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

Institute of Internal Auditors
The Netherlands

Colophon

Project team

Michel Kee RA
Hans Nieuwlands RA CIA CGAP CCSA
Daniela Danescu CIA CGAP

Sounding Board

drs. Simone Heidema RA
prof. dr. Leen Paape RA RO CIA
Thijs Smit RA CIA
prof. dr. Philip Wallage RA

Design

APPR bv

Table of contents

Foreword

Dear reader,

It is my pleasure to introduce this report that provides insight in 'in 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
- Financial reporting control frameworks are in place and several companies indicate that they have control frameworks in place that extend beyond financial reporting, for instance to business processes, IT and Tax
- The code of conduct needs to be actively 'kept alive' to preserve a sound ethical culture
- Oversight responsibilities related to risk management and internal controls are generally effectively fulfilled by the management board and the audit committee; however, improvements can be made
- Disclosure of risks is generally discussed with the management board and supervisory board/audit committee

The role of the IAF (chapter 3)

- The IAF is broadly seen as an independent expert on governance, risk management, compliance and control systems. Many companies, therefore, ask the IAF for advice to support management in establishing and implementing risk, control and compliance frameworks. After implementation, the IAF can fulfil its core tasks of independently reviewing progress on and effectiveness of applying the frameworks developed and advising on continuous improvements. The role of the IAF can vary depending on the 'risk maturity' of the company; he strives to bring the organisation to a higher level
- The IAF - as does the external auditor - generally plays a key role in Corporate Governance, both supporting the management board and the audit committee in their oversight accountabilities

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 these 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 oversee 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
   (best practice II.1.3)
C. Disclosing risks and risk management and internal control systems
   (best practice II.1.4)
D. In control statement over financial reporting
   (best practice II.1.5)
E. Reporting alleged irregularities (best practice II.1.7)

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 areas being researched. The research provides clear opportunities for additional - more detailed - research on specific areas. IIA 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.

	AEX (#17)	AMX (#5)	AScX (#2)	Other (#10)
Non-financials (#25)	Ahold Air France KLM Akzo Nobel ASML DSM Heineken KPN PostNL Randstad Shell TNT Express Unilever Wolters Kluwer	AMG ASMI Nutreco USG People Vopak	Grontmij Wessanen	Eneco Friesland-Campina Nuon SHV Tata Steel
Financials (#9)	AEGON Corio Delta Lloyd ING			ABN AMRO AON Eureko Rabobank Robeco

Table 1: Respondents by Amsterdam stock exchange category

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.

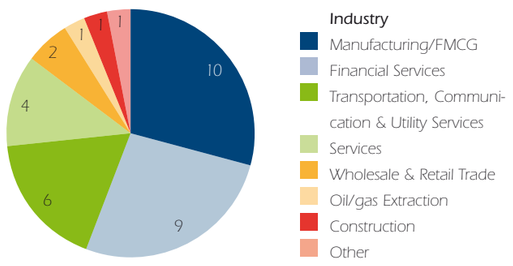


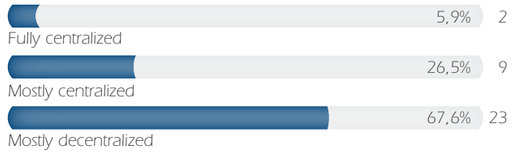
Diagram 1: Respondents by industry

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

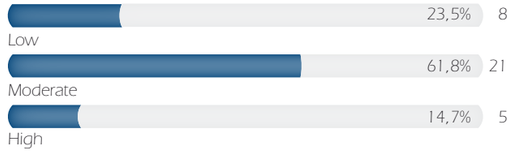
The majority of the respondents (68%) say that their company is mostly decentralised in structure. Of this group, 6 companies indicate that they are moving towards more centralisation, which affects the control environment.



Graph 1: Management philosophy

1.3.5 Company risk profile

As shown in the graph below, 24% of the respondents indicated that their company has a low risk profile, while 15% classify the risk profile as high. Most companies that have a high risk profile mention that this is because of emerging markets and a cyclical industry. The higher the company risk profile, the more demanding the risk management and control systems.



Graph 2: Company risk profile

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.

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)[1]

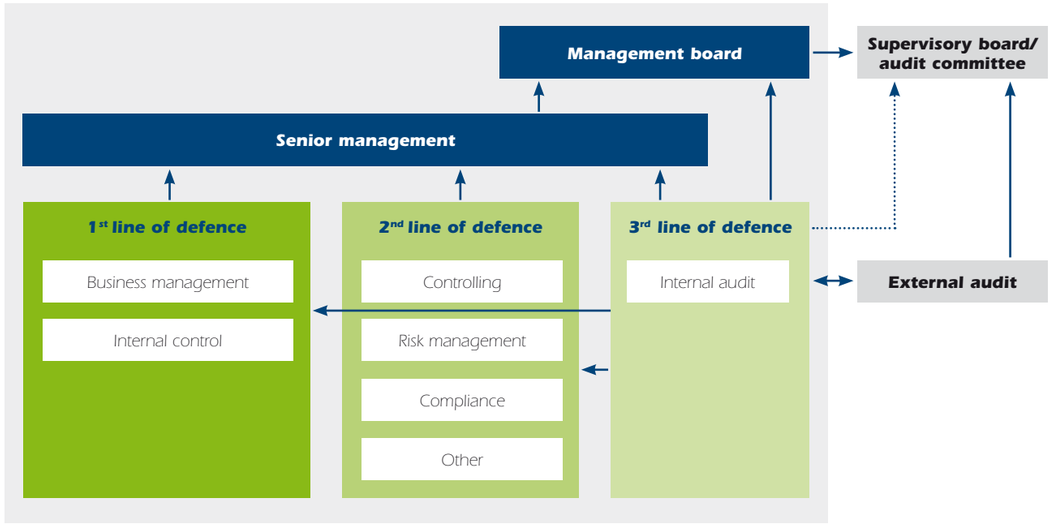
The 'three lines of defence' model - as illustrated in diagram 2 - is a useful tool to explain and demonstrate the different roles in internal governance and the interaction between them.

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 systems at 91% of the participating companies, showing the need for improvement 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 facilitate the implementation of effective risk management practices by business management.

