GUIDELINES FOR THE RISK MANAGEMENT FUNCTION

2017

IIA Norge

Guidelines for the Risk Management function

PREFACE

"Guidelines for the Risk Management function" has been developed by a group whose members work in the risk management area in several different industries. The working group is a committee of Network Risk Management, a sub-faculty of the Association of Internal Auditors Norway (IIA Norge).

IIA Norge would like to thank the following people for their help with the development of this guidance and incorporation of responses following the consultation round:

Ayse B. Nordal, Municipal Undertaking for Educational Buildings and Property in Oslo
Martin W. Stevens, Gjensidige Insurance
Ole Martin Kjørstad, BDO
Petter Kapstad, Statoil.

The goal of the working group has been to describe the purpose, responsibilities and duties of the Risk Management functions, as well as the relevant assumptions and success factors, regardless of industry. The principles in this guidance may also be useful for organizations without a discrete Risk Management function, but which have a similar function with comparable duties.

The target group for these guidelines is organizations that would like to either establish a Risk Management function, or develop their existing risk management function further.

It was a considerable help in developing these guidelines that the working group could draw on the structure and formulations in the "Guidelines for the Compliance function" published by IIA Norge in 2015. A debt of gratitude is owed to those who developed the Compliance guidelines.

Translated from the Norwegian original by Martin W. Stevens.

ISBN 978-82-92750-12-4

CONTENT

1 INTRODUCTION

1.1 The purpose of this guidance

The need to establish a Risk Management function will depend on, amongst other things, the industry and the organization. Typical drivers have been the need for management and control in challenging areas which are exposed to a high risk of significant financial losses, physical damage and loss of human life. Furthermore there are a number of regulated industries which place concrete requirements on the organisation, structure and performance of risk management activities which will raise requirements over and above the recommendations described in these Guidelines. Increasingly it is seen that the management of positive and negative uncertainty related to a volatile environment and future financial development has led to risk management achieving acceptance as an important strategic tool. It is the case that, in line with international development, Norwegian statute requires the establishment of a Risk Management function as an element of sound governance.

In this guidance we have tried to describe "best practice" for the Risk Management function regardless of industry, regulation and size. It does not cover legal requirements; rather it introduces the basic principles of the function. Individual adaptations will naturally depend on each organisation's nature, size, complexity and organisational culture.

These Guidelines seek to provide some clarification and limitations regarding the organization of a Risk Management function. This includes the distribution of roles and responsibilities between the different control functions of an organization, such as internal audit, the Risk Management function and the Compliance function.[1]

A number of industry-specific guidelines have been developed internationally which describe the elements and requirements characteristic of an efficient and effective Risk Management function adapted to specific regulatory requirements. There are however common elements in these and it is these, together with experience, from Norwegian organisations which form the basis for these Guidelines.

Risk management will take place at many and varied levels in an organisation. These Guidelines describe the function for Enterprise Risk Management (ERM). The principles which are described will also have validity for those working with risk management within a more limited and specialised area of an organisation.

1.2 Enterprise Risk Management - ERM

The taking of risk is a natural part of running any enterprise[2], but it is often not explicitly stated in the formulation of business decisions. The expression risk has often been exclusively associated with unwanted events, and risk management has been defined as analysing and restricting the probability and impact of unwanted events. This is only one dimension of the total picture. Evaluating positive outcomes is just as important an element of ERM as evaluating the downside as ERM is concerned with the whole picture enterprise-wide and evaluating risk strategy in relation to a portfolio of risks.

The objective of ERM is to maintain risk at an acceptable level and ensure the best balance possible between threats and opportunities – in line with the risk appetite and business strategy of the Board[3] and Executive Management. It is concerned with ensuring the achievement of goals as the enterprise develops and appropriate management of the organisation's assets, including avoidance of losses as a result of unwanted events. This will include matters occurring in all levels of the organisation. A pre-requisite for being able to exercise sound risk management is therefore that there are clearly defined goals at the strategic level, to which goals at other levels in the organisation may be linked. In this way risk evaluations at all levels will be linked to a hierarchy of objectives which supports the enterprise's overall strategy.
In practice this means ensuring the best possible basis for arriving at decisions at the various levels of the organisation, so that the decisions made will support the overall objectives. Subsequently it is important to have a sound mechanism to ensure the achievement and monitoring of the decided activities. ERM's role in governance is illustrated in figure 1.

