IIA Norge

# ERM – guidelines for the risk function

2025

# Governance

The combination of processes and structures implemented by the board to inform, direct, manage, and monitor the activities of the organization toward the achievement of its objectives.

In corporate governance, risk management, compliance and internal audit are important elements, which together can contribute to good governance and value creation.

## Risk management

A process to identify, assess, manage, and control potential events or situations to provide reasonable assurance regarding the achievement of the organization's objectives.

## Compliance

Adherence to laws, regulations, contracts, policies, procedures, and other requirements

## Internal auditing

An independent, objective assurance and advisory service designed to add value and improve an organization's operations.

# Contents

# About these guidelines

The need to establish an Enterprise Risk Management function (hereinafter Risk function) manifests itself in all organisations both in the public and private sectors, irrespective of the organisation's size, type of activity and complexity. The key drivers for establishing a Risk function will accordingly also vary according to the context such as business sector, and the type of operation and organisation.

Typically, these drivers have arisen from the need to implement management and control in those areas which have experienced in the past, and may experience in the future, significant financial losses, physical damage, violation of individual rights, poor health and safety performances or loss of human life. Because of the potential social and economic impact of such events it is also common for external regulators to make specific demands on the organisation, structure and performance of risk management activities, additional to the good practice recommendations described in this document.

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, some national statutes will require the establishment of a Risk function as an essential element of sound governance.

In this guidance, we outline "good practices" for the Risk function regardless of industry, regulation and size. It does not cover legal or regulatory requirements; rather it introduces the basic principles of the function. Each organisation needs to make individual adaptations depending on its nature, size, complexity and organisational culture.

The guidance delineates the organisation of a Risk function, responsible for the overall risk management in an organisation. This includes the segregation of roles and responsibilities between the different control and assurance functions of an organisation, such as internal audit, the Risk function and the Compliance function.

Several industry-specific guidelines have been developed internationally which describe the elements and requirements characteristic of an efficient and effective Risk function adapted to specific regulatory requirements. There are however common elements in these, which, together with the experience of Norwegian organisations, forms the basis for this guidance.

Risk management must take place at all levels of the organisation. Hence, whilst the focus in this guidance is on ERM, the principles are also valid for those working with risk management within more defined, specialised areas of an organisation.

## Concerning the 2025-edition

The guidelines were first published with the title «Guidelines for the Risk Management function" in 2017 originally in Norwegian but with a translation to English. In 2018 it was updated to take account of changes in the framework for COSO ERM and an update of ISO-standard 31000:2018. In 2020 a «Good Practice Guidelines for the Enterprise Risk Management Function» was published based on the English translation of the Norwegian guidelines. This was adjusted and developed further by a steering group appointed by IIA-associations in the Nordic and Baltic countries.

This edition builds further on the 2020 version but was expanded and adapted to the work performed in 2024 by IIA Norway on standardising Norwegian professional terms regarding corporate governance. The decision was also made to remove the professional appendices from the main document and make these available as standalone white papers. Thereby making it easier to update and expand the number of white papers.

## Contributors

IIA Norway expresses its gratitude to the following members for drafting the original guidelines and some later updates:

- Ayse B. Nordal, Nordal visjon
- Martin W. Stevens, Gjensidige
- Ole Martin Kjørstad, BDO
- Petter Kapstad, Equinor

We also thank representatives from IIA Associations in Denmark, Estonia, Iceland, Latvia and Lithuania, as well as risk management associations in Finland, Latvia and Lithuania for their contributions.

# Executive summary

Enterprise Risk Management (ERM) is widely recognized as an essential component of good corporate governance and value creation.

ERM involves a systematic and objective process that includes:

Identifying potential risks

Analysing and evaluating those risks

Designing and implementing measures to manage risks within defined risk parameters

These activities aim to improve the quality of decision making and ensure risks are managed effectively across the organisation.

To achieve consistent and holistic risk management processes, it is essential to have a dedicated role or function responsible for these efforts.

These guidelines delineate key criteria that guide the establishment of such a function:

1. Risk management is a line management responsibility
2. The Risk function ensures the integration of risk management into decision-making at all levels of the organisation
3. The Risk function maintains transparent communication with executive management and the Board as well as with other control and assurance functions
4. The Risk function has a clearly defined mandate
5. Risk employees should operate independently, have no operational responsibilities, and demonstrate professional integrity.
6. The Risk function should have access to all information relevant to the performance of its activities.
7. The Risk function's remuneration should not contain significant financial performance-based components that could lead to conflicts of interest and influence the objectivity of the employees working in the function
8. Remuneration in the Risk function should be sufficient to attract and retain employees of sufficient seniority and professional and business knowledge.

