1 Design of internal control frameworks are owned by management.

B.0.0 Design of internal control frameworks are owned by management.

Question

<table>
<thead>
<tr>
<th>Question</th>
<th>Disagree</th>
<th>Agree</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Fully</td>
<td>Mostly</td>
</tr>
<tr>
<td>B.4.1 A code of conduct to define expected behaviour of employees is established and available on the company's website.</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>B.4.2 The code of conduct is approved by the management board.</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>B.4.3 The code of conduct is applied to joint ventures, other partnerships and key suppliers.</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>B.4.4 The code of conduct is periodically reviewed/updated.</td>
<td>0</td>
<td>6</td>
</tr>
<tr>
<td>B.4.5 The code of conduct is actively kept alive in the business.</td>
<td>0</td>
<td>6</td>
</tr>
<tr>
<td>B.4.6 The code of conduct is applied to joint ventures, other partnerships and key suppliers.</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

Question

<table>
<thead>
<tr>
<th>Question</th>
<th>Disagree</th>
<th>Agree</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Fully</td>
<td>Mostly</td>
</tr>
<tr>
<td>B.7.1 The IAF acts independently and objectively as ‘third line of defence’.</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>B.7.2 The IAF reports to … *</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>B.7.3 Number of FTE in the IAF *</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>B.7.4 Indicate the scope of work of the IAF … *</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>B.7.5 The IAF is making a strong contribution to oversee overall effectiveness of the company-wide risk management and control systems.</td>
<td>0</td>
<td>6</td>
</tr>
<tr>
<td>B.7.6 The IAF is making a strong contribution to provide assurance on mitigation strategies concerning selected key risks.</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>B.7.7 The IAF is making a strong contribution to oversee overall effectiveness of the company-wide risk management and control systems.</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>B.7.8 The IAF is making a strong contribution to the identification and evaluation of key risks.</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>B.7.9 The IAF is making a strong contribution to continuously evaluate and improve the company-wide risk management.</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>B.7.10 The IAF is making a strong contribution to improve the company-wide risk management and control systems.</td>
<td>0</td>
<td>6</td>
</tr>
<tr>
<td>B.7.11 The IAF is making a strong contribution to the identification and evaluation of key risks.</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>B.7.12 The IAF is making a strong contribution to oversee overall effectiveness of the company-wide risk management and control systems.</td>
<td>5</td>
<td>20</td>
</tr>
<tr>
<td>B.7.13 The IAF acts independently and objectively as ‘third line of defence’.</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>B.7.14 The IAF reports to … *</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>B.7.15 The IAF acts independently and objectively as ‘third line of defence’.</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>B.7.16 The IAF acts independently and objectively as ‘third line of defence’.</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>B.7.17 The IAF acts independently and objectively as ‘third line of defence’.</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>B.7.18 The IAF acts independently and objectively as ‘third line of defence’.</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>B.7.19 The IAF acts independently and objectively as ‘third line of defence’.</td>
<td>3</td>
<td>2</td>
</tr>
</tbody>
</table>
### B.9 Oversight

**B.9.1** Regular meetings/oversight bodies are in place to effectively oversee results from assurance/ compliance/audit activities and effectiveness of management follow-up.

<table>
<thead>
<tr>
<th></th>
<th>Fully</th>
<th>Mostly</th>
<th>Mostly</th>
<th>Fully</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0</td>
<td>2</td>
<td>11</td>
<td>21</td>
</tr>
</tbody>
</table>

**B.9.2** These meetings/oversight bodies are attended by the internal auditor.

<table>
<thead>
<tr>
<th></th>
<th>Fully</th>
<th>Mostly</th>
<th>Mostly</th>
<th>Fully</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0</td>
<td>5</td>
<td>12</td>
<td>17</td>
</tr>
</tbody>
</table>

**B.9.3** These meetings/oversight bodies are cascaded to lower management levels to enable accountability.

<table>
<thead>
<tr>
<th></th>
<th>Fully</th>
<th>Mostly</th>
<th>Mostly</th>
<th>Fully</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>6</td>
<td>16</td>
<td>11</td>
</tr>
</tbody>
</table>