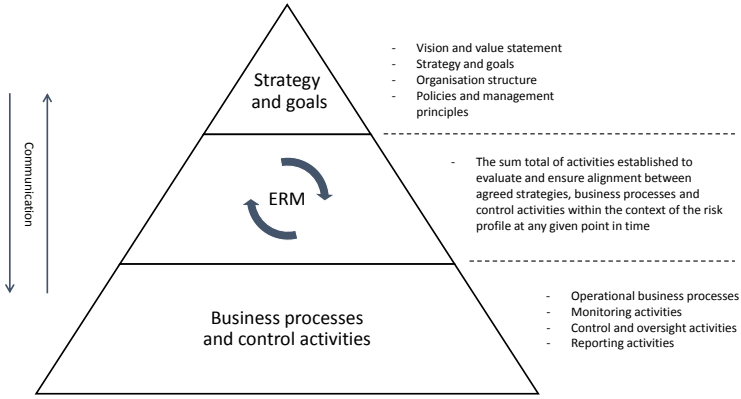

Figure 1 The interrelationship between ERM and governance

Risk management may be defined as systematic, co-ordinated and pro-active activities aimed at the evaluation and treatment of uncertainty and events which can impact the achievement of goals.
This includes amongst other things the organisation's ability to:

- Influence the probability and positive or negative impact of events
- Understand/exploit correlation between various types of risk
- Monitor development of the risk profile over time
- Initiate activities which align the path of development with the required direction
- Build a culture which ensures the implementation of activities and leads to sound risk management.

This presupposes a holistic perspective is applied across all organisational units, functions and risk categories (strategic, financial, operational and other risks) thus avoiding "silo" thinking and sub-optimisation.

In essence risk management is concerned with obtaining the best possible basis for decisions and facilitating the efficient and effective performance and monitoring of decisions made. This will be achieved through a conscious attitude to an acceptable level of risk and the required risk exposure.

1.3 Risk management at various organisational levels

Risk management takes place at various levels of the organisation dependent on the relevant focus. In ERM the focus is on the consequence for the whole enterprise. If the focus is in respect of personal goals or goals within the individual's own business area this can be defined as "personal" risk management. The totality of personal risk management in an organisation can lead to sub-optimisation from the perspective of the enterprise as a whole. The performance of task risk management should also have a basis in an enterprise-wide perspective through amongst other matters the goal-setting and any incentive structure. These three separate perspectives: ERM, task risk management and personal risk management are illustrated in figure 2.

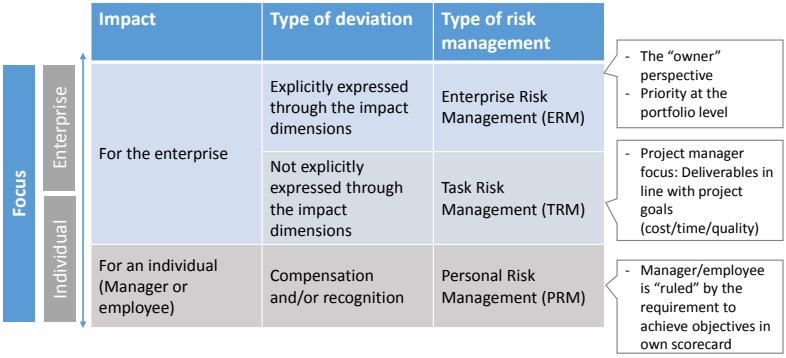

Figure 2 Types of risks and risk management[4]

1.4 The relationship between risk management, internal control and governance

Risk management and internal control are concepts that are frequently mentioned in conjunction. The concepts are often perceived too narrowly and separately to one another. Risk management is more than the analysis and reporting of downside risk, and internal control concerns the management of an enterprise and is therefore not limited to specific control activities.

The American foundation "*The Committee of Sponsoring Organizations of the Treadway Commission"* (COSO) provided a definition of internal control which was first published in 1992 and has received broad international acceptance. The original document was revised in 2013[5]. The same foundation also provided a definition of ERM in 2004[7]. This latter document is currently being revised and a new updated version is expected in the course of 2017.[6]

Definition of internal control	Definition of ERM
Internal control is a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting and compliance.[5]	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.[7]

Figure 3 COSO definitions

A comparison of the two definitions shows that there is a high degree of overlap between the two. Internal control may be looked upon as the consequence or a sub-process of ERM. This sub-process can be defined as the sum total of management and control mechanisms.

ERM means taking a holistic perspective, not just of the enterprise's status at a given moment, but also probable positive and negative developments in the future. In this way it becomes a tool for the balanced prioritisation of resource utilisation. For this reason this work should also be harmonised with other management activities such as performance scorecards.

The holistic focus within an overall goal of value creation is even more clearly expressed in the proposed new definition of ERM in the proposed update to the COSO ERM document[6]:

"The culture, capabilities, and practices, integrated with strategy-setting and its execution, that organizations rely on to manage risk in creating, preserving, and realizing value."

ERM contributes to value creation via reduced sub-optimisation as well as a reduction of uncertainty related to future cash flow.

2 THE RISK MANAGEMENT FUNCTION – IMPORTANT PRINCIPLES

2.1 The function's tasks and responsibility

In these Guidelines we have used the expression the "Risk Management function". This does not necessarily refer to there being one person, or one fixed group of people totally dedicated to these tasks, rather and more importantly Risk Management tasks represent a systematic and objective approach to identifying, analysing and evaluating risk as well as designing and implementing activities which will allow risk to be managed within defined risk parameters. In addition the tasks shall provide input to strategy and development plans.