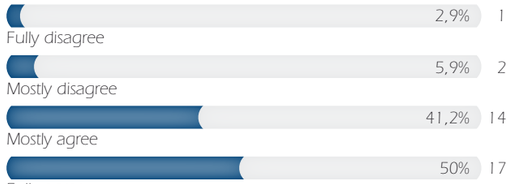
As a 3rd line of defence, the IAF, using a risk-based approach, will provide independent assurance[3] to senior management, executive board and audit committee on the adequacy of the design of the risk management and internal control processes and the effective operation of the 1st and 2nd lines of defence. This assurance task covers all elements of an organisation's risk management, internal control and compliance framework. The IAF acts fully as 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[2]

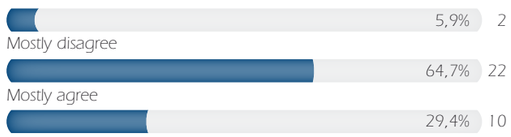


Generally, as illustrated in the graphs below, roles and responsibilities of risk, compliance and assurance functions are clearly defined and formally documented. 50% of the respondents, however, indicate that certain improvements can be made. Cooperation between the various functions can be further optimised at 71% of the participating companies.

"It is not the ship so much as the skillful sailing that assures the prosperous voyage"
George William Curtis



Graph 3: Roles 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

[1] References are made to the sections in the annex providing the detailed quantitative results
[2] Based on Model publiced in European Governance Magazine (October 2011)
[3] Independent assurance is also referred to as re-assurance

All respondents reported that responsibility for the risk management function/ activities of the company lies with (a member of) the management board. The various 2nd line assurance functions mostly report to the chief financial officer (CFO), while the IAF in most cases reports to the chief executive officer (CEO) in order to optimise its independence (see section 3.2.1).

Separate risk, compliance and audit functions are in place at 62% of the participating companies. All of these functions report to a member of the management board. The separation of risk, compliance and audit functions may be driven by legislation and regulations and is fully applied in the financial services sector. We also see a trend towards combining some of the risk, compliance and audit functions under single leadership (reporting to the CEO and functionally to the CFO) in order to limit the number of direct reports to the CEO or the CFO and ensure a more holistic and coordinated approach (see also chapter 3 showing maturity levels of the IAF and the roles the IAF may not or cannot combine/integrate).

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[4].

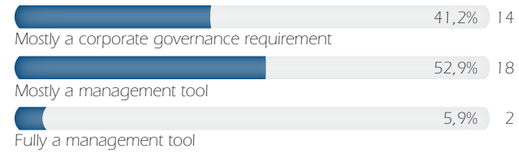
Risk maturity of the organisation can be qualified in 5 categories: (1) Risk naïve, (2) Risk aware, (3) Risk defined, (4) Risk managed and (5) Risk enabled[5].

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[6].

"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 then 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 complexities, 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[7]. 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 'form over substance'. 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[8].

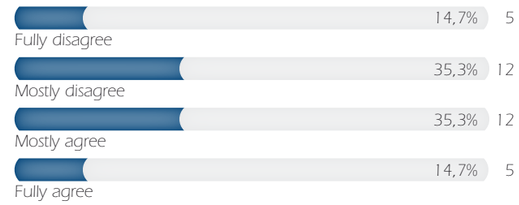


Graph 5: Perception of the risk management process

"If you risk nothing, then you risk everything"
Geena Davis

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 level[9].

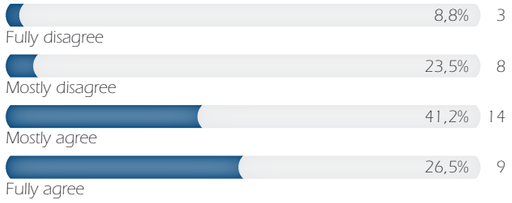
The risk appetite is effectively defined and documented, as indicated by only 50% of the respondents. As a rule the financial services sector has defined (quantified) and documented the company risk appetite; as this is also required by the Banking and Insurance Codes. A non-financial services company 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 6: Risk appetite is clearly defined and documented

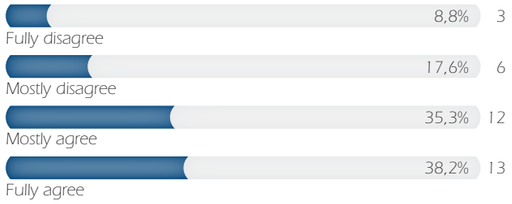
Structured risk assessments are not always effectively performed by regional/divisional management (12% of respondents), corporate functions (15%), management board (21%) and operating unit management (30%). Risk reports are considered structured and concise and are valued by management, as indicated by 79% of the respondents. Risk assessments, however, do not effectively contribute to management decision-making for 32% (23% AEX and 40% other companies) of the respondents (mostly outside the financial services sector) as illustrated below. This is consistent with the 41% of the participating companies perceiving risk management as a corporate governance requirement (see above).

[4] Committee of Sponsoring Organisations: Enterprise Risk Management - Integrated Framework (2004)
[5] Professional Guidance IIA UK & Ireland - An approach to implementing Risk Based Internal Auditing (2005)
[6] IIA Practice Guide - Assessing the adequacy of Risk Management (2010)
[7] Also the Banking Code provides specific provisions to risk management responsibilities and practices (see also note 23)
[8] Second report on compliance with the Dutch Corporate Governance Code (2010)
[9] Professional Guidance IIA UK & Ireland - An approach to implementing Risk Based Internal Auditing (2005)



Graph 7: Risk assessments contribute to management decision making

Research shows that most of the participating companies have established detailed guidelines and templates to ensure consistency in the application of risk management. Such guidance is not in place at 26% of the respondents, mostly non-financial services companies.



Graph 8: The risk management process is supported by detailed guidelines and templates

The effectiveness of risk management is subject to continuous evaluation and improvements, as indicated by 79% of the respondents. Considerable improvement has been achieved in the past 3 years in the company-wide risk management and internal control systems, as reported by 88% of the respondents, while 91% indicate that further improvements are currently in progress or planned.

Internal Control Framework (B3)

As shown in the table below, generally companies have formalised and structured company-wide internal control frameworks in place.

