THE GOVERNANCE CHALLENGE

A FIRST EXPLORATION FOR INTERNAL AUDITORS

Institute of Internal Auditors

The Netherlands
Preface

Governance is a hot topic. It is the basis of how an organisation is structured, how it operates and how it is managed. So it is essential for internal auditors to understand it, analyse it and assess it. And many of us have to provide an opinion on it. But strangely enough, not many detailed publications are yet available to assist the internal auditor in his or her assessment. This document aims at filling in some of these gaps: it provides a clear overview of all related definitions of the term, it brings a clear framework that could act as a starting point for the analysis, and it formulates a lot of questions that need to be asked when assessing governance. We also include some good practices, identified by the authors of this report. I would like to thank the members of the project group as well as the internal auditors that assisted the project group by reading draft versions and providing their suggestions and real live examples (Korstiaan Kegel, Harrie de Poot, Paul Voets, René van Wijk, Frans Wolf, Arjan Spruit, Peter Baudewijns, Marco Brinkman, Tracey Stanley and Tim Keohane).

Whilst this report is intended for internal audit practitioners, we would encourage further circulation to other key stakeholders in governance (such as risk managers, controllers, corporate secretaries and also students), as we also expect that they will find this document a worthwhile read.

Michel Kee
President of The Institute of Internal Auditors, The Netherlands
1. Introduction

This paper is about governance. Governance is a widely used concept, and we have found as many definitions and opinions as people that talk about it. Internal auditors often have to report on it, and sometimes have to give their view on it. This paper is meant to help.

Every organisation, whether private or public, needs guidance for its organisational behaviour, not only to help ensure that the actions of its staff are aligned to its strategic objectives, but also that they are compliant with all relevant regulatory requirements. This guidance is strongly manifested by rules: from general principles, via policies, towards detailed instructions (procedures) in business and administrative processes.

At a process level, rules are generally well documented. Monitoring and controlling of their observance is fully accepted. However, for rules (or controls) which exceed process levels (such as those related to governance), documentation, monitoring and controlling is often less formalised. Quite often, rules are not even documented at all. These unwritten rules (referred to by fashionable terms like “Culture” or “Tone at the top”) are equally important.

Most organisations have usually laid down their rules formally in documents like:
- Statements regarding the mission or vision of the organisation and the related objectives and strategy;
- Different codes (e.g. Code of Conduct, Code of Ethics);
- Policies for the corporate functions, defining their roles, functions, responsibilities and their authority over the operating companies (hereafter referred to as Opcos);
- Management contracts with the Opcos defining their objectives and authorizations (ranging from “tight” to “loose” control or “central” to “decentralised”).

Some organisations have combined all these statements, principles and policies into a consistent and coherent framework, thus outlining “the governance of the company”. This framework can be materialized in different ways. Because it is presenting “the state of the art of a company’s governance” at a certain moment, it is a living and continuously evolving framework. This framework is a forceful tool to support the overall governance of a company.

Not only driven by its charter, but also by stakeholders’ expectations, Internal Audit increasingly has to deal with this governance framework. Top management more and more asks for Internal Audit’s opinion on the governance of the organisation. And as a consequence, it is or may become an area of focus for the audit plan in order to ensure compliance with it.

The IIA definition of Internal Audit mentions governance processes explicitly, but also the Dutch banking and insurance codes require the Internal Audit function to report on the governance and internal control of its organisation. Some guidance is already available for internal auditors, and several professional bodies and other institutions, such as external consultancy firms are adding guidance. However, for the day-to-day audit activities the internal auditor could need some practical guidance and this paper aims to do so.

We have used the IIA definition for governance as a starting point. In the second chapter, “Governance”, we take a closer look at this definition. In the third chapter, “Building blocks of governance”, we unravel the definition, leading to major building blocks. These blocks materialise the actual content of governance and together these blocks should form a consistent and manageable governance framework. In the fourth chapter the question “How to formalise governance?” is being addressed. In the chapter “How to audit governance?” we provide practical guidance, using the insights of the earlier chapters. Additional information, either received during interviews or via other means, is presented in the sixth and last chapter, “Good practices”.
2. What is governance?

We need a definition of the term "governance" for the purpose of this paper. In the following chapters we want to define the (minimum) elements of governance, how to formalise it, and what the involvement of the Internal Audit function should be. Therefore, this chapter will lead us to a definition that we can use for this purpose.

2.1 Governance

There are multiple definitions for governance, corporate governance, organisational governance and other terms that are closely related to the governance of the organisation. In the appendix, some examples are given of definitions that are used in national corporate governance codes or that are used by authoritative organisations around the world. We can fairly conclude that there is no single, globally accepted definition of governance. However, when looking at the wide myriad of definitions, a certain "common denominator" can be found: governance is all about directing and managing the company, its policies, structures, processes and procedures to realize the objectives of the company and its main stakeholders.