In an enterprise it will be the Board or the highest decision making body that will ensure that the enterprise has established adequate risk management and internal controls. In accordance with the requirements of the Norwegian Code of Practice for Corporate Governance issued by the Norwegian Corporate Governance Board (NUES[8]) this responsibility encompasses amongst others the following:

- The board of directors must ensure that the company has sound internal control and systems for risk management that are appropriate in relation to the extent and nature of the company's activities. Internal control and the systems should also encompass the company's corporate values, ethical guidelines and guidelines for corporate social responsibility.

- The board of directors should carry out an annual review of the company's most important areas of exposure to risk and its internal control arrangements.

- The board of directors must provide an account of the main features of the company's internal control and risk management systems as they relate to the company's financial reporting.

The Chief Executive has overall operational responsibility for risk management. In their daily tasks all managers shall ensure that there is adequate risk management and internal control within their areas of responsibility in line with the organisation's overall objectives.

The Risk Management function shall assist the organisation in its work in designing and implementing efficient and effective processes to identify, analyse and treat risk. In addition the Risk Management function has a standalone responsibility to monitor the risk profile and to flag developing trends for existing risks and the potential consequence of new threats/opportunities – so called "emerging risk".

The Risk Management function should have responsibility to monitor and review the performance of risk management tasks taken as a whole, and to assist line management in communicating relevant risk information to a higher level in the organisation and to external parties. The function shall:

- Make operational *guidelines* for risk management, defining roles and responsibilities and establishing goals for the implementation of the risk management tasks. Risk management tasks should be integrated with the organisation's strategy work.
- Prepare a *framework* for risk management encompassing the whole organisation, and where necessary addressing specific processes, functions or departments of the organisation.
- Promote risk management *knowledge* throughout the organisation.
- Establish a common risk management terminology (e.g. in respect of risk categories and concepts applicable to probability and impact assessment).
- Choose model / tool for the identification, scoring, evaluation and monitoring of risk including emerging risk.
- Assist management in the development of risk reporting and monitor the risk reporting process, including establishing a system for early warning flags or a trigger system for breaches of the organisation's risk appetite or risk limits.
- Ensure ongoing communication with the Chief Executive and the Board based on an independent and qualified evaluation of risk management and ensure that decisions are operationalised.

The Risk Management function shall lay the groundwork for and monitor the implementation of:

- Effective risk management principles for Executive Management and assist risk owners[9] in defining planned risk exposure.
- Communication of risk related information to the organisational, including making expert pronouncements.
- Reporting lines that ensure that risk related information is communicated to the right organisational level at the right time and that this communication is in an understandable and balanced format. The Risk Management function should be involved at the outset to ensure that *risk evaluations* form a part of all major decisions whilst at the same time, and when necessary, influencing and challenging decisions which may cause material risk.

In addition the Risk Management function shall monitor that the above-mentioned processes are performed in practice and react if the situation should arise that these are inadequate.

In addition to a centralised Risk Management function (which is part of the second line of defence) some organisations have established a separate Compliance function to monitor risks related to breaches in legal regulations and internal and external regulations (including fraud risk). The Compliance function will normally report directly to Executive Management. There is a presumption that the Compliance and Risk management functions work closely together, especially in respect of the areas of legal risk, reputation risk, establishment of a sound risk culture and monitoring of ethical guidelines.

Other specific review and monitoring functions can be found within the areas of Health, Safety and Environment (HSE), procurement and Quality/ Continuous Improvement. In connection with the latter area it should be noted that the updated standard for Quality Management ISO 9001:

2015 requires to a greater extent than before (ISO 9001: 2008) a risk-based approach to the design of an effective Quality Management system.

Risk management encompasses the managing of both financial and operational risk (including for example risk related to internal processes, systems, human behaviour and other aspects of the organisation). Other relevant risks can be related to Compliance with laws, regulations and ethical standards (compliance risk), environmental risk etc. as well as the handling of external risk factors such as, for example, political risk, macroeconomic factors or catastrophe scenarios.

In short ERM entails using a systematic approach to facilitate the organisation's ability to realise its objectives through organisational structure, business processes, control activities and decision making.

An important task for the Risk Management function is therefore to ensure that objectives are adequately communicated amongst the various control environments and grounded in these (cf. figure 4). Furthermore it is important to ensure that information from these environments is taken into account and included as a part of the work with ERM.

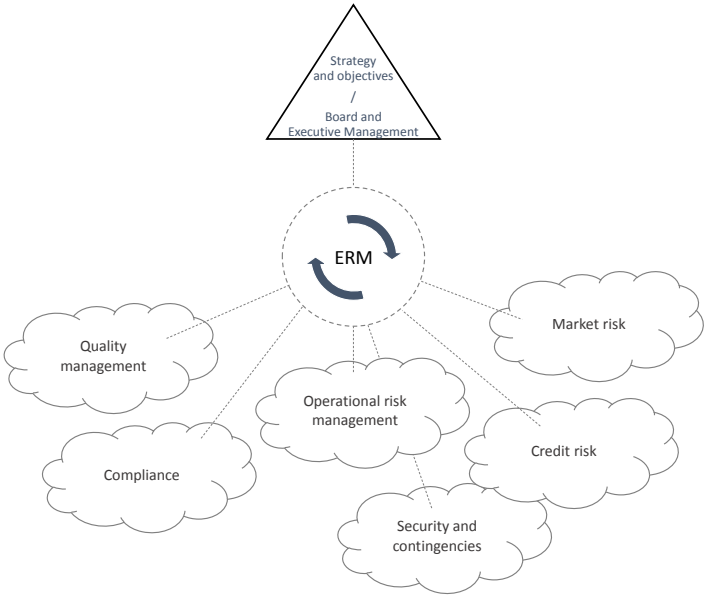

Figure 4 Example of the ERM coordinating role and the management of various risk areas