	Fully disagree	Mostly disagree	Mostly agree	Fully agree
Financial reporting	2,9% 1	0% 0	14,7% 5	82,4% 28
Business processes	5,9% 2	14,7% 5	44,1% 15	35,3% 12
IT	2,9% 1	20,6% 7	32,4% 11	44,1% 15
Tax	2,9% 1	14,7% 5	23,5% 8	58,8% 20
Compliance	5,9% 2	14,7% 5	41,2% 14	38,2% 13
Other	11,8% 4	14,7% 5	47,1% 16	26,5% 9

Table 2: A formalised and structured company-wide internal control framework exists

Almost all respondents have a control framework in place regarding financial reporting, supporting the disclosure of the positive 'in control' statement on financial reporting as required by the Code (see 2.3.1). The fact that the Code requires a positive 'in control' statement regarding financial reporting may have led to the wrong perception that controls over business processes, for instance, are considered less important. In areas beyond financial reporting, companies have broadly established formal control frameworks as well. Respondents indicate that a structured control framework is not effectively in place for business processes (21%), IT (24%), tax (18%) and compliance (21%). This could, therefore, mean, for example, that the formalised internal control framework includes controls to ensure that provisions for doubtful debts are properly made, while controls to immediately stop doing business with customers who are not able to pay their bills anymore are not part of the formal framework. Other areas for which formal control frameworks have been established by several of the participating companies include corporate responsibility, integrity and quality management. Several companies have room for improvement with respect to a better balance of the combined set of control frameworks beyond financial reporting. As specialists in control frameworks, internal auditors may play an advisory role in supporting management to establish such frameworks.

"If everything seems under control, you're just not going fast enough"
Mario Andretti

Where internal control frameworks are in place, these are derived from the COSO[10] 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 AEX funds compared to the other companies.

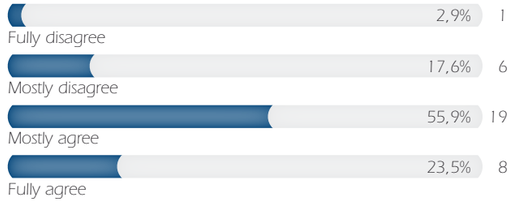
Graph 9: Responsibility for reviewing the effectiveness of the design of internal controls

Graph 10: Responsibility for reviewing operating effectiveness of internal controls

[10]*Committee of Sponsoring Organisations: Internal Control - Integrated Framework*

"To know is to control"
Scott Reed

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.



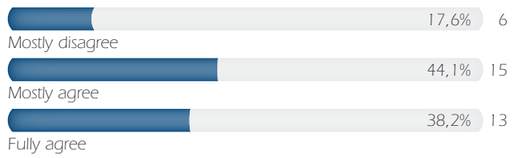
Graph 11: Documented guidelines support reviewing internal control frameworks

Code of conduct (B4)

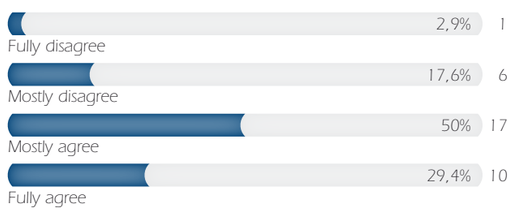
With only a few exceptions, companies have established a code of conduct defining expected behaviour of employees. These codes are approved by the management board and available on the companies' websites. In 5 cases (15%) no structured program is/was in place to implement the code of conduct, including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

"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 training and communication (62%) and to apply it to joint ventures, other partnerships and key suppliers (all outside the financial services sector) in order to maintain a sound business ethical climate (71%).



Graph 12: The Code of Conduct is actively kept alive in the business



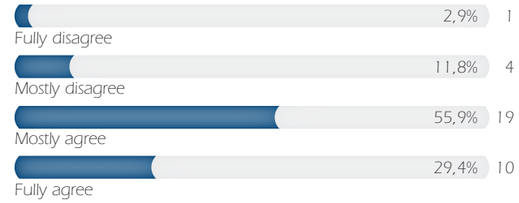
Graph 13: The Code of Conduct is applied to joint ventures, other partnerships and key suppliers

Policies (B5)

Companies have a structured and documented process in place to establish, update, review, approve and communicate policies, as indicated by 82% 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.

"You have to learn the rules of the game. And then you have to play better than anyone else"
Albert Einstein

Graph 14: Company policies are clear, easily assessable and up to date



Graph 15: Compliance with policies is monitored and non-compliance is acted upon

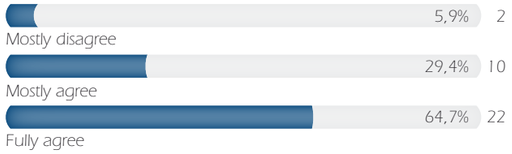
Management representation (B6)

A formal system of letters of representation (LOR) is in place requiring management to show their accountability by signing for statements concerning financial reporting disclosures, financial reporting controls and compliance with financial policies, as reported by 94% of the respondents. Aspects of compliance with the code of conduct, compliance with other policies, business controls and fraud and irregularities are generally part of such a LOR. The LOR supports the external disclosure requirements from the Code.

"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 59% 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.

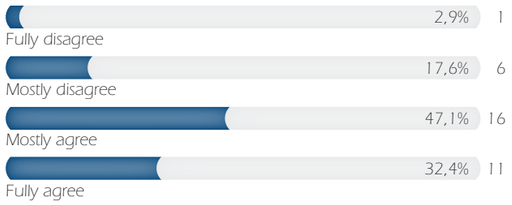
The graph below shows that follow-up and monitoring of reported non-compliance/issues could be improved at 35% of the participating companies.



Graph 16: Reported non-compliance/issues is actively followed-up and monitored

Oversight (B9)[11]

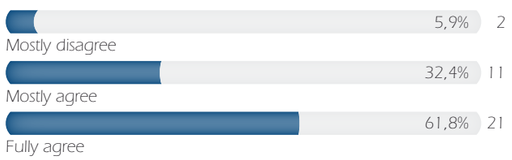
Regular meetings/oversight bodies (in addition to the audit committee) are in place to oversee results from the risk, compliance and audit activities, according to 94% of the respondents. All meetings/bodies are attended by the internal auditor at 91% of the participating companies, while the external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



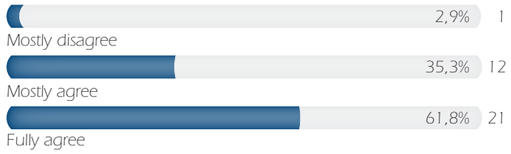
Graph 17: Oversight meetings/bodies are cascaded to lower management to enable accountability

"A good decision is based on knowledge and not on numbers"
Plato

The survey shows that the CEO and CFO are fulfilling their oversight responsibilities effectively at 91% of the participating companies, while the audit committee[12] is effectively overseeing the effectiveness of the company-wide risk management and control systems at 97% of the respondents. As discussed in the roundtable sessions, these scores might be affected by the focus on financial reporting ('in control' statements), and, therefore, too high overall when we consider the entire risk management and internal control scope. The absence of a defined risk appetite in 50% of the cases and the fact that several companies still perceive risk management as a corporate governance requirement also indicate that these scores are somewhat inconsistent and might overall be too high.