# Chapter 1: Enterprise Risk Management defined

## 1.1 The concept of risk

The taking of risk is a natural part of running any organisation, however often risk is not explicitly mentioned in the formulation of business decisions. The term “risk” has often been exclusively associated with unwanted events, and “Risk management” as analysing and restricting the probability and impact of undesirable events. This is only one dimension of the total picture. Evaluating positive outcomes – or the upside - is just as important a part of ERM as is evaluating negative outcomes – or the downside - because ERM is concerned with the whole picture and evaluating risk strategy in relation to a portfolio of risks. In these guidelines, the term “risk” shall be understood as referring to “The positive or negative effect of uncertainty on the organisation’s ability to achieve its objectives at every level”.

## 1.2 Enterprise Risk Management (ERM)

Risk management is a process to identify, assess, manage, and control potential events or situations to provide reasonable assurance regarding the achievement of the organization’s objectives at every level. This means that both risk management and strategic efforts will be performed as integrated and repetitive processes. It is a question of ensuring both the achievement of objectives as the enterprise develops and the appropriate management of the organisation’s assets, including human resources, reputation and the avoidance of losses or waste as the result of adverse events.

ERM encompasses matters occurring at all levels of the organisation. ERM must therefore be an integrated part of strategic activities. A further pre-requisite for being able to exercise sound risk management is therefore the existence of 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 support the enterprise’s overall strategy.

In practice, this means that ERM should provide the best possible basis for decision making at the various levels of the organisation, so that the decisions made support 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.

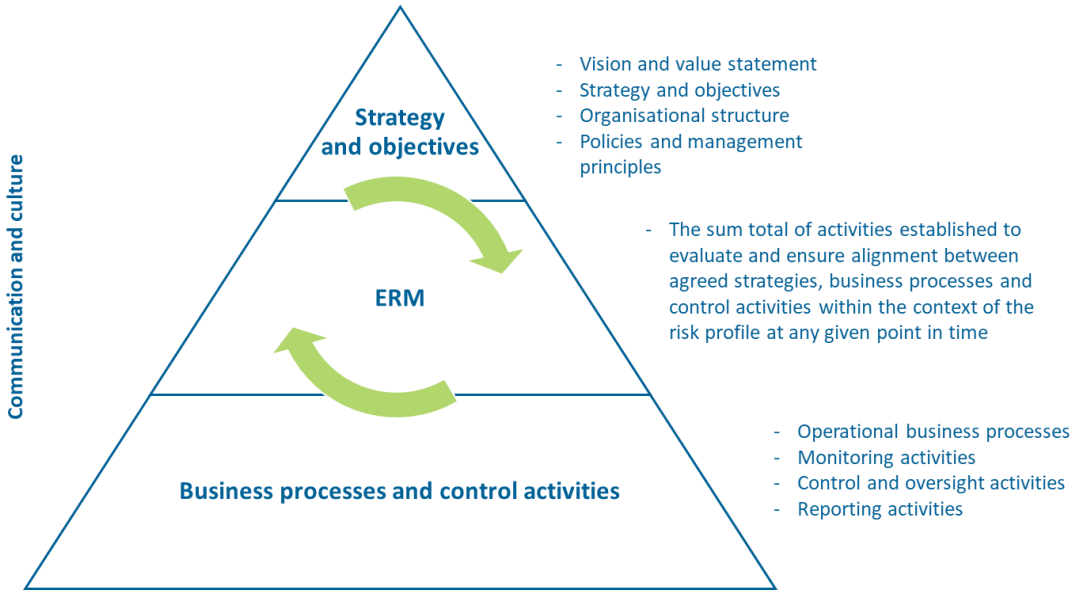


**Figure 1:** The interrelationship between ERM and governance. Source: IIA Norway

## 1.3 More about risk management

Risk management is defined as systematic, co-ordinated, pro-active, post-active and ongoing activities which direct and control an organisation with regard to risk.