2.2 Risk appetite

Risk appetite expresses the level of uncertainty an organisation is both willing and has the ability to take on in order to carry out its activities and realise its goals. Risk appetite may be defined qualitatively or quantitatively in terms of limits to authorities and exposures applicable to the various risk types. Risk appetite will vary from organisation to organisation dependent on strategy, industry and organisational culture. In addition legal requirements such as the Company Act's requirements for minimum equity will influence risk appetite.

It is important that defined risk appetite can be translated into operational practice. There should be a common thread going through an organisation's various objectives, management limits, authorities and scope of action which accords with the total risk appetite and strategy. In those organisations where it is difficult to quantify risk appetite it is especially important to devise suitable guiding principles delineating who as a decision maker can decide what should be the acceptable level of risk based on the relevant qualitative evaluations.

Risk appetite has both an aspect of desired situation and capability. The expression should not be confused with the expression "risk tolerance" which may be defined as an absolute limit to the level of risk an organisation can take.

2.3 "Risk gaps"

"Risk gaps" is an expression which is often used to describe the imbalance that can arise between actual risk exposure and expected return on investment (including societal gains). This can especially be seen where the probability for a given event is low, but the impact is high. An important task of the Risk Management function is to identify such gaps and ensure that these are communicated to Executive Management and the Board.

2.4 The Board's responsibility and communication with the Board

The Board is responsible for the organisation being managed in accordance with applicable laws and regulations and to ensure that sound risk management is established in the organisation. In the Norwegian Code of Practice for Corporate Governance this is expressed in the following way: *The board of directors must ensure that the company has sound internal control and systems for risk management that are appropriate in relation to the extent and nature of the company's activities*[8]. The Board must make clear demands on the Risk Management activities to ensure that all risks which influence the achievement of objectives are treated satisfactorily. In addition the Board must set the organisation's risk appetite/tolerance levels[i].

It is preferable that the Head of the Risk Management function has the possibility to report directly to the Board. This can be organised in various ways for example the Head of Risk Management may have a direct reporting line to the Board, or to a Risk or Audit Committee of the Board. The objective of this reporting line is to ensure that, if required, there is the possibility for an independent reporting to the Board in respect of the organisation's risk profile.

i The limit to the amount of risk an organisation is willing to take (appetite) or has the ability to take (tolerance).

2.5 Grounded in the Executive Management

The Chief Executive is responsible for the establishment and performance of sound risk management and internal controls within a clear mandate, within the framework of the guidelines and risk appetite which the Board has approved. This responsibility applies also to situations where risk appetite is difficult to quantify.

The organisation, responsibilities, activities and authority of the Risk Management function should be determined by a description of the function which should be approved by the organisation's Executive Management. The following are the main elements that should be described:

- Organisational position, interaction with and segregation of duties from other control functions and line management.
- Mandate and resources which match to the responsibilities, tasks and authority.
- Access to information.
- Reporting responsibility.

2.6 Risk management, Executive Management and decision making

Risk management and decision making are interconnected. When making any major strategic decision Executive Management should require a set of scenarios to be presented detailing impact and alternative actions especially in the situation where there may be a high level of uncertainty. Figure 6 describes the relationship between risk management and decision making, in the situations where active use is made of risk management.

Decision maker	Outcome properties	Outcome
Decision maker belongs to the organisation Example: Drinking a cup of coffee	Deterministic	Known and sure – the coffee cup is empty
Decision maker belongs to the organisation Example: Estimation of future students in district X	Stochastic affected by randomness	Probability of the outcome is known/ guessed
Decision maker belongs to the organisation Example: Introducing a new product to a new market (first-to-market)	Stochastic	Probability distribution is unknown
Outside decision maker – partly perceived by «what if» scenarios («known unknowns») Example: Riots	Cascade-, snowball effects, «fat tailed distribution»	«Grey Swan»
Outside decision maker – unknown event comes by surprise («unknown unknowns») Example: 9/11	Probability not computable by known techniques. Not perceived by «what if» scenarios	«Black Swan» 

Figure 6 Decisions and outcomes

This illustration was originally published in "Y. Ayse B. Nordal, Risk Management Practices, Decision Making and Corporate Governance, Book of Proceedings", International May Conference on Strategic Management, University of Belgrade, May 2015.

Enterprises, institutions and individuals will be affected by both their own and others' decisions. The common element of these is that there is uncertainty attached to the outcome of a decision. There are very few decisions which have a «certain» outcome, i.e. are deterministic. An example of a deterministic outcome can be the decision to drink a cup of coffee. Under normal conditions we can foresee that the coffee cup will be empty if the decision to drink the coffee is fulfilled.