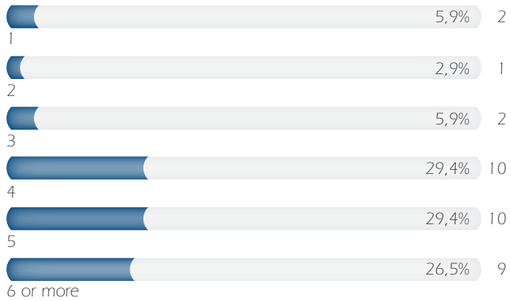


Graph 19: The supervisory board/audit committee is effectively overseeing the effectiveness of the company-wide risk management and control systems



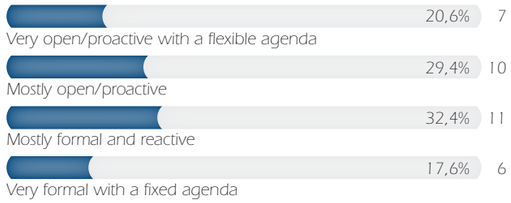
Graph 18: The CEO and CFO are fulfilling their assurance oversight responsibilities effectively

The supervisory board/audit committee is discussing financial reporting and the company-wide risk management systems with varying frequency, as illustrated in the graph below. Audit committees acting in the financial services sector on average meet more frequently compared to the other respondents.



Graph 20: Number of audit committee meetings to discuss financial reporting, risk management and control systems

The tone in the supervisory board/audit committee is very different across the range of participating companies, as indicated below. The roundtable discussions indicate room for improvement on scope of the audit committee agenda, pro activeness of the audit committee members and overall quality of the 'in control' dialogue during the meetings. Further research may be required.



Graph 21: Style of audit committee meetings

2.1.2 Conclusions

- Generally, risk management and internal controls systems have improved over the past few years and further enhancements are planned
- Business management (1st line of defence) is broadly made accountable for ensuring effective risk management and internal control systems and is supported by a variety of 2nd line of defence functions as business control, risk management, compliance etc. Generally there is room for improvement on the cooperation between the 2nd line functions as well as with IAF as 3rd line of defence
- Risk management is widely implemented. In the financial services sector risk management is a core activity and, therefore, seen as a management tool, while the majority of companies outside the financial sector still perceive it as a requirement from the Code. Consistently, one-third of the respondents indicate that risk assessments do not effectively support decision-making. Risk appetite is not clearly defined or documented for 50% of the respondents

[11] Section B7 and B8 are included in chapter 3
[12] In the absence of an audit committee, this is the responsibility of the entire supervisory board

"My heroes are the ones who survived doing it wrong, who made mistakes, but recovered from them"
Bono

- Formal control frameworks also beyond the scope of financial reporting are generally in place. There is room for improvement to expand on frameworks outside financial reporting into, for instance, the area of key business controls required to ensure effective operational processes
- In general, companies comply with the requirement to have a Code of Conduct; generally, however, improvements can be made on keeping it alive, especially outside the financial services sector
- Management representation is in place; follow-up on reported issues can broadly be improved, however
- Oversight responsibilities on risk management and internal controls are generally effectively fulfilled by the management board and the audit committee; there is room, however, for improving scope and quality of the 'in control' dialogue

2.2 Disclosing risks and risk management and internal control systems (C)

2.2.1 Summary of current practice

There is a process in place to review formal risk assessments for the purpose of selecting major risks for disclosure in the annual report at 88% of the participating companies. In 94% of the cases, major risks to be disclosed are being discussed with and approved by the management board and supervisory board/audit committee. This is required by best practice III.1.8.
Companies have a process in place to evaluate and disclose major failings in the internal risk management and control systems, as reported by 85% of the respondents.

"Control of a company does not carry with it the ability to control the price of its stock"
Paul Getty

The function/manager responsible for coordinating the preparation of disclosing main risks and description of the internal risk management and control systems differs across the participating companies. Involvement of the risk management function is mentioned in 47% of the cases and IAF in 32% of the cases, while the controller (15%), finance (15%), CFO (12%), chief risk officer (6%) and legal (6%) are also mentioned[13]. Few companies report on the existence of a cross-functional disclosure committee, which is considered good practice supported by the research.

2.2.2 Conclusions

- Disclosure of risks is generally based on formal risk assessments and is discussed with the management board and supervisory board/audit committee
- A wide variety of people are in charge of coordinating the disclosure of risks and risk management and internal control systems
- Establishing a cross-functional disclosure committee should be considered by the companies

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 IAF (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 (56%).

"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 summarises the activities which are most relevant in supporting the 'in control' statement.

	Fully disagree	Mostly disagree	Mostly agree	Fully agree
Performance analysis/reviews	*0%* *0*	*8,8%* *3*	*32,4%* *11*	*58,8%* *20*
Regular supervision	*0%* *0*	*2,9%* *1*	*38,8%* *13*	*58,8%* *20*
Formal control framework	*0%* *0*	*5,9%* *2*	*20,6%* *6*	*73,5%* *25*
Formal management self-testing	*5,9%* *2*	*17,6%* *6*	*26,5%* *9*	*50%* *17*
Letter of representation	*2,9%* *1*	*5,9%* *2*	*11,8%* *4*	*79,4%* *27*
Audits	*2,9%* *1*	*5,9%* *2*	*14,7%* *5*	*76,5%* *26*
Other	*20%* *7*	*11,4%* *4*	*25,7%* *9*	*42,9%* *15*

Table 3: Activities supporting the 'in control' statement

2.3.2 Conclusions

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.