Since this document is at least intended to assist internal auditors, we will use the IIA definition of governance. In the International Standards for the Professional Practice of Internal Auditing and Practice Advisories PA 2110-1, governance is defined as "The combination of processes and structures implemented by the board to inform, direct, manage, and monitor the activities of the organisation toward the achievement of its objectives."

Given our research on the topic, we would like to make two remarks. We emphasise the importance of culture and behaviour on governance, including the company's ethical standards. We will include these in this document when considering governance. Also, given the fact that the definition implies a one tier board and in many countries two tier boards exist, governance is in our opinion not limited to directing and controlling by the managing board, but also includes the supervision role of e.g. a supervisory board.

2.2 Formalisation of governance

In our view each company should formalise its governance to some extent, as governance plays an important role in how the organisation is directed, monitored, managed and informed. This formalised governance can be in different forms, such as interactive portals on internet sites or tangible documents. But irrespective of its form, it must reflect how a specific company is governed, including its structure, processes, policies, authorities and so on. The formalised governance framework can be used by employees and certain groups of stakeholders to learn and to get an understanding of how the specific company is governed. It provides clarity on roles and responsibilities, assists management and support functions with the execution of their tasks and supports auditors by assessing the governance of the company.

However, it should be noted that governance is not static. As the organisation is constantly changing, also the formalised governance of an organisation needs to be regularly adapted and updated, to ensure the company remains agile and resilient in the pursuit of its objectives. And last but not least, culture and behaviour are of course key elements of an effective governance.
3. The building blocks of governance

3.1 The building blocks

This chapter aims to provide practical guidance on how to unravel the complex field of governance. It will list and structure the building blocks of governance, in order to provide management and staff with a starting point to design and implement it, and internal auditors to assess it, as required in IPPF standard 2110.

Based on the definition stated in chapter 2, the building blocks of governance are:

- **The organisation’s objectives**, which provide direction to the organisation, based on its vision and strategy;
- **Ethical standards**, which give moral guidance to all individuals within the organisation;
- **Policies, governance processes and structures**, which describe the formal environment and acknowledge the informal environment of the organisation;
- **Stakeholder expectations**, which provide boundaries and guidance for the organisation;
- **Culture and behaviour**, which are more informal controls for the governance of the organisation; the society in which the organisation is active and the behaviours of the staff and other stakeholders within and outside the organisation who are strong influencers of the governance.

Figure: Building blocks of governance in an organisation

The design of each building block should be tailored to the characteristics and needs of each individual organisation. Every type of organisation has its own characteristics, and even similar organisations are rarely identical, since they all make their own (strategic) choices and objectives and define their own ways in how to reach them. We will in this document not provide definitions of the many elements that could be seen as part of the governance. But we will discuss for each building block the important design principles that organisations have - more or less implicitly - used to create their governance structure. These design principles strongly influence the way governance is structured and an analysis of them is an elementary part of any sound assessment of the governance framework. The design principles are:

- The location of management control and responsibility [centralised versus decentralised];
- The organising principle [formal versus informal];
- The level of defined detail [rules-based versus principles-based].
A reflection of these design principles will be given at the end of each section, and thus could act as a starting point for the analysis of the building blocks in any organisation.

### 3.2 Organisation’s objectives

The most important building block of the organisational governance consists of the objectives of the organisation. These are derived from the mission and the business strategy that management has formulated. Key questions to ask for a good understanding of the objectives are:

- What is the organisation’s mission?
- What vision does management have on the environment and market in which the organisation is operating or should be operating?
- What are the long term and short term objectives of the organisation?
- What process was implemented to develop this strategy and these objectives?
- How are the strategy and objectives communicated within the organisation?
- When do these have to be formulated and what ‘update process’ is in place?
- How does the monitoring process (feedback loop) work and what is reported on the realisation of the objectives?
- How do the objectives cascade down into the organisation? How much freedom do decentralized parts and business units of the organisation have to deviate from the organisation’s objectives? Is this clearly understood by all?
- What guidelines (or design principles) are given to the organisation for the other governance building blocks?

The objectives are the anchor point for all actions that are taken by the organisation. If the organisation undertakes actions that are not linked to the realisation of its objectives, the organisation should consider eliminating these actions or reconsider its objectives.

**Design principles**

We would expect the organisation’s objectives to be formulated centrally by the board. Also the degree of freedom decentralized entities have to formulate additional objectives or to deviate from them will be set centrally. When objectives are formulated clearly and measurably, one could say these are more formalised and rules-based. The objectives could also be formulated at a higher level, creating more room for interpretation and thus they follow more the ‘principles-based’ approach.

If decentralized entities have the liberty of setting their own objectives, it is important to understand whether this is the result of an explicit choice, or the result of employees being able to freely interpret an informal design of the organisation’s governance structure. When understanding the use of these design principles in this building block, it will be possible to make – as internal auditors - explicit choices on what to include to which extent in the assessment.