**B.9.4** These meetings/oversight bodies are attended by the CEO and CFO.

<table>
<thead>
<tr>
<th></th>
<th>Fully</th>
<th>Mostly</th>
<th>Mostly</th>
<th>Fully</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>3</td>
<td>0</td>
<td>12</td>
<td>19</td>
</tr>
</tbody>
</table>

**B.9.5** These meetings/oversight bodies are attended by the external auditor.

<table>
<thead>
<tr>
<th></th>
<th>Fully</th>
<th>Mostly</th>
<th>Mostly</th>
<th>Fully</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>5</td>
<td>6</td>
<td>16</td>
<td>7</td>
</tr>
</tbody>
</table>

**B.9.6** The supervisory board/audit committee is effectively overseeing the effectiveness of the company-wide risk management and control systems.

<table>
<thead>
<tr>
<th></th>
<th>Fully</th>
<th>Mostly</th>
<th>Mostly</th>
<th>Fully</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0</td>
<td>2</td>
<td>11</td>
<td>21</td>
</tr>
</tbody>
</table>

**B.9.7** These supervisory board/audit committee meetings are supported by formal charters describing objectives, attendances, agenda.

<table>
<thead>
<tr>
<th></th>
<th>Fully</th>
<th>Mostly</th>
<th>Mostly</th>
<th>Fully</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0</td>
<td>5</td>
<td>12</td>
<td>17</td>
</tr>
</tbody>
</table>

**B.9.8** These supervisory board/audit committee meetings are supported by formal charters describing objectives, attendances, agenda.

<table>
<thead>
<tr>
<th></th>
<th>Fully</th>
<th>Mostly</th>
<th>Mostly</th>
<th>Fully</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>6</td>
<td>16</td>
<td>7</td>
</tr>
</tbody>
</table>

**B.9.9** These supervisory board/audit committee meetings are attended by the internal auditor.

<table>
<thead>
<tr>
<th></th>
<th>Fully</th>
<th>Mostly</th>
<th>Mostly</th>
<th>Fully</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>3</td>
<td>0</td>
<td>12</td>
<td>19</td>
</tr>
</tbody>
</table>

**B.9.10** The external auditor is attending all audit committee meetings (or if not in place the supervisory board).

<table>
<thead>
<tr>
<th></th>
<th>Fully</th>
<th>Mostly</th>
<th>Mostly</th>
<th>Fully</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0</td>
<td>5</td>
<td>16</td>
<td>11</td>
</tr>
</tbody>
</table>

**B.9.11** The external auditor is attending all audit committee meetings (or if not in place the supervisory board).

<table>
<thead>
<tr>
<th></th>
<th>Fully</th>
<th>Mostly</th>
<th>Mostly</th>
<th>Fully</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>5</td>
<td>6</td>
<td>16</td>
<td>7</td>
</tr>
</tbody>
</table>

**B.9.12** These supervisory board/audit committee meetings are attended by the external auditor.

<table>
<thead>
<tr>
<th></th>
<th>Fully</th>
<th>Mostly</th>
<th>Mostly</th>
<th>Fully</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0</td>
<td>2</td>
<td>11</td>
<td>21</td>
</tr>
</tbody>
</table>

### B.8.1 External Audit

**B.8.2** The external auditor is reviewing and reporting on the company-wide risk management and control systems within the boundaries of the regular financial audit assignment.

<table>
<thead>
<tr>
<th></th>
<th>Fully</th>
<th>Mostly</th>
<th>Mostly</th>
<th>Fully</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>7</td>
<td>10</td>
<td>11</td>
<td>6</td>
</tr>
</tbody>
</table>

**B.8.3** The external auditor is assigned to review risk management and control systems beyond the regular financial audit assignment.