This includes amongst other things the organisation's ability to:

- Influence the likelihood of the positive or negative impact of events
- Understand/exploit the correlation between various risk types
- Proactively initiate activities which steer development in the required direction
- Reactively mitigate the consequences of negative events and optimise the consequences of positive events
- Build a culture which enables every employee to make simple and complex risk-based decisions contributing to action being taken and the sound risk management of strategic objectives.

This presupposes the application of a holistic perspective across all governing bodies, organisational units, functions, processes, duties and risk categories (strategic, financial, operational and other risks) thus avoiding "silo" thinking and sub-optimisation.

To summarise, risk management is about providing the best possible basis for decision making and facilitating the effective implementation and monitoring of those decisions. This includes also raising awareness of what is the acceptable risk level and necessary risk exposure.

## 1.4 The benefit of risk management

All organisations, whether in the commercial or public sector experience uncertainty in

relation to future development. This uncertainty is the definition of risk. The choice is therefore between whether to attempt to consciously manage future development in a positive direction (manage the risk) or abdicate responsibility for influencing future development, thus leaving it purely up to chance.

This is also seen in our private lives where we have to make conscious decisions to choose fully comprehensive or third-party vehicle liability insurance, fixed or floating mortgage rates or charge at the closing doors of a carriage in order to avoid waiting for the next service. Most of us will want to weigh up the best choice to make, not only in theory, but also based on previous experience, available information and discussion with, amongst others, advisors, family and friends. For example, you may decide to give weight to having experienced a market with 15% mortgage rates or having witnessed an accident when somebody rushed the doors of a carriage.

A conscious framework for sound risk management is therefore something all people and organisations can derive benefit from, not just commercial companies and financial institutions. An example from Norway was when the country's major oil company, Equinor, took the initiative to assist the skiing federation to formulate its risk profile by analysing the organisation's value drivers. The conscious management of risks will contribute positively to preserve and create value, making people and organisations better equipped to meet current and future challenges.

## 1.5 The relationship between risk management, internal control and governance

Risk management is a process to identify, assess, manage, and control potential events or situations to provide reasonable assurance regarding the achievement of the organization's objectives. Control processes, often shortened to "internal control", are the policies, procedures, and activities designed and operated to manage risks to be within the level of an organization's risk tolerance. From these definitions it is possible to consider internal control as an element or subprocess of risk management. Unfortunately, it sometimes appears that both terms are interpreted too narrowly and detached from each other. As already pointed out, risk management concerns more than analysing and reporting downside risk, and internal control concerns how an organisation is governed and not just control activities.

This approach to risk management has achieved wide acceptance over the last few years as illustrated by the figure 2 below published in 2021 in Norwegian government guidelines for "Overall management and control of information security" (Norwegian: Helhetlig styring og kontroll av informasjonssikkerhet).


**Figure 2:** The relationship between Management and control, Risk management and Overall governance. Source: Norwegian digitalisation directorate

Enterprise risk management (ERM) as its name implies requires taking a holistic perspective, not just of the organisation's current status, but also of likely positive and negative developments in the future. In this way ERM should be a tool for a balanced prioritisation of resources.

ERM contributes to value creation by reducing sub-optimalisation as well as uncertainty connected to achievement of the organisation's objectives; both objectives that may affect future cash flows as well as non-financial goals. Thus, it makes sense that ERM activities are harmonised with other governance activities, such as strategic planning and management by objectives.

## 1.6 Dynamic risk management

The concept of "dynamic risk management" is now frequently used. This concept does not represent a separate discipline within risk management but is to be understood as a principle promoting the timely management of uncertainty. We have therefore chosen to include this in these guidelines as an example of good practice.

In these guidelines dynamic risk management is defined as relating to the need to adapt the activities for risk identification and management to the reality that the organisation's activities are not static. In order to be in a position to react in a timely manner to uncertainty it is not possible to rely solely on processes that only provide a snapshot on a periodic basis the organisation's risk exposure. As mentioned on a number of occasions in these guidelines risk management is about more than a regularly

performed risk analysis, for example on an annual basis. If risk is to be managed dynamically it is necessary to integrate risk evaluations in the day-to-day decision-making processes and in the methods used to measure, communicate and report the achievement of objectives.