### 3.3 Ethical standards

An organisation is a social group which distributes tasks for a collective goal. Ethical standards are the moral compass of the individuals which form part of that group. These standards formulate the values of the organisation, guide the employees in their behaviour and help them in making decisions. By expressing ethical standards formally in a Code of Ethics, the organisation makes them clear, both internally and externally. Normative standards such as ethical standards are also part of the (formalised) culture of the organisation. Key questions in order to properly understand the ethical standards are:

- Where are the ethical standards derived from?
- What is the relation between the organisation’s Code of Ethics and other Codes, e.g. industry associations or professional bodies?

---

1 Wikipedia
- How are they communicated and implemented?
- Are these standards ‘enforced’, and if so, how?
- How does the organisation report on compliance with these standards?
- Is the Code of Ethics clarified, e.g. by conduct examples or instructions?
- Are the ethical standards sufficiently normative for the other governance building blocks?

**Design principles**

Ethical standards by their nature are more suited to a principles-based approach. It is possible to be confronted with situations or behaviours not formally covered by a rule, although not desirable. But to cover every undesired situation or behaviour with rules would usually be ineffective and is described in literature as the risk-rule reflex dilemma. Multinational companies often face issues like ethical principles that are not equal among different cultures. This would suggest that decentralised freedom should be provided to create region specific ethical standards. However companies will usually strive to have corporate ethical standards that cover all countries in which the company is active. These reflections are even more true for conduct principles. Given the intangible element of ethics and conduct, a formal approach would assist in having these standards at least clearly formulated and communicated. On the other hand, this should not replace the principle based character of the topic.

### 3.4 Policies, processes and structures

Key policies in operation across an organisation and the organisational main structure are usually quite easy to find. However, the governance processes are often more difficult to find. Key questions that should be addressed to understand this building block are:

- What are the policies, governance processes and structures within the organisation?
- How do the policies, governance processes and structures relate to the organisation’s objectives and the ethical standards?
- Who (at board and at executive level) is accountable for the key risks, key policies and governance processes?
- Is it clear how key parties within the governance structure (e.g. boards, management, risk and compliance functions, financial/business control functions, internal audit) interact?
- Do the policies, governance processes and structures support the other governance building blocks?
- Are the processes sufficiently set out in clear procedures that target audiences will understand and are able to use?
- Is performance management sufficiently embedded in the governance?
- Are the design principles, as described in the Organisation’s objectives section, sufficiently operationalised into allocation of responsibilities to the various entities?
- Is it clear what level of freedom exists for the decentralized entities and divisions?

The list below outlines the policies that can usually be found in organisations:

- Charters of the boards, the board’s committees and key departments within the organisation’s governance structure, like Risk Management, Compliance, Legal and Internal Audit. A charter usually addresses the scope, objectives, roles, responsibilities, main stakeholders, and authority of the function.
- The allocation of the power of attorney
- Compliance policies
- Financial reporting policy
- Treasury policy
- Information and communication technology policy
- Quality standards
- External communications policy
- Procurement policy
- Recruitment policy
- Investment policy
- Credit policy
• Outsourcing and contracting policy
• Human resources policy
• Remuneration policy
• Risk management policies (financial – non financial)
• Corporate social responsibility policy
• Employee participation policy

Next to a set of policies, a number of governance processes will be found in organisations. Related procedures and/or work instructions that give clear guidance on how to act should be attached. Important governance processes are:

• Business planning process
• Planning and control cycle
• In control statement process
• Financial reporting process
• CSR (Corporate Social Responsibility) reporting processes
• Process for reporting to supervisory authorities
• Incentive processes
• Risk management processes

‘Structure follows strategy’ is a well known saying. The question how an organisation ought to be structured and which models are available, is a broad topic. Set out below is an overview of some of the options that could be employed:

• Organisational structure:
  - Divisional structure
  - Matrix structure
  - Regional structure
  - Functional structure
• Legal:
  - Legal structure
  - Tax structure
• Monitoring structure:
  - Board and other governance related committee composition
  - Allocation of accountabilities and responsibilities
  - Committees, like Audit Committee, Remuneration Committee, Risk Committee, Integrity Committee, Ethics Committee, Disclosure Committee
  - Three lines of defence principle
• Business model:
  - Joint ventures and major participations
  - Partnerships and outsourcing
  - Operating structure
  - Geographical structure
• Management structure:
  - Communication structure
  - Business unit and corporate function level structure

**Design principles**

Policies, governance processes and structures, when described, are formal by definition. However, it is important to recognise that informal ‘habits’, processes and structures always exist in an organisation and they are by their nature not formalised. It is recommended that the agreed levels of freedom at decentralised entities and principle based policies are sufficiently documented and that the guiding principles of behaviour are communicated to those involved.

A description of best practices may help in finding the balance between explicitly desired informal processes and structures and too flexible interpretations. An ‘informal policy’ is probably a contradiction in terms, but habits or ‘common practices’ do exist and these can be
very strong. Multinational organisations always face the challenge of various jurisdictions. It is clear that local law and regulations should prevail over company policy and regulations. And again, a balance has to be found between (1) providing strict central and/or rules-based guidance from which local entities only can deviate in case of a legal conflict, and (2) providing guidance at high level only and allowing local decentralised entities to have the liberty to create their own local policies. The first approach will create maximum standardisation, but more work at head office; the second will work better in a more empowered environment. Some regions prefer in general principles-based policies, while others prefer more rules-based policies. In particular, companies that operate in multi-national environments face challenges in this area, where advocates of both approaches claim superiority over the other. It is important to take this into account when designing and assessing governance.