<table>
<thead>
<tr>
<th></th>
<th>Fully</th>
<th>Mostly</th>
<th>Mostly</th>
<th>Fully</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>14</td>
<td>9</td>
<td>10</td>
<td>7</td>
</tr>
</tbody>
</table>

### C. Risk Management and Internal Control Disclosure

**Best practice II.1.4** In the annual report the management board shall provide:

a) A description of main risks related to the strategy of the company;

b) A description of the design and effectiveness of the internal risk management and control systems for the main risks during the financial year;

c) A description of any major failings in the internal risk management and control systems which have been discovered in the financial year, any significant changes made to these systems and any major improvements planned, and a confirmation that these issues have been discussed with the audit committee and the supervisory board.

**Best practice II.1.5** As regards financial reporting risks the management board states in the annual report that the internal risk management and control systems provide a reasonable assurance that the financial reporting does not contain any errors of material importance and that the risk management and control systems worked properly in the year under review. The management board shall provide clear substantiation of this.

### B.8.4 Internal Control

**B.8.5** The audit committee is in place to monitor the financial reporting.

<table>
<thead>
<tr>
<th></th>
<th>Fully</th>
<th>Mostly</th>
<th>Mostly</th>
<th>Fully</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0</td>
<td>4</td>
<td>7</td>
<td>23</td>
</tr>
</tbody>
</table>

**B.8.6** The IAF has reported on these.

<table>
<thead>
<tr>
<th></th>
<th>Fully</th>
<th>Mostly</th>
<th>Mostly</th>
<th>Fully</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0</td>
<td>4</td>
<td>7</td>
<td>23</td>
</tr>
</tbody>
</table>
E. Reporting alleged irregularities

Best practice II.1.7

The management board shall ensure that employees have the possibility of reporting alleged irregularities of a general, operational and financial nature within the company to the chairman of the management board or to an official designated by him, without jeopardising their legal position. Alleged irregularities concerning the functioning of management board members shall be reported to the chairman of the supervisory board. The arrangements for whistleblowers shall be posted on the company’s website.

<table>
<thead>
<tr>
<th>Question</th>
<th>Disagree</th>
<th>Agree</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Fully</td>
<td>Mostly</td>
</tr>
<tr>
<td>E.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mostly</td>
<td>Fully</td>
</tr>
<tr>
<td>E.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E.3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E.4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E.5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E.6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E.7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E.8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E.9</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| E.1 | A whistle-blowing procedure is in place to allow employees to report irregularities and wrongdoings | 0 | 0 | 4 | 30 |
| E.2 | Whistle-blowing/fraud cases are investigated independently, timely and effectively | 0 | 0 | 6 | 28 |
| E.3 | VIIF is involved in whistle-blowing and fraud investigations | 1 | 8 | 7 | 18 |
| E.4 | The Director VIIF has an active role in the follow-up of whistle-blowing cases (trusted person) | 7 | 6 | 6 | 15 |
| E.5 | There is a possibility to report potential irregularities and wrongdoings anonymously | 0 | 0 | 3 | 31 |
| E.6 | A formal cross-functional committee (e.g. ethics/integrity committee) is in place to oversee effectiveness of code of conduct and whistle-blowing | 6 | 3 | 9 | 16 |
| E.7 | The Director VIIF is member of the Ethics/Integrity Committee … respectively … yes/no * (not applicable 12) | 15 | 7 |
| E.8 | Results from whistle-blowing/fraud cases are periodically reported to the management board | 0 | 0 | 4 | 30 |
| E.9 | Results from whistle-blowing/fraud cases are periodically reported to the supervisory board/audit committee | 0 | 1 | 4 | 29 |
Annex 3 Reference to other research and guidance

The following list of other research material and guidance reports have been reviewed and referred to in this research:

7. IAARF: Internal Audit Capability Model for the Public Sector (2009)
10. Impact on governance, research on cooperation internal and external auditor - Nivra and IIA (2009)
11. ECIIA - European Governance Magazine (2011)
IIA Netherlands

The Institute of Internal Auditors - Netherlands, is the only professional body in the Netherlands solely dedicated to the profession of internal auditing. We are part of the global Institute of Internal Auditors, which sets the International Professional Practice of Internal Auditing, and the Code of Ethics, which all members agree to follow. The IIA represents, promotes and develops the professional practice of internal auditing. We have more than 170,000 members in 165 countries worldwide, and 2,500 members in the Netherlands.