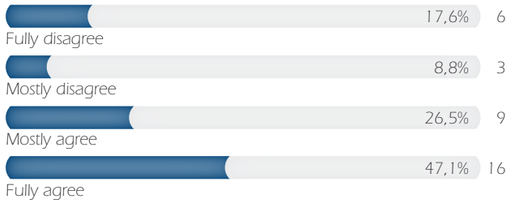
[13] The sum of the percentages adds up to above 100% because several companies mention more than one function/manager

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 auditors may assist management with providing training to the employees. Whistle-blowing/fraud cases are generally investigated independently, in timely fashion and effectively, although 18% of respondents indicate 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 whistle-blowing; 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



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

Results from whistle-blowing/fraud cases are as a rule periodically reported to the management board and supervisory board/audit 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[14]

'Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.' - Definition The Institute of Internal Auditors[15].

Internal audit's 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's 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's 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*	Tasks of directors and line management. Not to be performed by IAF
▪ 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 systems ▪ Assist with implementation of control systems ▪ Facilitate risk control self-assessments ▪ Assist/prepare controls for approval 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 ▪ Decide on whether to implement recommendations from audit reports ▪ Issue 'in control' statements to external stakeholders ▪ Carry responsibility for the quality of quality control systems

Table 4: Roles 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 controls systems. It is good practice to have a written confirmation on the scope of the work, the role and responsibilities of both IAF and management in these types of advisory work. If assurance on a project is needed a reasonable amount of time should be taken into account (e.g. one year) if the same persons would do the audit. As facilitator of risk/control self assessments the auditor should make it very clear that he/she is not part of the discussion, but just acts as a moderator. The auditor is not responsible for the outcome of the assessment. Another option is to outsource certain assurance assignments.*

Size of the IAFs

Respondents from the survey lead small to large IAFs. An overview of the size of IAFs across the 34 participating companies is shown below. All 11 IAFs with a staff up to 10 FTE are from outside the financial services sector, while 5 out of 7 IAFs 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.

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 IAFs 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[16].

"Change before you have to"
Jack Welch

Diagram 3: Internal audit capability model

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 that the IAF mostly has multiple reporting lines; hierarchical reporting line is mostly to the CEO (65%). 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.

[14] Based on 'The Internal Auditor in the Netherlands - Position Paper Update 2008'
[15] IIA International Professional Practices Framework
[16] IIA Research Foundation: Internal Audit Capability Model for the Public Sector (2009)

IAF Reporting to …	#	Hierarchically		Functionally	
CEO	34	22	65%	8	23%
CFO	34	11	32%	14	41%
Audit committee	34	6	18%	27	79%
Others	34	0	0%	5	15%
Total		39		54	

Table 5: IAF reporting lines

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 has undergone.

3.2.2 Scope of work

Overview

As illustrated in the diagram below, the IAF - on average - spend most of its 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.

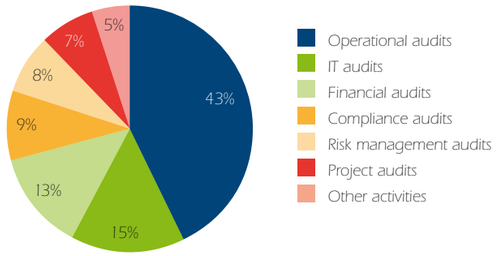


Diagram 3: Scope of work of the IAF

The scope varies across the range of participating companies; few companies have allocated more than 50% of their capacity to risk management audits, while other companies fully rely on external auditors for their financial audits. Broadly speaking, while companies are strengthening the embedding of effective risk management and control systems, the IAF is gradually shifting its focus from compliance, financial reporting and transactional controls to management control, key change projects and effective risk management also on a strategic level.

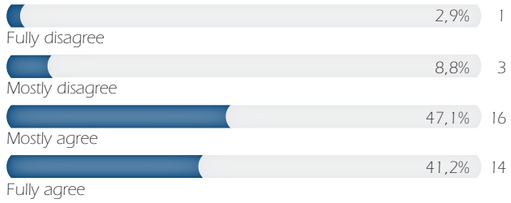
Risk management and internal control systems

The IAF is the catalyst in forming risk management and provides proactive advice on risk management practices, as reported by 77% of the respondents[17]. The IAF contributes to the facilitation of the identification and evaluation of key risks at 62% of the participating companies, as illustrated below.

Graph 24: The IAF facilitates the identification and evaluation of key risks

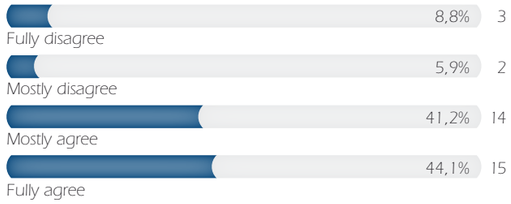
"If you can dream it, you can do it"
Walter Elias (Walt) Disney

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[18].

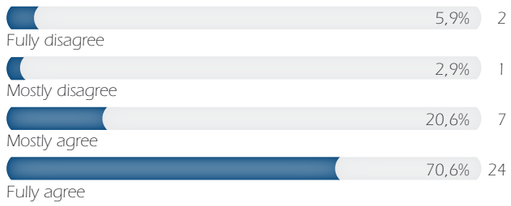


Graph 25: The IAF has effective oversight over the 2nd line assurance functions

Almost all respondents (97%) indicate that the audit plan aligns with company risk assessments aimed at providing assurance on mitigation strategies concerning selected key risks.
The Institute defines Risk Based Internal Auditing as a methodology that links internal auditing to an organisation's overall risk management framework. Risk Based Internal Auditing allows the IAF to provide assurance to the board that risk management processes are managing risks effectively, in relation to the risk appetite[19].
The effectiveness of the company-wide risk management process is regularly being reviewed by 85% of the IAFs. Internal control frameworks are regularly reviewed by 91% of the participating companies.



Graph 26: The IAF regularly reviews the effectiveness of the company-wide risk management process



Graph 27: The IAF independently reviews the design and operating effectiveness of internal control frameworks

Less than 50% of the IAFs report on the fairness of the letter of representation, as illustrated in graph 28. The score is the lowest for companies listed at AEX.