3.5 Stakeholder expectations

Organisations operate in a landscape containing multiple stakeholders with nearby or more remote interest. Stakeholders are often seen as external, but the border between internal and external is not always clear. First of all, the organisation should know all its stakeholders and should assess their current and future relevance. Key questions for better understanding this building block are:

- Who are the stakeholders and what is their relevance?
- What are their expectations?
- When and how is stakeholder analysis undertaken?
- Who communicates about what with the stakeholders and with what frequency?
- Who is responsible for managing each stakeholder’s expectations?
- Who is allowed to represent the company externally, and in which areas and to what extent?
- What governance-related information is revealed to the internal and external stakeholders?
- Is information proactively sent to the stakeholders or do we respond to specific stakeholder requests for information?
- Are the other building blocks of governance used by stakeholder management, e.g. by setting boundaries?

An overview of possible stakeholders includes:

- Employees
- Works councils
- Shareholders
- Suppliers
- Customers
- Business partners
- External auditor
- Regulatory authorities
- Unions
- Branch organisations
- Customer organisations
- Pressure groups
- Rating agencies
- Standard setting organisations
- Social circle of employees
- Competitors
- Local communities
- General public
- Politicians
- Government
Design principles

Managing the stakeholders should be a mixture between a formal and informal approach, for example where the identification of stakeholders is formal, but treatment in various cases more informal. Since stakeholders operate at different levels, a certain degree of responsibility devolved to decentralised parts of the organisation will be effective. Some stakeholders need to be treated at a company level, others can better be treated from decentralized units. A clear challenge, especially for multinational organisations, is the difference between rules-based and principles-based cultures. Explicit stakeholder management of course will not solve this, but will certainly help.

3.6 Impact of culture and behaviour

Culture and behaviour are crucial to the governance strategy of an organisation. This includes both culture of the organisation itself and the culture in which the organisation operates, as well as the behaviour of the people that work in the organisation and external stakeholders. Culture and behaviour are enablers and restrictors – they stimulate empowerment and formulate boundaries. Culture and behaviour can be influenced by management, and therefore are powerful instruments that could make or break the effective governance of an organisation.

In order to analyse culture and behaviour in more detail, it is relevant to distinguish between the actual and the desired culture. What is culture? According to Taylor, the culture in an organisation could be seen as the reflection of all the ‘messages’ that staff receive and that influence their behaviour. All kinds of messages show what is important and what is valued in the organisation. These messages ‘tell’ you how you should behave in order to be successful and respected. For example: Who gets promoted/fired by performing certain behaviours? How approachable are board members and how do they behave? How does staff talk about customers? What happens when you make a mistake? How is good and bad news dealt with? And so on. These messages come from three main sources:

- Behaviour of others, especially board members and those who appear to be important;
- Symbols, as in observable events, artefacts and decisions to which people attribute meaning (e.g. who gets promoted, what happens when a milestone is reached, how are reorganizations managed);
- Systems or mechanisms for managing people and tasks (e.g. the bonus system, the budget cycle, the new products approval process).

These sources, or drivers, behind the actual culture of the organisation should be clearly understood and analysed. Once understood, they should be mapped to the so called ‘desired culture’. This desired culture usually is described by means of identity, brand value, stakeholder’s expectations and desired risk, control and governance structures. The desired culture is often outlined in a company’s brand statement, or strategy, but is not often clearly substantiated in the drivers of culture. So in order to create an effective and efficient ‘governance culture’, the systems, symbols and behaviours of important people should be aligned with the way the organisation would like to have its governance organized. Or in other words: the organisation as a whole should ‘walk the talk’. Culture and behaviour can be measurable and influenced, but that requires different skills for many business controllers, internal auditors, risk managers, legal staff etc, who often tend to focus on more formal controls.

4. How to formalise governance?

Paragraph 2.2 states that organisations should formalise their governance to make it accessible and understandable for management and staff. This section presents some (conditional) essentials for the formalisation of governance in a constantly changing and moving organisation, specifically:

- Requirements;
- Accessibility;
- Communication;
- Keep it alive.

The exact form and contents depend on several factors, such as: the size of the company, the “state of the art” of an organisation’s governance and “the tone at the top”. In “The Building blocks of governance” a list of possible topics is presented.