In summary, it is important to establish processes and mechanisms which allow the organisation to mitigate – or exploit risks. This points to ensuring that the first line has adequate tools to enable risks to be addressed on a timely basis, rather than focussing solely on the second line's ability to present a risk profile. The following are examples of mechanisms which may support dynamic risk management:

- Tailored methods and routines for evaluating risk in connection with investment decisions or in advance of concrete decisions in project processes
- Ongoing monitoring of Key Risk Indicators with the related processes for responding when specific warning levels are breached
- A bank's credit process with principles for evaluating credit commitments and ongoing monitoring of the bank's portfolio exposure
- Events that trigger the performance of risk evaluations and the potential escalation of appropriate responses requiring the involvement of executive-level decision makers
- Ongoing updating of models for evaluation of risks related to proposed investments with the aim of exploiting opportunities giving the highest risk reward ratio
- Integration of risk aspects in the reporting on achievement of objectives providing the decision makers with timely information about uncertainties attached to the organisation's achievement of goals

How the organisation succeeds in establishing sound processes making risk management dynamic will vary according to the organisation's type, complexity and ambitions. There are however a number of common factors which should be considered when building risk management that is as dynamic as possible. Below are some examples:

- The possibility to extract risk data in a timely and intuitive way, for example by a combination of internal and external data
- An understanding of the organisation's appetite, tolerance and capacity for risk
- A clear governance structure outlining roles and responsibilities in the organisation's decision-making processes

It is additionally critical to have a good and open working relationship between the first and second line functions in monitoring risks. A good second line function supports the first line (risk owners) in establishing good quality processes to respond to risks in an optimal and timely fashion. The second line shall additionally be in a position to

demonstrate to its stakeholders how the organisation's internal control framework ensures such timely response.

### 1.7 The concepts of GRC and IRM

Internal control and risk management may be seen as mutually dependent whilst they are also at the same time dependent on their organisation's structure and management principles. Compliance also plays a key role here. For this reason, these professional disciplines may be described under one umbrella as "Governance, Risk and Compliance" (GRC). When talking about ERM it is also important to have an awareness of how these domains are part of an integrated whole in the organisation. These constitute separate areas which should not and cannot be managed in isolation.

When working with ERM it is important to see the overall governance picture. IIA Norway makes this clear in the 2021 publication "Guidelines for governance - IIA". In these guidelines "Risk management" is both one of the 17 identified components of governance as well as a means to achieving overall good governance.

Confusingly, the concept of "GRC" is also used in the marketplace to define systems and technological solutions which allow the registering of risk assessments, control data and test results across functions such as IT security, risk and compliance. Another abbreviation that may be encountered describing the same concept is "Integrated Risk Management" (IRM). This narrowly defined concept should not be confused with Enterprise Risk Management (ERM).

## Chapter 2: Tasks and responsibility for risk management

### 2.1 Tasks and responsibility

In these Guidelines we refer to the "Risk function". This does not necessarily refer to a person or group of people, rather, and more importantly, ERM 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 should be able to contribute to the organisation's financial reporting.

### 2.2 The Board

In an organisation, it will be the highest decision-making body (hereinafter referred to as the Board) which ensures that the organisation has established adequate risk management and internal control systems. In accordance with the requirements of the Norwegian Corporate Governance Board ("NUES") this responsibility includes, amongst other matters, the requirement that the Board shall:

- Ensure that the organisation has sound internal control and risk management

systems that are appropriate in relation to the extent and nature of the organisation's activities. Internal control and risk management systems should also encompass the organisation's corporate values and ethical guidelines

- Perform an annual review of the organisation's most important areas of exposure to risk and its internal control arrangement.
- Provide an account of the main features of the organisation's internal control and risk management systems in the annual financial statements.

The Board should set clear requirements for risk management activities to ensure that all risks that can influence the achievement of objectives are adequately addressed. Furthermore, the Board should approve the organisation's risk appetite and risk tolerance levels.

## 2.3 The Chief Executive and management

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

## 2.4 The goal for risk management

Managers at all levels should ensure that the risk management process is fully integrated across all levels of the organisation and is strongly aligned with the organisation's objectives, strategy and culture. An organisation's risk management activities will take place at various levels of the organisation dependent on the relevant focus.

"Dealing with risk is part of governance and leadership and is fundamental to how an organization is managed at all levels." — ISO 31000:2018 introduction

In ERM the focus is on the consequence for the whole organisation as opposed to personal goals or goals within the individual's own business area. this can be defined as "individual" risk management. The totality of individual risk management in an organisation can lead to sub-optimisation from the perspective of the organisation taken as a whole.

The performance of task risk management should therefore also have a basis in an enterprise-wide perspective through the goal setting and incentive structure. These three separate perspectives: ERM, task risk management and individual risk management are illustrated in figure 3.