However both *normal conditions and deterministic outcomes* are rarities. In many cases the decision maker in an organisation makes up his/her mind by estimating the uncertainty with reference to probability distributions based on historical data, comparable data or previous experience regarding variables that may affect the outcome. As an example we can consider a decision maker in district X who needs to determine how many school places will required in the district over the coming years. Historical data which will affect school places can be analysed for example in the areas of population trends and movement into and out of the district. On this basis it is possible to estimate a probability distribution for the effect of the known factors, which have been shown to be significant in experience to date.

For a number of decisions it is not possible to determine the factors which may affect the outcomes and it is therefore not possible to use probability distributions. An example may be an enterprise which is "first- to- market" in a new market with a completely new product. In this case there is no historical data regarding sales volume and there may be few comparable metrics which can be used as a basis for calculations. The enterprise simply does not know with any degree of certainty the probability distributions of relevant factors.

From time to time, organisations will face "outcomes" even when they were not responsible for or have participated in the decision making. The organisation may envisage *a possible outcome,* and this may be realised now or in 100 years[ii] . The organisation may prepare itself for such events by scenario exercises performed in connection with contingency planning.
Moreover organisations may also be affected by an event where it is not possible to foresee the outcome even through standard scenario analysis. The literature concerning «Black swans»[10] describes this type of event. The event, the outcome and relevant variables are completely unknown to the organisation.

ii Such events e.g. a riot may have snowball effects leading to a characteristic "fat tail" distribution, which describes a higher than expected chance of an extreme outcome.

3 ORGANISATION AND SEGREGATION OF DUTIES

3.1 The three lines of defence

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, avoid 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 in figure 5) provides a high level overview of the roles and responsibilities for internal control and risk management. Even in organizations 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.

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).

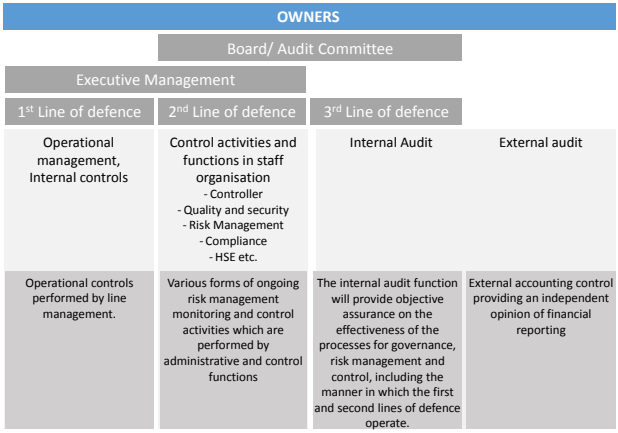

Figure 5 Description of the three lines of defence

The first line of defence owns and manages operational risk, and must therefore ensure the adequacy of internal control performed by employees in this line, e.g. sales people, clerical staff and other such functions. Line management has responsibility for maintaining an effective internal control. This will entail ownership of and responsibility for risk management and risk treatment. The daily operational control activities are typically performed by staff in this line within limits established by operational management. Executive Management is responsible for establishing various controls and monitoring functions to contribute to the development and/ or monitoring of controls to be performed by employees in the first line.

The second line of defence has a role which is both proactive and reactive. On the proactive side the second line contributes to the development and performance of, for example, the framework for risk management, management and decision making principles as well as the development of activities in the first line.

On the reactive side the second line shall monitor reports and maintain a dialogue with the organisation. The objective of this work is to identify matters deviating from the desired development and ensure that the organisation focuses on and reacts to these issues.

The support and control activities in the second line are, for example, performed by Finance, Compliance, Risk Management, Health and Safety, Legal and Quality Management. The specific functions will vary by organization and sector.

The third line of defence is performed by internal audit, and provides governing bodies and Executive Management with a greater degree of independent and objective assurance than the second line of defence regarding the design and operation of internal controls. Internal audit can, among other things, evaluate whether the organisation's processes for governance and control are effective and whether internal controls function as intended, including whether the first and second lines of defence are working efficiently and effectively, and are contributing to the organization's achievement of its goals. The third line of defence gives an independent evaluation of risk management to the organisation's highest authority.

In addition to these three lines of defence the external audit will provide an independent confirmation of the financial reporting.

It is important to be aware that the functions of the second and third line of defence should act independently of the units they monitor and control. In other words, they should not perform tasks that are the responsibility of the first line, rather they should verify and monitor that the tasks are performed in accordance with external and internal rules and regulations. A well-developed risk management system will also form a sound basis for internal audit's independent risk assessment.

Clear mandates and job descriptions are important for being able to distinguish the different functions one from another as well as their areas of responsibility. Management should assess and consider the positioning of the various functions within the organisation.

3.2 The position of the Risk Management function in the organisation

The Risk Management function's organizational positioning will vary dependent on the characteristics of the organisation and its maturity level in respect of ERM. Many frameworks recommend that the Risk Management function shall report to Executive Management without specifying its positioning in greater detail.