4.1 Requirements

Irrespective of how the governance of an organisation is formalised, it should always meet the following requirements:

- **Ownership**: Ownership for the governance framework, which also means ownership for the quality of it, should be at the highest level in the organisation, preferably with the CEO or the COO. The selection of one of these roles as sponsor should help to make clear to the organisation that governance is something for the whole organisation, and at all levels, and not only for the financial function.
- **Coordination**: One function should be responsible for a periodic screening and adjustment of the whole formalised governance.
- **Relevant**: The building blocks used in governance should be relevant for the business strategy and for management and employees executing it.
- **Clear and understandable**: The formalised governance should consist of clear texts and simple language. The more difficult the language, the less it is read, understood and applied.
- **Concise**: The formalised governance framework ought to be complete but concise and well structured. The structure should facilitate both providing an overview as well as facilitating access to detailed information. Obviously, detailed documentation is often available on the intranet. For an efficient use, a well thought out retrieval system ought to be in place.
- **Easy access**: The formalised governance should be easily accessible for all company employees globally. This can be achieved e.g. by making a ‘governance site’ on the company’s intranet. Making a governance site will also facilitate an easy search functionality which enhances its use.
- **Laws and regulations**: It is clear that any statement or policy in the internal governance must not be in conflict with the local laws or regulations where a specific organisation (or part / division of a larger company) is operating.
- **Up to date**: if the content is outdated, employees may not be willing to adopt and apply the principles of governance as they perceive governance is deemed as “not important enough to keep up to date”.

4.2 Accessibility

There are several ways to formalise the governance framework in an organisation. Key consideration is that the formalisation should fit the organisation in its size, complexity and way of working. We have found three main solutions:

- A compact booklet outlining the key principles of the governance of the organisation (possibly with references to more extended information on the company’s intranet);
- An extensive collection of all relevant governance documentation, all accessible via a kind of governance home page on the company’s intranet;
- A governance manual, being a hardcopy document containing all relevant governance documentation.
More and more used nowadays is an internet based solution, that offers several functionalities which are not available in traditional hardcopy manuals or "pdf" files. For example users can:

- Easily navigate through the pages. By entering some key words, the site can present relevant pages or text directly.
- Add comments to the text, for example experiences in the application of corporate policies. Such a “wikipedia” function enhances the content to an interactive and dynamic level. If this functionality is applied, a moderator should monitor and review the comments or adjusted text and remove or correct content that is not useful or appropriate.
- Rate the governance texts. A rating system can help the owner to increase the quality and clarity of the text.
- Use the formalised governance on modern devices like tablets and mobile phones, which will increase the acceptance and accessibility of the content. In such a way, the content can be re-used in for example “governance apps” specifically developed for the company.

4.3 Communication

An important aspect of communication is to open up the governance framework on the organisation’s intranet. Specific attention should be paid towards the presentation of the formalised governance. Its launch (and later versions) should be accompanied by a periodic “marketing campaign” to attract and to keep the attention of employees and management. This can be achieved, for example, through periodic blogs by senior management in which they discuss governance principles or building blocks, banners on the front page of the intranet, governance workshops in management forums or Management Development programs or by explaining the governance building blocks in (mandatory) e-learning activities. Additionally the topic can be addressed in meetings of management and employees.

4.4 Keep it alive

Some important cornerstones to make governance “living” have already been mentioned in section 4.1. However, proper implementation and communication contribute to the sustainability of the governance framework as a reflection of the governance, policies and desired behaviour. It is obvious that also appropriate actions are required:

- Every owner of a policy or other part of the governance framework should feel responsible for its relevance and should ensure it is kept up-to-date;
- Every owner of a policy or other part should monitor compliance with that element of the framework;
- Infringements should be reported and appropriate follow-up should take place.

The more and more widely used ‘three lines of defence’ principle, which allocates accountabilities and responsibilities to business and support functions, supports strongly an effective implementation of governance:

- The first line, i.e. business management, is accountable for the governance in all its aspects;
- The second line, i.e. support functions like Risk Management, Compliance and Controlling, assist management with specialist support in designing policies, providing advice and executing monitoring tasks to validate that the first line complies to the policies;
- The third line, i.e. Internal Audit, assesses the effectiveness of the functioning of the first and second line functions and processes, identifies potential gaps or overlaps between these functions and ultimately should be able to provide comfort to the Board and the Supervisory Board that the governance of the organisation is adequate.
5. How to audit governance?

In previous sections, we have defined “governance”, identified the “building blocks” of governance and determined the requirements of the formalised governance framework. It is clear that governance is part of every audit universe. In fact, elements of governance will be part of each and every audit. This section will give some more thought on how to include governance in the audit plan and how governance can be assessed. This section is not intended as a checklist for completeness: it is more a summary of ideas and suggestions.

5.1 The Internal Audit function and governance: the IIA view

The definition of Internal Audit from the IIA is:

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.

The role Internal Audit has regarding governance is further elaborated in Standard 2110 and the related practice advisory 2110-3 on Governance: Assessments. The Standard is very clear on what the role and responsibility of Internal Audit is regarding governance:

- The Internal Audit activity must assess and make appropriate recommendations for improving the governance process in its accomplishment of the following objectives:
  - Promoting appropriate ethics and values within the organisation.
  - Ensuring effective organisational performance management and accountability.
  - Communicating risk and control information to appropriate areas of the organisation.
  - Coordinating the activities of – and communicating information among – the board, external and Internal Auditors, and management.