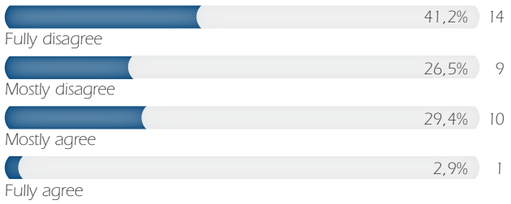
Graph 28: IAF reports on the fairness of the letter of representation

Compliance

Most of the IAFs (74%) are involved in whistle-blowing and fraud investigations, ranging from managing the investigations, requiring specific competencies, to partly contributing. The IAF directors of 21 companies (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.

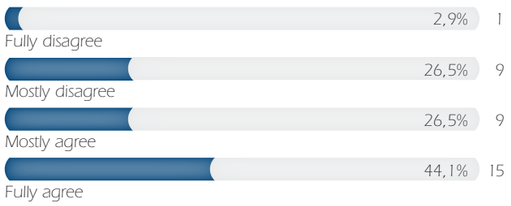
Role of the external auditor

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. At 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.



Graph 29: The external auditor is assigned to review risk management and control systems beyond the regular financial audit assignment

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[20].



Graph 30: External auditor is placing optimal reliance on the work performed by the IAF

3.2.3 Role on 'in control' statements and oversight

Half of the respondents assist in the preparation of the 'in control' statement. This is mostly at companies outside the financial services sector, in which other functions generally perform this task.

Graph 31: IAF assists in the preparation of the 'in control' statement

A special report/opinion to the management board and the supervisory board/audit committee with the objective of supporting the issuance of the annual 'in control' statement is provided by 41% of the respondents. Such a report/opinion is then mostly 'negative' in form (58%) providing 'reasonable' (71%) assurance.
In case major failings in the internal risk management and control systems have been disclosed, the IAF has reported on these failings in 79% of cases.
At 91% of the participating companies the IAF director attends the audit committee meeting[21], while the external auditor attends in 94% of the cases.
'Audit committee members indicated in interviews that the IAF has gained an increasingly important role in recent years. The IAF director is positioned uniquely between the management board and the audit committee. The hierarchical line from the IAF director to the CEO and the direct communication line between the IAF director and the audit committee are considered to be of great importance. The audit committees in general find this of great value'[22].

3.2.4 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 accountabilities
- 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 internal auditor is that he 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 within the boarders of the financial audit assignment
- The role of the IAF in the LOR process and the quality of the disclosure on risks and the system of risk management and internal controls could be further expanded

[17] *Please note the that impact of the IAF presented here is the perception of the responding internal auditor*
[18] *Considered best practice by the IIA and Nivra research report 'Allies in governance - The relationship between the audit committee and the IAF in the Netherlands' (2008)*
[19] *Professional Guidance IIA UK & Ireland - An approach to implementing Risk Based Internal Auditing (2005)*
[20] *Consistent with IIA/Nivra research on cooperation internal and external auditor where 30% reported that the external auditor does not sufficiently rely on the internal audit work (Impact on governance, 2009)*
[21] *Considered best practice by the IIA and Nivra research report 'Allies in governance - The relationship between the audit committee and the IAF in the Netherlands' (2008)*
[22] *From the IIA and Nivra research report 'Allies in governance - The relationship between the audit committee and the IAF in the Netherlands' - providing 9 best practices (2008)*

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. This 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 IAF, based on the results from 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;

b) 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 III.1.8. Concerning the code of conduct (b), the recommendation is to add that, in order to maintain a sound ethical culture, the code needs to be kept actively alive (e.g. continuous awareness training, employee induction programs, oversight and monitoring). Research shows that this is considered best practice.

"Control your own destiny or someone else will"
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 ~~for the main risks~~ 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 thereto. Reference to these discussions shall be made in the report of the supervisory board.

The research shows that risk appetite is not effectively defined and documented by 50% of the respondents (mostly outside the financial services sector), while the notes to best practice II.1.4 require companies to disclose their risk appetite. Adding risk appetite to the discussions with the supervisory board is considered best practice (in the financial sector approval by the supervisory board is even required). Risk mitigation by the 1st and 2nd line of defence is generally considered most effective 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 recommendation is to change the principle and best practice provisions concerning the IAF also inspired by the 'Banking Code 2010'[23] and the Insurance Code.

"The secret to success is to own nothing, but control everything"
Nelson Rockefeller

In the current section V.3 of the Code the principle and best practices on the IAF are described as follows.

'Principle: The internal auditor shall operate under the responsibility of the management board

Best practice provisions

V.3.1 The external auditor and the audit committee shall be involved in drawing up the work schedule of the internal auditor. They shall also take cognizance of the findings of the internal auditor

V.3.2 The internal auditor shall have access to the external auditor and to the chairman of the audit committee.

V.3.3 If there is no IAF, the audit committee shall review annually the need for an internal auditor. Based on this review, the supervisory board shall make a recommendation on this to the management board in line with the proposal of the audit committee, and shall include this recommendation in the report of the supervisory board.

The following revised principle and best practice provisions are recommended.

Principle: The management board shall ensure that an IAF is established

Best practice provisions

V.3.1 Each company shall have its own IAF who shall occupy an independent position within the company. The head of the IAF shall report to the chairman of the management board. The Charter of the IAF needs to be published on the Company website.
In the notes to be added that this is supported by a functional reporting line to the CFO and/or audit committee.

V.3.2 If there is no IAF, the audit committee shall review annually the need for an internal auditor. Based on this review, the supervisory board shall make a recommendation on this to the management board in line with the proposal of the audit committee and shall include this recommendation in the report of the supervisory board. *Current V.3.3*

V.3.3 The internal auditor shall have the task of assessing whether the systems of governance, risk management and internal controls 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.3.4 The internal auditor, management board, external auditor and audit committee shall consult periodically, including as regards the risk analysis, the (conjunction between) internal and external audit plans and the outcome of the audits performed by internal and external auditors. *Current V.3.1 included*

V.3.5 The internal auditor shall have unrestricted access to the chairman of the audit committee. *Current V.3.2 slightly adjusted*

[23] *The Banking Code contains principles that are based on the Dutch Corporate Governance Code of 10 December 2008. The Banking Code focuses in particular on the role of the bank's executive board and supervisory board and on the function of risk management and auditing at banks. The Banking Code also uses the 'comply or explain' principle*

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 as instruments 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