In some organisations the Risk Management function is organised into its own separate unit reporting to the Chief Executive on a par with other administrative functions. Other organisations have positioned the function together with other risk and control functions for example in the finance department reporting to the Chief Financial Officer, or together with the Compliance function. In smaller organisations the responsibility for risk management tasks may be included in another role description for example that of the Chief Financial Officer.

These examples show that there is no one right answer as to where the Risk Management function should be positioned in the organisation. Before deciding where the Risk Management function should be positioned Executive Management should assess what will be the function's areas of focus, what milieux the Risk Management function will interconnect and can therefore achieve synergies and professional co-operation with, and what position in the organisation will lead to the Risk Management function exercising its responsibilities in a satisfactory manner.

3.3 Mandate, authority, competency and resources

The organisation should appoint one person with the overall responsibility for the Risk Management function. That person and all people performing tasks within the Risk Management function must amongst others understand the organisation's business concept, strategy, market and operating parameters. Ideally this should be combined with ensuring that some of the employees in the risk management area also have detailed knowledge of the organisation's various processes, products and systems. For all risk management positions requirements should be stated relating to experience and competency.

Responsibility should be placed at a suitably senior position in the organisation in order to ensure the required level of authority and access to key decision makers. The function should be assigned a budget, framework conditions, and the necessary mandate in order to keep its staff up to date ensuring the necessary access to knowledge and skills development. The assessment of required resources should make allowance for an appropriate buffer allowing for the taking up of ad hoc tasks and the offering of professional advice.

3.4 Independence and integrity

People employed in and responsible for the organisation's Risk Management function, should as far as possible be organised independently from operational activities. This should not preclude employees with risk responsibility (the Risk Management function) from informing about and reinforcing requirements as well as preparing decision proposals which affect the business operations. It is however a prerequisite that the function does not perform or have responsibility

for operations, or make decisions which affect the business operations. Persons employed in the Risk Management function shall equally not work in units that they themselves are responsible for monitoring.

Some small organisations will not be in a position to establish a separate position for working with risk management. In such circumstances it is important that the function description addresses the issue. A mix of roles may weaken the Risk Management function's independence. The starting point should be that the organisation should have at its disposal sufficient resources to ensure a well-functioning and independent Risk Management function. The function may draw on operational resources to manage tasks so long as this does not compromise the requirement of independence.

Employees working in the Risk Management function must possess, in addition to a relevant professional competency, a high level of professional integrity, and in the case of the function head, authority and experience at taking responsibility for the development and communication of the risk management framework. This professional integrity is decisive to achieve confidence in the function and the function's value. Integrity is perceived through the fairness, care and responsibility put into the tasks performed. Integrity can be compromised through biased, unethical and illegal acts. Employees in the Risk Management function shall respect and contribute to the organisation's legitimacy and ethical objectives. Key prerequisites to ensure legitimacy and integrity are a mandate that is grounded at the Board and Executive Management level which defines clearly the Risk Management function's responsibilities and tasks, as well as an organisation, access to information and reporting that supports this mandate.

3.5 Access to information

The Risk Management function should have access to the required information regarding the company's operations and its decisions. This can with advantage be defined in the function description and include for example access to computer systems, governing documents, physical property, personnel and documents from governing bodies. In addition, the Risk Management function should have the right to participate in internal meetings, as and when necessary, in order to be able to perform reviews and monitoring of activities in a satisfactory manner.

3.6 Remuneration and incentive system

The organization should establish a remuneration and incentive system that ensures the function's independence. The remuneration and incentive system for the Risk Management function should not contain significant performance-based components that could lead to conflicts of interest and influence the objectivity of the staff working in the function. Furthermore, remuneration should be at a level that makes it possible to employ individuals possessing the necessary competence and seniority.

3.7 Reporting requirements

Irrespective of how the Risk Management function is formally positioned in the organisation it should have a requirement to report to the Board and Executive Management with a regularity agreed with the governing bodies. The function should also be able to provide ad hoc reporting to the Board as and when required.

In order to ensure a well-functioning Risk Management it is necessary that centralised as well as de-centralised Risk Management functions are positioned at the "senior management" level, that the employees have sufficient experience combined with both a professional and personal authority.

3.8 Outsourcing the function

If management chooses to outsource all or part of the Risk Management function, it must ensure that the fundamental requirements of a Risk Management function are safeguarded. It should be noted that specific legislation may limit the possibility of outsourcing. Such use of outsourcing is most usual at the commencement of the process to establish ERM, until such time as the organisation has built up a common language, risk culture and a well-functioning framework for risk management.

4 PRACTICAL APPROACH TO DEVELOPING RISK MANAGEMENT IN AN ORGANISATION

4.1 Framework and standards

There are two relevant standards/ frameworks which are internationally accepted (and have also been translated into Norwegian). These are:

1. ISO 31000:2009 - Risk Management – Principles and Guidelines[11]

ISO 31000 Risk Management – Principles and Guidelines is an international standard structured according to a description of principles which describe eleven characteristics of risk management. It consists of a five part framework (mandate and commitment, design of framework for managing risk, implementing risk management, monitoring and review of the framework, and continual improvement of the framework), as well as a six part generic process description (establishing of context, risk identification, risk analysis, risk evaluation, risk treatment and monitoring and review).

