Questions a Board may ask to understand how an organisation controls its risks

IIA Norge

Questions a Board may ask to understand how an organisation controls its risks

RESPONSIBILITY FOR RISK MANAGEMENT

The holding of a position on a Board or in a control committee in an organisation is a considerable responsibility and may also lead to personal liability.

The aim of this guidance is, through the presentation of a set of questions, to give a better understanding of the most important risks which can impact an enterprise and how these can be managed.

Reading the financial statements will seldom give sufficient information to understand the key drivers of an organisation´s bottom-line results. An understanding of the enterprise´s risk profile and how this is managed is an approach which can give valuable insight into the business. The definition of «risk» used in this guidance is «the effect of uncertainty on objectives», where «the effect» is defined as a «deviation from the expected — positive and/or negative» (cf. the definition used in the ISO standard on Risk Management).

All economic activity depends on taking one or more types of risk. It is, therefore, crucial to understand the relationship between risk and value added/profit and loss. Two apparently equal results can be the result of very different risk profiles. In order to understand how good a positive result achieved is, it is, therefore, necessary to understand the related level and type of risk taken by the enterprise.

Risk in this context includes short term risks occuring within a one year horizon, but perhaps even more importantly it includes strategic risk which includes the risks an enterprise takes, or will face, as a consequence of pursuing its strategy or major changes in geopolitical conditions, markets or regulatory requirements.

In modern risk management practice, it is usual to refer to «enterprise-wide» risk management as a method to both understand and manage the organisation in a holistic and unfragmented manner. This type of risk management is often defined as ERM (Enterprise Risk Management). Considerable advantage can be gained by adopting ERM, compared to an alternative approach of managing individual risks on a stand-alone basis, without modelling their combined effect on the enterprise.

The three lines of defence in a governance model

It is important to define clearly the roles and responsibilities of the various organisational functions. This will contribute to the efficient use of resources, a satisfactory level of control over all activities and avoid the duplication of tasks and functions (including activities connected to risk management and internal control). This also involves clarifying the interfaces between the functions and their positioning in the organization's overall risk management and internal control structure.

The Risk Management function, Compliance and other second line of defence functions have areas of responsibility and/or tasks which may overlap with each other. Although these functions are independent of each other, it is important to maintain open communication between these functions to ensure an efficient use of resources. It is also possible to consider consolidating these functions organisationally to strengthen professional co-operation and the delivery of results.

The «Three Lines of Defence» model (cf. illustration below) provides a high level overview of the roles and responsibilities for internal control and risk management. Even in organisations where a formal risk management framework or system does not exist, the model can help improve understanding of the organisation´s ERM and internal control.

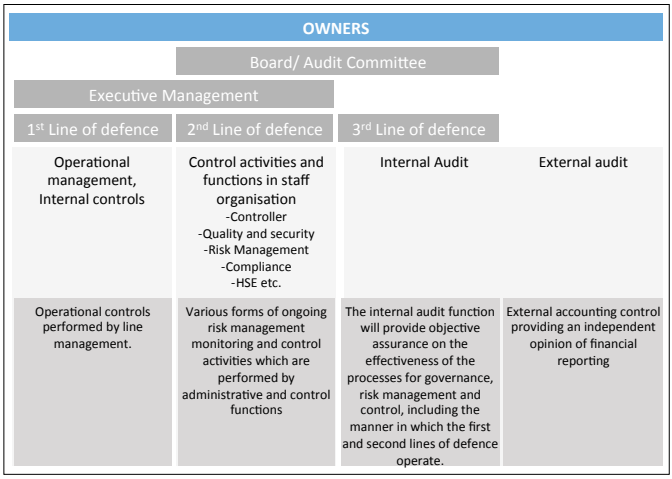

Figure - Description of the three lines of defence

The model distinguishes between three groups (or lines) that are involved in effective internal control and risk management:

- Functions that own and manage risk (first line)
- Functions that exercise oversight over risk (second line)
- Functions that provide independent assurance (third line).

In the marketplace, there are a number of organisations which build a bridge connecting these three important components within governance: Governance, Risk Management and Compliance (collectively abbreviated to «GRC») with the aim of ensuring that these functional areas work in unison and perform as efficiently and effectively as possible.