The Internal Audit function has a prominent role in assessing the effectiveness of governance, and by advising on improvements. This is done by answering two questions:

- Does the organisation have a consistent governance model that addresses in a proper way all relevant requirements? This question addresses the design of the governance model.
- Is the governance model effectively communicated and adhered to?

The building blocks as described in chapter 3 could be used to answer these questions. For any Internal Audit function, governance should have a very high priority on the audit planning, not just because of the requirements, but also because good governance forms the basis of every system of internal control and as such good governance should be the guiding principle for any audit on management controls.

Another question is what comfort level Internal Audit functions could provide to their boards regarding governance and what kind of opinion (if any) could be given. This topic would need further and detailed analysis, and was outside the scope of the project group. But this document definitely could be seen as a stepping stone for this discussion.

5.2 The Internal Audit function and governance: rules and regulations

Many developments in the past few years have led to various discussions on governance and the role of internal audit. Sometimes it lead to regulation:

- According to the regulations of the New York Stock Exchange, every listed company ought to have an Internal Audit function.

3International Professional Practices Framework (IPPF) – The Institute of Internal Auditors
• The Dutch Corporate Governance Code also assumes that an Internal Audit function is established in listed companies. If not, companies have to explain why (“comply or explain”).

Besides stating these principles, these regulations do not elaborate on the objectives and responsibilities of Internal Audit.

However, in the financial services sector (banking and insurance) we are seeing developments that specify Internal Audit activities in more detail:
• CEIOPS\(^4\) advice with respect to the System of Governance in connection with compliance with Solvency II;
• The Dutch banking code (“Code Banken”), which was written by the Dutch Banking Association produced recommendations to improve governance and risk management in the banking sector in the aftermath of the financial crisis,
• The Dutch insurance code (“Code Verzekeraars”), written by the Dutch Association of Insurers, that listed recommendations and governance principles for the insurance sector,
• The recently published consultative document of the Basel Committee on banking supervision “The internal audit function in banks”.

All these regulations require internal auditors to report on “Governance”, or “the System of Governance” as part of their annual audit plan. What exactly the Internal Audit function should do, is only described at a very high level, e.g. “Internal Audit should address the quality of the governance” or “the Internal Audit function should include an evaluation of the adequacy and effectiveness of the internal control system and other elements of the system of governance”.

However the above mentioned regulations are focused on the financial services sector, many companies in other sectors take the key principles of these regulations as best practices. As said earlier, these regulations don’t address the topic what kind of comfort internal auditors should give.

### 5.3 Requirements

These regulations sometimes come with key requirements for Internal Audit functions, especially when it relates to their role in evaluating governance. Not surprisingly, as governance relates to the way the board of management is managing and directing the company, the key requirements for Internal Audit functions are:
• Independence and objectivity (Standards 1110 and 1100 and Practice Guide “Independence and Objectivity” (October 2011));
• A direct reporting line to the board (Standards 1110 and 1111)
• Sufficient staffing, not only in a quantitative perspective but also in a qualitative perspective. At least some staff members should have the appropriate training, experience and seniority (including the “guts”) to accomplish assignments in the governance area – (Standards 1200 and 2030).

These elements should be described and agreed in an Internal Audit Charter, approved by the Board and the Audit Committee [including the approval of the Supervisory Board].

Given the nature of governance and the high level of involvement of senior management, the key requirements mentioned above are, with respect to this topic, of even more importance than for other audit area.

---

\(^4\)CEIOPS: Committee of European Insurance and Occupational Pensions Supervisors

\(^1\)International Professional Practices Framework (IPPF) – The Institute of Internal Auditors
5.4 How can the Internal Audit function address governance?

The various (new) rules and regulations provide for definitions of governance and elements of corporate governance that an entity should have in place, or should consider. However, what good governance is, is highly dependent on the organisation itself, its culture, its business, its risks, etc. In many cases, governance can be seen as a mixing panel as used for optimizing music recordings: there are many switches, many settings, and the right mix is dependent on the music itself.

Therefore a general audit program which fits all situations cannot be realised. A dedicated, tailor made audit approach is required.

Below we formulate some key questions per governance building block that could be asked when building the governance assessment plan. Of course this list is not limitative.

**Organisation’s objectives:**
- What are the key risks of our company? This will include but not be limited to risks regarding: culture, structure, compliance, business model and alignment with authorisations, etc.
- What are the objectives of our company and are they clearly set, agreed upon and communicated?
- Is a clear strategy formulated and communicated to the appropriate levels in order to realise the objectives?
- Is the governance model sufficiently supporting the achievement of business objectives and implementation of the strategy?
- Have all relevant stakeholders been sufficiently involved in the objective and strategy formulation processes?
- Are the objectives formulated in a way that they give sufficient guidance and input for the design of the other building blocks?