This 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

Question					
A.1	What is the name of your company *	See chapter 1			
A.2	Which type of industry fits best your organisation *				
A.3	Total number of employees at the end of 2010 *				
A.4	Gross sales level (Annual Report 2010 in Euros) *				
A.5	Number of countries the company operates in … *				
A.6	Management philosophy … *respectively … fully centralised, mostly centralised, mostly decentralised, fully decentralised **	2	9	23	0
A.7	What is the overall company risk profile … *respectively, low, moderate high, very high **	8	21	5	0

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 as instruments 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

Question		Disagree		Agree	
		Fully	Mostly	Mostly	Fully
B.1	Organisation and accountability				
B.1.1	Business management is accountable to ensure effective risk management and control systems are in place	2	1	5	26
B.1.2	Which assurance/compliance functions are in place supporting the risk management and control systems *	Open-end question			
B.1.3	Roles and responsibilities of these assurance/compliance functions are clearly defined and formally documented	1	2	14	17
B.1.4	The coordination of activities of these assurance/compliance functions is optimised ensuring no overlaps and gaps on approach	0	2	22	10
B.1.5	The IAF has an effective oversight over the (second-line) assurance functions	1	3	16	14
B.1.6	Which member of the management board is responsible for the risk management function/activities of the company *	Open-end question			
B.2	Risk management				
B.2.1	The company has defined and documented its risk appetite in an understandable, useable and consistent manner, resulting in quantitative output	5	12	12	5
B.2.2	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	2	5	18	9
B.2.3	The risk management process is supported by detailed guidelines (definitions, criteria, steps) and templates	3	8	12	13
B.2.4	The risk management process is embedded in the regular management cycle	2	4	12	16

Question		Disagree		Agree	
		Fully	Mostly	Mostly	Fully
B.2.5	Structured risk assessments are performed on the level of …				
	Management board	2	5	12	15
	Corporate functions	2	3	16	13
	Regional/divisional management	2	2	17	13
	Operating units management	4	5	13	12
B.2.6	The risk management process is perceived to be … *respectively … fully/mostly corporate governance requirement, fully/mostly management tool **	0	14	18	2
B.2.7	Risk reports are considered structured, concise and valued by management	2	5	23	4
B.2.8	Risk assessments contribute to management decision making	3	8	14	9
B.2.9	The effectiveness of the risk management process is evaluated and continuous improvement is fostered	2	5	17	10
B.2.10	IAF is the catalyst in forming risk management and provides pro active advice on risk management practices	2	6	14	12
B.2.11	The IAF facilitates the identification and evaluation of key risks	5	8	11	10
B.2.12	The IAF aligns its audit plan to company risk assessments and provides assurance on mitigation strategies concerning selected key risks	2	1	18	13
B.2.13	The IAF regularly reviews the effectiveness of the company-wide risk management process	3	2	14	15
B.3	Internal Control Framework				
B.3.1	The company has a formalised and structured company-wide internal control framework in place for …				
	Financial reporting	1	0	5	28
	Business processes	2	5	15	12
	IT	1	7	11	15
	Tax	1	5	8	20
	Compliance	2	5	14	13
	Other	4	5	16	9
B.3.2	These internal control frameworks are based on or derived from COSO	1	2	13	18
B.3.3	Design of internal control frameworks are periodically reviewed and updated/documented	0	3	11	20
B.3.4	Internal control frameworks are owned by management	0	2	21	11
B.3.5	Internal control (update) design effectiveness review is performed by … *respectively … management only, generally by management with support from specialists, generally by specialists with support from management, specialist only **	2	12	14	6
B.3.6	Operating effectiveness of internal control frameworks are periodically reviewed and continuous improvement is fostered	0	4	17	13
B.3.7	Internal control operating effectiveness review is performed by … *respectively … management only, generally by management with support from specialists, generally by specialists with support from management, specialist only **	1	12	15	6
B.3.8	Documented guidelines are in place to support reviewing internal control frameworks (templates, timing, sample sizes, definition of significant/material deficiency, reporting results, resolution, disclosure)	1	6	19	8
B.3.9	The IAF independently reviews the design and operating effectiveness of internal control frameworks as part of its audit plan	2	1	7	24
B.4	Code of Conduct				
B.4.1	A code of conduct to define expected behaviour of employees is established and available on the company's website	1	1	4	28
B.4.2	The code of conduct is approved by the management board	1	1	0	32
B.4.2	The code of conduct includes …*	Open-end question			

Question		Disagree		Agree	
		Fully	Mostly	Mostly	Fully
B.4.3	A structured program is/was in place to implement the code of conduct including awareness sessions, training, defined roles & responsibilities	0	5	8	21
B.4.4	The code of conduct is periodically reviewed/updated	0	3	7	24
B.4.5	The code of conduct is actively kept alive in the business	0	6	15	13
B.4.6	The code of conduct is applied to joint ventures, other partnerships and key suppliers	1	6	17	10
B.5	Policies				
B.5.1	The company has a structured/documented process in place to establish, update, review, approve and communicate policies	0	6	11	17
B.5.2	Policies are formally approved and communicated by the management board	0	2	12	20
B.5.3	Company policies are clear, easily assessable and up to date	0	4	24	6
B.5.4	Activities are in place to effectively monitor compliance with policies and non-compliance is acted upon	1	4	19	10
B.6	Management representation				
B.6.1	A formal system of letters of management representation is in place requiring management to sign for certain statements/representations	0	2	8	24
B.6.2	The letter of representation is requested from …				
	Operating unit management	1	2	3	28
	Regional/divisional level	2	2	3	27
	Corporate functions	3	5	6	20
B.6.3	The letter of representation covers …				
	Financial reporting disclosures	1	2	1	30
	Financial reporting controls	1	2	2	29
	Compliance with financial policies	1	2	1	30
	Compliance with code of conduct	1	5	5	23
	Compliance with other policies	0	5	9	20
	Business controls	0	6	10	18
	Fraud and irregularities	1	3	4	26
B.6.4	The letter of representation … *respectively … is fully standard in text, standard text with a limited number of specific disclosures, mainly specific disclosures with a small amount of standard text, only specific disclosures **	5	20	6	3
B.6.5	The results from (internal) audits are taken into account when drafting the letter of representation	4	3	14	13
B.6.6	Letters of representation are required …(quarterly, bi-annually, annually, n/a)	9	10	14	1
B.6.7	Reported non-compliance/issues is actively followed-up and monitored	0	2	10	22
B.6.8	IAF reports on fairness of letters of representation	10	9	8	7
B.7	Internal Audit Function				
B.7.1	The IAF acts independently and objectively as 'third line of defence'	2	0	5	27
B.7.2	The IAF reports to … *	See chapter 3			
B.7.3	Number of FTE in the IAF … *				
B.7.4	Indicate the scope of work of the IAF … *				
B.7.5	The IAF is making a strong contribution to oversee overall effectiveness of the company-wide risk management and control systems	2	1	6	25
B.7.6	The IAF is making a strong contribution to continuously evaluate and improve the company-wide risk management and control systems	2	2	9	21
B.7.7	The IAF is equally positioned/involved/aligned/rewarded compared to other direct reports of Management Board	3	2	12	17