In line with this construction, this document has split the questions about governance into the following three components: Governance, Risk Management and Compliance. Under each caption, we have listed a set of specific risk management related questions applicable to the management of both business risk and operational risk.

GOVERNANCE

- How is the organisation´s Risk Management function organised? Is it organised per business area and only thus, or is there an ERM function which looks at the enterprise as a whole.
  Background: It is important to understand if the organisation manages its activities based on a holistic view of the risks the organisation is exposed to or only a partial view?

- How does Risk Management carry out its reporting? Does it report exclusively to the Executive Management or to the Board including Risk and Audit committees or to both of these stakeholder levels?
  Background: If the Board is to be in a position to place reliance on the robustness of Risk Management, it is essential that there is a high degree of professional integrity amongst those who are responsible for the function, and moreover, that there is a facility for directly communicating with the Board, should the situation arise that the Risk Management function does not share Executive Management´s view with respect to a critical situation/case etc.

- Are the organisation´s risk management and internal control processes aligned with the organisation´s goals and policies?
  Background: It is vital that both policies and processes are aligned with the strategy and associated risks.

- Is the adequacy of resources in the Risk Management function regularly evaluated against requirements and compared to similar organisations?
  Background: It is important that the Board understands whether the organisation has evaluated whether resources are in line with the scope and ambitions required by the risk management strategy.

RISK MANAGEMENT

- How are the competency and professional integrity of Risk Management employees evaluated? Is there a structure for systematic education/professional development in the risk management area applicable to both managers and staff?
  Background: It is important for the Board to understand whether the organisation is able to develop the required level of competency in this professional area.

- What activities has the Executive Management initiated to support a sound risk culture? Is risk ownership clearly delegated?
  Background: It is important not to encourage the failure to take responsibility, or the development of an unhealthy risk culture, e.g. through bonus and remuneration systems, which are based on sub-optimal incentives.

- Does the Risk Management function share information regularly with Internal Audit?
  Background: It is important to have in place a frank and open dialogue between the organisation´s Internal Audit and Risk Management functions. Internal Audit is required by international standards (published by IIA) to take account of the enterprise´s risk picture in the following specific areas:

– Preparation of a risk-based audit plan
– Evaluation of the enterprise´s strategies, objectives and risks
– Audit work aimed at improving processes for governance, risk management and control
– Inclusion of material risks in the reporting to Executive Management and the Board

- Has it been considered how the risk management system shall be integrated with other parts of the internal control system and how the Risk Management function shall co-ordinate its work with other control functions, such as Compliance, Quality Audit and Internal Audit?
  Background: It is important for the Board to understand whether related professional environments co-operate to avoid duplication of work, overlapping roles, development of two conflicting sets of terminology etc.

- How is the risk picture communicated to the Board both with respect to form (quantitative/ qualitative), content and frequency?
  Background: It is important to understand how hands-on the Board is able to be. Is the risk information sufficient for the Board to act on before an unwanted outcome is reality or is the Board limited to acknowledging in retrospect that the event happened?

- How are significant emerging risks identified before they are reality; the same question applies to material control weaknesses, are these communicated and reported to the Executive Management and the Board?
  Background: It is important that changes in the risk picture, as a result of external factors and identified weaknesses, are communicated to the Executive Management and the Board. It is usual to have in place a system for registering material loss events and that these events are reported to the management and the Board.

COMPLIANCE

- Is the organisation´s Compliance function part of a staff unit reporting at a sufficiently high level within the organisation? If not, who does Compliance report to?
  Background: it is important for the Board to understand where responsibility for the enterprise´s Compliance function is placed within the organisation and whether it operates independently of the organisation´s risk management and other risk processes.

- Is the Compliance function, however organised, responsible for monitoring both internal and external regulations and guidelines? What regulations and guidelines (internal and external) are included in the Compliance function´s area of responsibility?
  Background: It is important that the Board understands the extent of Compliance work, who is, in fact, leading it, or if the function happens to be split, as well as Compliance priorities, and how these are communicated.

MANAGING BUSINESS RISK

- Does the enterprise have a high level risk strategy and, if so, who is responsible for this?
  Background: It is important that the Board understands whether the organisation sees risk management as a strategic and integrated part of business development.