**Ethical standards:**
- Is a clear set of ethical standards available?
- Have sufficient measures been taken to communicate and implement them?
- Do we ‘walk the talk’, and is the tone at the top in line with them?
- Are incidents sufficiently registered and have appropriate actions to address them been formulated?
- Do the ethical standards address the relevant key risks?

**Policies, governance processes and organisational structures:**
- Is the governance design formally reviewed and approved by the Board and the Supervisory Board?
- Is there a comprehensive, yet concise, governance framework available like described in this document?
- Which elements of the policies and procedures relate to key risks, and how can Internal Audit obtain assurance on the operating effectiveness of the controls?
- Does this building block sufficiently address the relevant key risks? (Design evaluation: completeness of policies, adequacy of structures, etc.)
- Are policies and governance processes sufficiently implemented and understood by staff and others? (E.g. by training and tests of operating effectiveness)
- Does the organisational structure sufficiently support a proper execution of policies and governance processes?
- Does our governance design meet legal requirements as included in laws and regulations?
- What are the key governance related policies and procedures? And are they properly linked or referenced in the manual?
- Does the organisation place authority (including formal authorisations) at the appropriate level to meet strategic objectives?
- Are policies and procedures agile to respond to changes and do they sufficiently address key risks?
• Are all relevant policies and procedures, as included in the governance manual, compliant with applicable laws and regulations?
• What entity level controls are relevant in connection with governance?
• Is there a process in place by which management and the board regularly review all assumptions and decisions relating to governance? If so, how are changes embedded in the organisation?
• Is there a periodical review, initiated by the board, that all policies and governance processes are properly adhered to?

Stakeholder expectations:
• What are the expectations of stakeholders and are these sufficiently addressed in our governance design?
• Are relevant governance provisions sufficiently disclosed to external stakeholders and regulators?
• Are stakeholder expectations sufficiently understood by staff and others?
• Are all stakeholder expectations sufficiently managed (as far as possible)?

Culture and behaviour:
• Are our culture and behaviour risks sufficiently addressed?
• Is the importance of culture & behaviour sufficiently understood by staff and others?
• Which culture & behaviour oriented controls are relevant in relation to the governance model, and how can Internal Audit obtain some level of assurance on the effectiveness of these controls?
• Does the organisation give the staff authorisations in line with their skills and values?
• Do we have the actual culture and the desired culture sufficiently clear?
• Do we ‘walk the talk’?
• How do we measure culture and behaviour in our organisation and to what actions does this measurement lead?

The chapter “Building blocks of governance” gives more background on what internal auditors can expect and can consider. Both presence of these elements as well as the effectiveness of the implementation thereof can be part of the audit scope.
6. Good practices

In this chapter we provide a number of good practices, both regarding how governance can be formalised in an organisation and how governance can be audited. Again we stress that both the design (and formalisation) of governance as well as auditing governance is quite organisation specific. Nevertheless we as internal auditors should strive to create some standardisation on it. These good practices act as a starting point on this.

Formalisation of governance:
- **Definition** - A company has a clearly defined governance as outlined in the governance building blocks and acknowledged its importance, including three basic principles: minimization of possible conflicts of interest, acknowledgement of the relevant corporate governance codes and a group-wide Code of Conduct.
- **Communication** - A company has a clear and concise manual that is updated yearly and comprises the key messages regarding governance. This booklet is distributed to all employees and includes references to the location (intranet) where more extensive information can be found.
- **Accessibility** - A company has listed on its intranet all relevant governance documents including publication date. These are accessible in a number of ways: for example via an overall governance portal, via sub-sites for specialist departments and via general search and find functionalities.
- **Training** - A company uses mandatory yearly e-learnings for relevant staff that includes the key governance messages and changes. In this way, specific themes that require attention are addressed annually.
- **Governance structure** - A company has created a clear picture in which all governance parties are listed (boards, relevant support departments, key business lines and relevant committees), including the relevant reporting lines (hierarchical, functional, statutory). This picture is available on the intranet and at the various parties can be ‘clicked’ for further information (charters, ways of working, etcetera).
- **Three lines of defence** - A company clearly acknowledges the use of the three lines of defence model in the allocation of the various accountabilities of all parties in achieving the organisation’s objectives. The management board oversees the governance framework; business management acts as the first line of defence (with ultimate responsibility for objective realisation including risk management and controls); specific support functions (acting as second line of defence) are responsible for setting corporate policies, monitoring the related controls and reporting on it and provide guidance and assistance to the first line of defence; the Internal Audit function acts as the third line of defence and provides independent assurance regarding the design and operational effectiveness of the governance, risk management and control processes, including the roles of first and second line.