This International Standard is intended to meet the needs of a wide range of stakeholders, including:

- Those responsible for developing risk management policy within their organization
- Those accountable for ensuring that risk is effectively managed within the organization as a whole or within a specific area, project or activity
- Those who need to evaluate an organization's effectiveness in managing risk
- Developers of standards, guides, procedures and codes of practice that, in whole or in part, set out how risk is to be managed within the specific context of these documents.

The standard underpins a disciplined decision making process in respect of risk and return which contributes to the organisation's achievement of planned results. The standard provides

the principles and guidelines for managing any form of risk in a systematic, transparent and credible manner and within any scope and context.

2. COSO: 2004 Enterprise Risk Management - Integrated Framework[7] (currently being updated[6])

In a previous chapter of these Guidelines concerning risk management and internal control it was explained that COSO has published a framework for ERM which build further on the framework for internal control. In COSO ERM organisations are recommended to introduce ERM to achieve a better connection between risk monitoring and the development and protection of the organisation's value creation. It defines ERM as "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."

Furthermore it states that ERM "consists of eight interrelated components. These are derived from the way management runs an enterprise and are integrated with the management process."
These eight components are:

- Internal environment
- Objective setting
- Event identification
- Risk assessment
- Risk response
- Control activities
- Information and communication
- Monitoring.

Enterprise risk management is not strictly a serial process, where one component affects only the next. It is a multidirectional, iterative process in which almost any component can and does influence another.

These components are analysed in relation to achieving an entity's objectives set forth in the following four categories which apply to the whole organisation and at all organisational levels:

- Strategic
- Operations
- Reporting
- Compliance.

COSO accepts that there may be different ways to reaching the goals but because the framework is based on leading practice as well as the development of consistent terminology and approaches it is believed that it can be used by an organisation as a means to achieving its objectives.

4.2 Designing a framework in practice

A common denominator for the current standard and framework is a definition that risk management encompasses methods and processes used by organisations to manage risks and exploit opportunities.

A *framework* for risk management will typically include the following elements:

- Identification of internal and external matters which influence an enterprise's achievement of objectives
- Determination of risk appetite and risk management policy
- Design of the Risk Management function and organisation as well as areas of responsibility
- Establishment of internal and external communication and reporting structures
- Allocation of resources to the function.

Based on this there arises therefore a need to establish a process for risk management which will typically consist of:

- The identification of specific events and significant matters affecting the organisation's achievement of objectives (threats and opportunities)
- The analysis and evaluation of specific events and significant matters based on probability and impact or the modelling of future outcomes through the use of other statistical methods
- Choice of strategy for risk treatment as well as the implementation and monitoring of performance.

Through the identification and proactive evaluation of threats and opportunities an organisation can protect as well as create value for its stakeholders, including owners, employees, customers, regulators and society in general. This includes external risk (related to regulation, reputation etc.), strategic risk (an inherent part of the decision making process), financial risk, compliance risk and operational risk. As a result of amongst other things the globalisation of business the risk of contagion between companies and markets (systemic risk) and dependencies between various risks have become important elements that must be addressed in the risk management process.

As a key element of the management structure in an enterprise, ERM contributes to protection of value and improving decision making processes by establishing acceptable levels for risk appetite and by grounding risk management in the business planning and management processes. When risk management is grounded in the organisation it becomes a part of its culture.
The basis for sound risk management is that all parts of the organisation are responsible for the treatment of risks within their areas of responsibility. However risk management shall be practised according to an integrated, enterprise-wide approach in order to achieve accordance with the organisation's objectives and strategy viewed as a whole.

Key elements related to **risk management:**

- The organisation defines its risk strategy and appetite. The Chief Executive appoints a Risk Manager or related position. Risk owners[9] are identified for all significant risks.
- Risk owners[9] determine meaningful and measurable objectives and control mechanisms which are accepted throughout the organisation.
- A centralised Risk Management function is responsible for establishing and maintaining the risk management processes. It provides the organisation with a formal risk management framework and appropriate training programmes aimed at improving the risk management culture and promote a common risk terminology and concepts applicable to the whole organisation.
- Executive Management regularly reviews reports showing the development of significant risks as well as the status of actions taken to treat risks. Management provides the Board and if appropriate the Audit Committee with regular relevant, comprehensive and timely information.
- Critical, new and emerging risks are brought to the attention of the appropriate level of management as soon as they are identified.