Question		Disagree		Agree	
		Fully	Mostly	Mostly	Fully
B.8	External Audit				
B.8.1	The external auditor is reviewing and reporting on the company-wide risk management and control systems within the boarders of the regular financial audit assignment	0	2	13	19
B.8.2	For this, the external auditor is placing optimal reliance on the work performed by the IAF	1	9	9	15
B.8.3	The external auditor is assigned to review risk management and control systems beyond the regular financial audit assignment	14	9	10	1
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	0	2	11	21
B.9.2	These meetings/bodies are supported by formal charters describing objectives, attendances, agenda	0	5	12	17
B.9.3	These meetings/bodies are cascaded to lower management levels to enable accountability	1	6	16	11
B.9.4	These meetings/bodies are attended by the internal auditor	3	0	12	19
B.9.5	These meetings/bodies are attended by the external auditor	5	6	16	7
B.9.6	The CEO and CFO are fulfilling their assurance oversight responsibilities effectively supported by structured reporting and meetings	0	2	11	21
B.9.7	The supervisory board/audit committee is effectively overseeing the effectiveness of the company-wide risk management and control systems	0	1	12	21
B.9.8	How many times per year does the supervisory board/audit committee meet to discuss financial reporting and the company-wide risk management and control systems *	See chapter 2.1.1			
B.9.9	The internal auditor is attending all audit committee meetings (or if not in place the supervisory board on this agenda)	1	2	3	28
B.9.10	The external auditor is attending all audit committee meetings (or if not in place the supervisory board on this agenda)	0	2	7	25
B.9.11	These supervisory board/audit committee meetings are mostly … *respectively … very open/pro active with a flexible agenda, mostly open/proactive, mostly formal and reactive, very formal with a fixed agenda **	7	10	11	6
B.10	Continuous improvement				
B.10.1	Over the past 3 years strong improvements have been achieved in the company-wide risk management and internal control systems	0	4	12	18
B.10.2	Improvements on the company-wide risk management and internal control systems are currently progress or planned	1	2	10	21

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; 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.

Question		Disagree		Agree	
		Fully	Mostly	Mostly	Fully
C.1	There is a process in place to review formal risk assessments for the purpose of selecting main risks for disclosure in the annual report	0	4	7	23
C.2	Main risks to be disclosed in the annual report are being discussed with and approved by the management board and supervisory board/audit committee	0	2	5	27
C.3	Which function/manager is responsible to coordinate preparation of disclosing main risks *	Open-end question			
C.4	Which function/manager is responsible to coordinate preparation of the description of the design and effectiveness of the internal risk management and control systems *	Open-end question			
C.5	There is a process in place to evaluate and disclose major failings in the internal risk management and control systems	0	5	10	19
C.6	In case major failings in the internal risk management and control systems have been disclosed, the IAF has reported on these (not applicable 10)	3	2	9	10

D. In-control statement on financial reporting

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.

Question		Disagree		Agree	
		Fully	Mostly	Mostly	Fully
D.1	Which function/manager is responsible to coordinate preparation of the in-control statement on financial reporting *	Open-end question			
D.2	Clear framework and guidelines are in place to evaluate the effectiveness of internal controls on financial reporting	1	2	8	23
D.3	The following activities support the in-control statement …				
	Performance analysis/reviews	0	3	11	20
	Regular supervision	0	1	13	20
	Formal control framework	0	2	7	25
	Formal management self-testing	2	6	9	17
	Letter of representation	1	2	4	27
	Audits	1	2	5	26
	Other/mention	7	4	9	14
D.4	The IAF assists in the preparation of the in-control statement	9	8	7	10
D.5	The in-control statement goes beyond financial reporting	9	6	6	13
D.6	The IAF is issuing a special report/opinion to management board and supervisory board/audit committee with the objective to support the issuance of the annual Company's in-control statement … *respectively … yes/no **	14		20	
D.7	Such internal audit report/opinion provides <type> of assurance … *respectively … positive, negative * (not applicable 22)*	5		7	
D.8	Such internal audit report/opinion provides <level> of assurance … *respectively … reasonable, limited* (not applicable 20)*	10		4	

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.

Question		Disagree		Agree	
		Fully	Mostly	Mostly	Fully
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	IAF is involved in whistle-blowing and fraud investigations	1	8	7	18
E.4	The Director IAF 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 IAF 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:

1. Second report on compliance with the Dutch Corporate Governance Code (2010)
2. Committee of Sponsoring Organisations: Internal Control - Integrated Framework (1992)
3. Committee of Sponsoring Organisations: Enterprise Risk Management - Integrated Framework (2004)
4. IIA Practice Guide - Assessing the adequacy of Risk Management (2010)
5. The Internal Auditor in the Netherlands - Position Paper Update (2008)
6. IIA International Professional Practices Framework (2011)
7. IIARF: Internal Audit Capability Model for the Public Sector (2009)
8. Allies in governance - The relationship between the audit committee and the IAF in the Netherlands' (2008)
9. Professional Guidance IIA UK & Ireland - An approach to implementing Risk Based Internal Auditing (2005)
10. Impact on governance, research on cooperation internal and external auditor - Nivra and IIA (2009)
11. ECIIA - European Governance Magazine (2011)
12. Banking Code, Dutch Banking Association (2010)

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 practivce of internal auditing. We have more than 170.000 members in 165 countries worldwide, and 2.500 members in the Netherlands.

Institute of Internal Auditors
The Netherlands

IIA Netherlands
I www.iia.nl
E iia@iia.nl
T +31 880 037 100