Auditing governance:
- The Internal Audit function has a charter that explicitly mentions that it evaluates the effectiveness of governance and provides recommendations for improvement to the board and management. The charter further details the assessment of governance and includes strategy and objectives setting, accountabilities, integrity, transparency, adequate staff competencies, enterprise risk management processes and control processes.
- The Internal Audit function has included in all its audit programs a standard section that addresses the related governance items of the audit object, so that annually an efficient consolidation can take place of all audited elements of governance. In addition, separate audits are executed on missing elements of the governance.
- The Internal Audit function reports annually on governance. Given the challenges, with no substantially crystallized and generally available accepted standards, it provides a ‘negative assurance’ statement at the best.
- An Internal Audit function can use its entity level control assessment as the basis for determining the audits on governance, thus creating clarity to the organisation, making optimal use of available structures and preventing overlap.
### Appendix: Examples of definitions of governance

The table below provides some examples of statements on or definitions of corporate/organisational governance and their source. These definitions are included in arbitrary order for information purposes only and this is not intended to be a complete list.

<table>
<thead>
<tr>
<th>Source / Reference</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>IIA - Glossary</td>
<td>The combination of processes and structures implemented by the board in order to inform, direct, manage, and monitor the activities of the organisation toward the achievement of its objectives.</td>
</tr>
<tr>
<td>OECD, Principles of Corporate Governance, revised May 2004</td>
<td>Corporate governance involves a set of relationships between a company’s management, its board, its shareholders and other stakeholders. Corporate governance also provides the structure through which the objectives of the company are set, and the means of attaining those objectives and monitoring performance are determined.</td>
</tr>
<tr>
<td>Report of the Committee on the Financial Aspects of Corporate Governance (Cadbury Committee), December 1992.</td>
<td>Corporate governance is the system by which companies are directed and controlled.</td>
</tr>
<tr>
<td>Principles of Corporate Governance for Listed Companies, Tokyo Stock Exchange, Inc., December 2009</td>
<td>Corporate governance is generally defined as the framework for disciplining corporate activities.</td>
</tr>
<tr>
<td>Hermes principles (UK), 2002</td>
<td>Governance sets out the structures and processes by which a company should be controlled through its board. It should encourage positive entrepreneurial behaviour, while having appropriate checks and balances through its independent directors and the right balance of power to ensure decisions are wisely made.</td>
</tr>
<tr>
<td>Corporate Governance in Denmark - recommendations for good corporate governance in Denmark, Second part in The Nørby Committee’s report, 2001</td>
<td>Corporate governance is the goals, according to which a company is managed, and the major principles and frameworks which regulate the interaction between the company’s managerial bodies, the owners, as well as other parties who are directly influenced by the company’s dispositions and business (in this context jointly referred to as the company’s stakeholders). Stakeholders include employees, creditors, suppliers, customers and the local community.</td>
</tr>
<tr>
<td>German Code of Corporate Governance, Berlin Initiative Group, 2000</td>
<td>Corporate governance describes the legal and factual regulatory framework for managing and supervising a company.</td>
</tr>
<tr>
<td>The Australian Stock Exchange Corporate Governance Council, Principles of Good Corporate Governance and Best Practice Recommendations, March 2003</td>
<td>Corporate governance is the system by which companies are directed and managed. It influences how the objectives of the company are set and achieved, how risk is monitored and assessed, and how performance is optimized.</td>
</tr>
<tr>
<td>Belgian Code on Corporate Governance, 2009</td>
<td>Corporate governance is a set of rules and behaviours which determine how companies are managed and controlled. A good corporate governance model will achieve its goal by setting a proper balance between leadership, entrepreneurship and performance on the one hand, and control as well as conformity with this set of rules on the other hand.</td>
</tr>
<tr>
<td>Source / Reference</td>
<td>Definition</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Toronto Stock Exchange Committee on Corporate Governance, Dey Report, December 1994.</td>
<td>Corporate governance means the process and structures used to direct and manage the business and affairs of the corporation with the objective of enhancing shareholder value, which includes ensuring the financial viability of the business. The process and structure define the division of power and establish mechanisms for achieving accountability among shareholders, the board of directors and management. The direction and management of the business should take into account the impact on other stakeholders such as employees, customers, suppliers, and communities.</td>
</tr>
<tr>
<td>Open Compliance and Ethics Group [OCEG]</td>
<td>Governance is the culture, values, mission, structure, and layers of policies, processes, and measures by which organisations are directed and controlled. Governance, in this context, includes, but is not limited to, the activities of the board, for governance bodies at various levels of the organisation also play a critical role. The tone that is set, followed, and communicated at the top is critical to success.</td>
</tr>
<tr>
<td>Forrester research, 2007</td>
<td>The culture, policies, processes, laws, and institutions that define the structure by which companies are directed and managed. Corporate governance includes the relationships among stakeholders and the goals for which the corporation is governed.</td>
</tr>
<tr>
<td>Wikipedia</td>
<td>Corporate governance is the set of processes, customs, policies, laws, and institutions affecting the way a corporation (or company) is directed, administered or controlled. Corporate governance also includes the relationships among the many stakeholders involved and the goals for which the corporation is governed. In contemporary business corporations, the main external stakeholder groups are shareholders, debt holders, trade creditors, suppliers, customers and communities affected by the corporation's activities. Internal stakeholders are the board of directors, executives, and other employees.</td>
</tr>
</tbody>
</table>
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.