4.3 12-point plan for the implementation of risk management

For those considering implementing risk management in their organisation we recommend the following plan of action:

1. Prepare a mandate for the function and define the role in the organisation as well as reporting lines. Ensure the Risk Management function has support and understanding at the Executive Management and Board level.
2. Appoint a Head of Risk Management with the appropriate experience and competency. Ensure there is provision of resources to build a function that has the required level of integrity.
3. Approve a policy for the implementation of risk management, including the framework to be used, responsibility and reporting. Evaluate the need to buy/ develop a support system for risk and enterprise management which can facilitate the establishment of the entity's risk profile and the management of risks.
4. The ERM function should encompass all types of risk including operational and financial risks, political risk, regulatory risk etc. The function should focus on actions taken to treat risks e.g. insurance coverage and «business continuity management».
5. The Board and Executive Management defines risk appetite and describes how an organisation can ensure that risks are kept within agreed parameters and where relevant upper and lower limits.
6. Communicate the implementation plan to the organisation and perform risk evaluations. Decide on the principles for the management and measurement of risk.
7. In order to retain and, not least, recruit employees to work in the risk management area it is important to put in place a career path which makes clear that this is a profession with specific requirements to education and experience, as well as describing a development path.
8. In larger organisations it may be effective to establish also Risk Management positions in the first line in addition to a centralised function which is concerned with the enterprise seen as a whole (the ERM function).

9. Perform regular communication of the status of risk exposure, risk appetite, risk evaluations and any emerging risks as well as changes to existing risk profiles.
10. Risk communication should as far as possible be pro-active and it is important that all risks have an owner.
11. A structure should be established to ensure that the centralised risk management unit works closely with the strategy function and business management.
12. Report annually to the Board and plan activities for the following year.

4.4 Reasons for failure in the establishment of ERM

As time passes experience has been gained both nationally and internationally in respect of what functions and what does not function. Some of the elements that have had greatest negative impact are, in our opinion, the following:

- Lack of clarity in vision and common values as well as badly formulated strategies and objectives which in turn lead to lack of co-operation and focus in the organisation.
- Lack of a link between strategic objectives and risk management.
- Imprecise mandate leading to lack of understanding of the role of the Risk Management function and the division of responsibilities.
- The Head of Risk Management does not possess competency in risk management, strategy and the wider picture so that he/ she is not able to take on the role of advisor and challenger.
- The Head of Risk Management does not understand the business.
- The risk management concepts are not understood or are misunderstood.
- Lack of ownership of the system tool used.
- A tool is used without understanding its weaknesses and limitations.
- Discussion is not encouraged, no effort is made to promote an honest and open evaluation of risk – "nobody should risk having their head cut off for telling it as it is".
- Lack of prioritisation of significant risks.
- Lack of understanding/ knowledge of correlation between risks.
- Lack of management/ monitoring of IT risk.
- Lack of focus on change in the risk profile and emerging risks.
- The organisation is not convinced of the value of risk management efforts resulting in a lack of commitment.
- The organisation and responsibility is unclear between the Head of Risk Management and the risk owners[9].
- Work performed by the various control functions is uncoordinated.
- There is damaging competition/ professional rivalry between the Head of Risk Management and related functions e.g. Quality Management, Compliance and Internal Audit
- Poorly performed risk evaluations lacking documentation of the underlying criteria for the evaluations so that Executive Management loses confidence in the accuracy of the risk profile presented.
- Lack of quality assurance measures in respect of analyses/ evaluations.
- Lack of a holistic view to reporting where differing formats for risk evaluations hinder aggregation at a higher level.

Always bear in mind it is not the form that is important but the substance!

Network Risk Management plans to develop further professional documents (white papers etc.) which can exemplify practical approaches to risk management tasks as well as arrange courses/ seminars in this professional area for further information see the home page of IIA Norge www.iia.no as well as Network Risk Management's own web page.

IIA Norge publishes twice a year "SIRK" which is professional magazine for the areas of Governance, Internal Audit, Risk Management, Compliance and Control. The magazine has some articles in the English language. It is possible to register to receive a printed copy by contacting IIA Norge and a pdf-version is available for download free of charge from the web page of IIA Norge.

End notes

1 The term "Compliance" is used to describe the function for control of conformity with laws as well as external and internal regulations – cf. further the Guidelines for the Compliance function published by IIA Norge in 2015.

2 The word enterprise when used in these guidelines is meant to apply to any organisational activity (including public sector and not-for-profit) and not exclusively an organisation dedicated to commercial purposes.

3 "Board" is used throughout these Guidelines to describe the highest decision-making body of the organisation

4 http://onlinelibrary.wiley.com/doi/10.1111/risa.12375/full

5 Internal Control – Integrated Framework, May 2013 http://www.coso.org/.

6 Enterprise Risk Management – Aligning Risk with Strategy and Performance – call for public comment closed 30th September 2016 http://www.coso.org/.

7 Enterprise Risk Management – Integrated Framework, September 2004 http://www.coso.org/.

8 Norwegian Code of Practice for Corporate Governance issued by the Norwegian Corporate Governance Board Norsk (NUES) 30th October 2014.

9 A risk owner has responsibility for the profits and losses associated with the defined risk.

10 Nassim Nicholas Taleb, The Black Swan 2007, Random House.

11 https://www.iso.org/

IIA Norge
Postboks 1417 Vika, 0115 Oslo
Office address: Munkedamsveien 3B, 3. etg.
E-mail: risikostyring@iia.no
www.iia.no/risikostyring

Guidelines for the Risk Management function