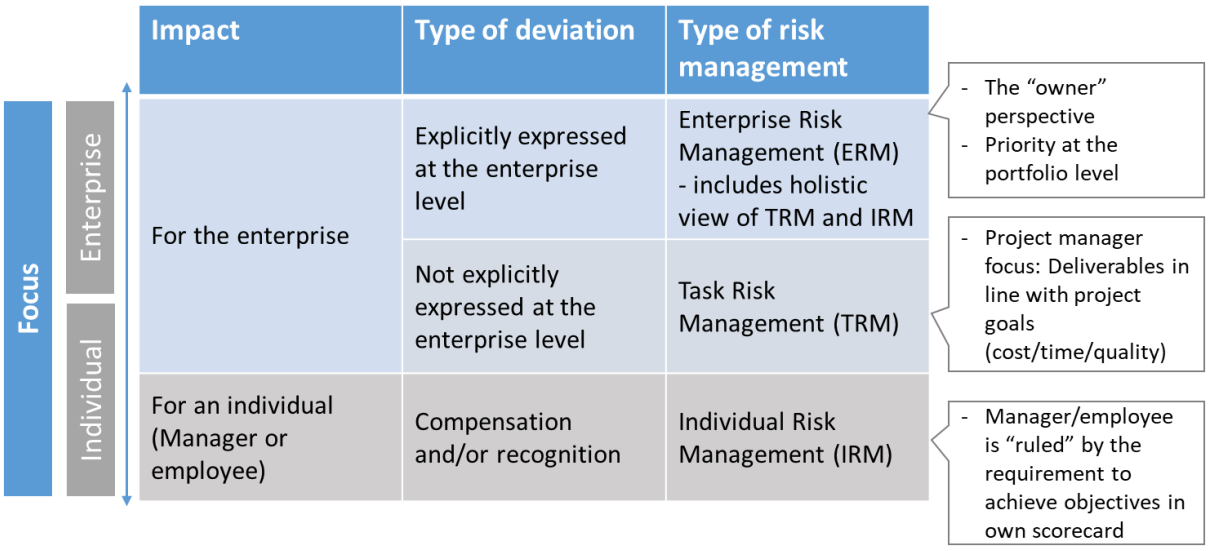


**Figure 3:** Types of Risk Management. Source: "On the Need for Rethinking Current Practice that Highlights Goal Achievement Risk in an Enterprise Context" Eyvind og Terje Aven.

## 2.5 Chief Risk Officer

The senior person responsible for the Risk function will often bear the title Chief Risk Officer (CRO). It may not be appropriate to have a discrete CRO position and these responsibilities may therefore be assumed by another person, however in these guidelines CRO will be used to identify this position.

The Risk function shall assist the organisation in its work in designing and implementing efficient and effective processes to identify, analyse, evaluate and treat risk. In addition, the CRO 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.

The CRO should have the responsibility to monitor and review the performance of risk management activities taken as a whole, and to assist line management in communicating relevant risk information to operational units and to the management and Board of the organisation as well as to external parties where appropriate.

Relevant responsibilities of the CRO are to:

- Provide risk management techniques and assessments in relation to strategy-and objective-setting tasks.
- Establish operational *guidelines* for risk management, defining roles and responsibilities, and establishing goals for the implementation of the risk management tasks.
- Prepare a *framework* for risk management encompassing the whole organisation, and where necessary addressing specific processes, functions or departments of the organisation.
- Promote the creation and preservation of 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).
- Develop a methodology for the identification, scoring, evaluation and monitoring of risk including emerging risk. As far as possible the objective should be to provide a quantitative assessment of risk so that there will be a common and understandable basis for making priorities and decisions.
- Assist management in the development of *risk reporting* and monitor the risk reporting process, including setting key risk indicators (KRI) which establishes 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 management, the Chief Executive and the Board based on an independent and qualified evaluation of strategy performance and risk management.

The CRO lays the groundwork for and monitors the implementation of:

- *Effective risk management principles* for senior management
- Assistance to risk owners in defining planned risk exposure.
- Communication of *risk related information* to the organisation, 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 to decision makers is in an understandable and balanced format.

The CRO 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 be the cause of material risk. The CRO shall monitor that the risk management processes are performed in practice and react if a situation should arise where these are inadequate.