- Has the enterprise articulated a risk appetite which is holistic and quantifiable?
  Background: It is important that the Board understands to what extent this has been formulated if at all. If a risk appetite has been formulated how much of the enterprise´s profitability and risk capital have been tied up as a result of the risk profile?

- What are the organisation´s most important value drivers?
  Background: It is important that the Board understands the main source of value creation, in order to facilitate comprehension of the risks, which can affect the value creation both in a positive and negative direction.

- Has the organisation quantified the risks which can affect the most critical value drivers and is there a reasonable connection between allocated risk capital and expected profitability?
  Background: A quantitative measure ensures a common language, which most people will understand. One million US dollars will mean the same to everyone, whereas a yellow flag on a risk chart is more open to interpretation. A quantitative expression ensures an easier comprehension of the connection between value creation and potential loss that may be suffered in the process.

- What is the enterprise´s strategy in relation to the most critical value drivers, both in a short-term and long-term perspective?
  Background: Recent research shows that many organisations are exclusively focussed on the coming few months, whilst the greatest effect on the business will be what happens to strategic risks. Strategic risks often have a major effect but still are paid little attention because they are more difficult to articulate, and they require some degree of co-operation between the strategy unit and Risk Management (something which is gradually becoming more and more common).

- Have risk management and hedge strategies been developed and are these evaluated in relation to securing against fluctuations in profitability or balance sheet values? Does the organisation´s risk management also take into account taxation effects?
  Background: Accounting rules for hedging can be both inflexible and may not be aligned with the enterprise´s high level economic exposures e.g. from an economic perspective the management of risk should be post tax as it makes little sense to protect more of the profit than the enterprise will end up with after tax has been charged.

- Is the set up for risk communication between Executive Management and the Board pro-active or reactive?
  Background: In order to understand and influence strategic development it is important to obtain forward-looking information. In this way a Board can to a greater extent be a contributor to and owner of important decisions proactively.

- Are decision making documents both to Management and the Board adequately focused on shedding light on the underlying risk aspects? In critical cases, the decision making document should detail both potential impact and probability, based on a risk perspective.
  Background: An objective a risk picture as possible is an essential element in ensuring a relevant basis for a decision.

- Does the enterprise have major positions/ exposures which can lead to major differences between the economic outcome and the accounting profit and loss?
  Background: As a result of accounting requirements, it is possible that major differences can arise between the economic outcome and the accounting profit and loss e.g. in respect of hedging of future income and costs in foreign currency.

MANAGING OPERATIONAL RISK

- Has the enterprise discussed which operational risks may have the greatest impact on net profit?
  Background: It is important to clarify and reconcile that there is a consensus concerning the risk picture and the implication of the various risks, as well as an overall understanding of what this picture means for the organisation

.

- Does the enterprise have a Business Continuity Plan which is based on a risk assessment?
  Background: It is important to evaluate the value chain and ensure that plans/ spare parts etc. are in place so that the value chain can be brought in order again after a loss event. This will save the enterprise from experiencing unnecessarily long downtime and will be viewed favourably in respect of insurance and coverage in the market.

- Have catastrophe scenarios been prepared?
  Background: All businesses should think through and define for themselves what a catastrophe is and what it may mean for profitability/ balance sheet values. Based on such an analysis, it should be possible to identify less significant activities which, nevertheless, have the potential to overturn the whole enterprise, even though the probability of occurrence is extremely low. A question which should then be addressed is – do we wish to continue with these activities/ does it make economic sense?
  It is also important to identify these type of scenarios because normally the probability of such events is so low that they will likely never be included in the documentation of high level risk charts.

- How are insurance policies integrated/ included in risk management?
  Background: If the enterprise has its own captive insurance company, is the scope of cover aligned with the enterprise´s high level needs or is the business area defined by the insurance specialists themselves? The person responsible in the enterprise for arranging insurance and the risk manager should work closely together.

This guidance has been developed by
the Risk Management Network of IIA Norge
and has been translated from the Norwegian original.

1st edition published January 2017.

For further information please send an email to
risikostyring@iia.no
or refer to our home page at www.iia.no/risikostyring

IIA Norge
Post box no. 1417 Vika, 0115 Oslo
Office address: Munkedamsveien 3B, 3rd floor
Email: post@iia.no
www.iia.no