## 2.6 Responsibility for ERM

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

In short ERM is concerned with using a systematic approach to facilitate the organisation as a whole’s ability to achieve its objectives via its organisational structure, internal processes, control activities and decision-making.

An important task for the CRO is therefore to ensure that objectives are adequately communicated between the various control entities and grounded in these (see figure 4). It is also important to ensure information from these functions are taken account of and included in the ERM activities.

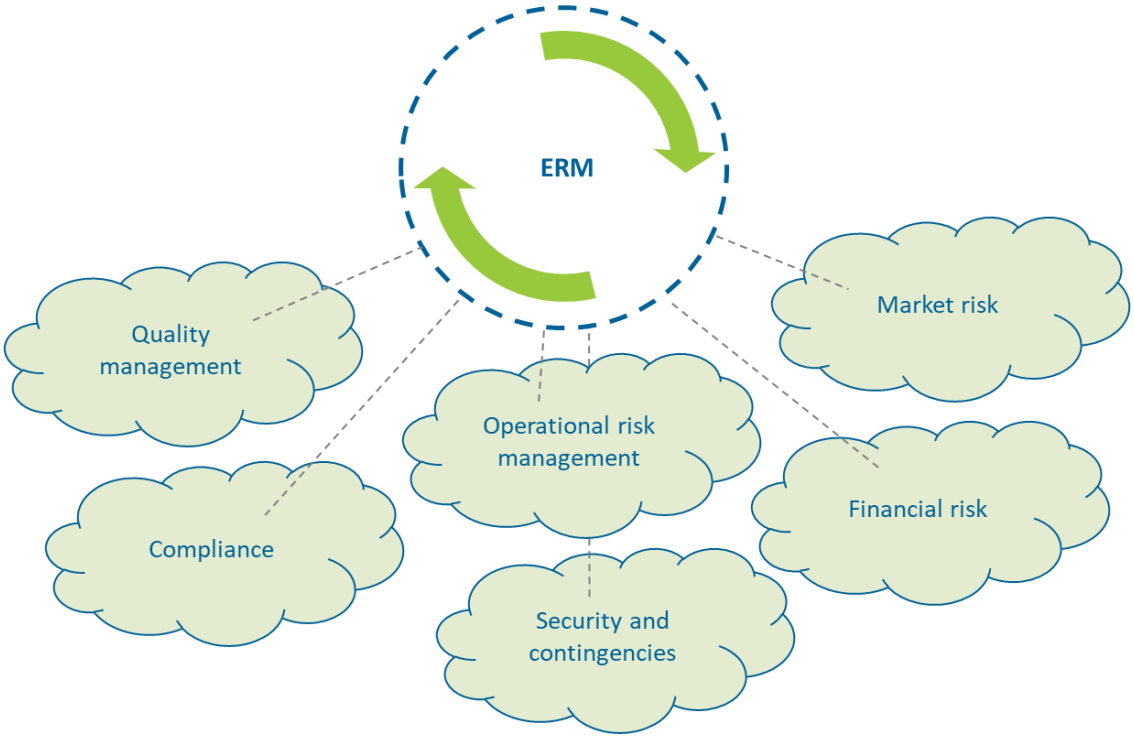


**Figure 4:** Example of the CRO coordinating role and the management of various risk areas. Source: IIA Norway.

### 2.7 Other functions for risk management

Other specific review and monitoring functions can be found within the areas of Health, Safety and Environment (HSE), procurement and Quality/ Continuous Improvement.

In this connection 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.

# Chapter 3: Important topics in risk management

### 3.1 Risk culture

"Risk culture" is an expression which received much attention after the financial crisis in 2008. In short, the crisis showcased that it is not sufficient for a financial institution to publish ethical guidelines and formal risk management structures if this remains a theoretical exercise and not actual practice. Risk culture is well-known from internal control frameworks such as COSO Internal Control and COSO Enterprise Risk Management where it was described firstly as "control environment", then "internal

environment" and lastly "governance and culture". In ISO 31000:2018 Risk Management one of the principles that must be addressed in the creation and protection of value is defined as "human and cultural factors".

Risk culture refers to the norms, attitudes, and behaviours related to risk awareness, risk-taking, and risk management within an organization. It shapes how individuals and groups within the organisation identify, understand, discuss, and act on risks. This can be further illustrated by the model presented by "Institute of Risk Management" shown in figure 5. The five blue elements are at the overall management level and the three red elements relate to human development

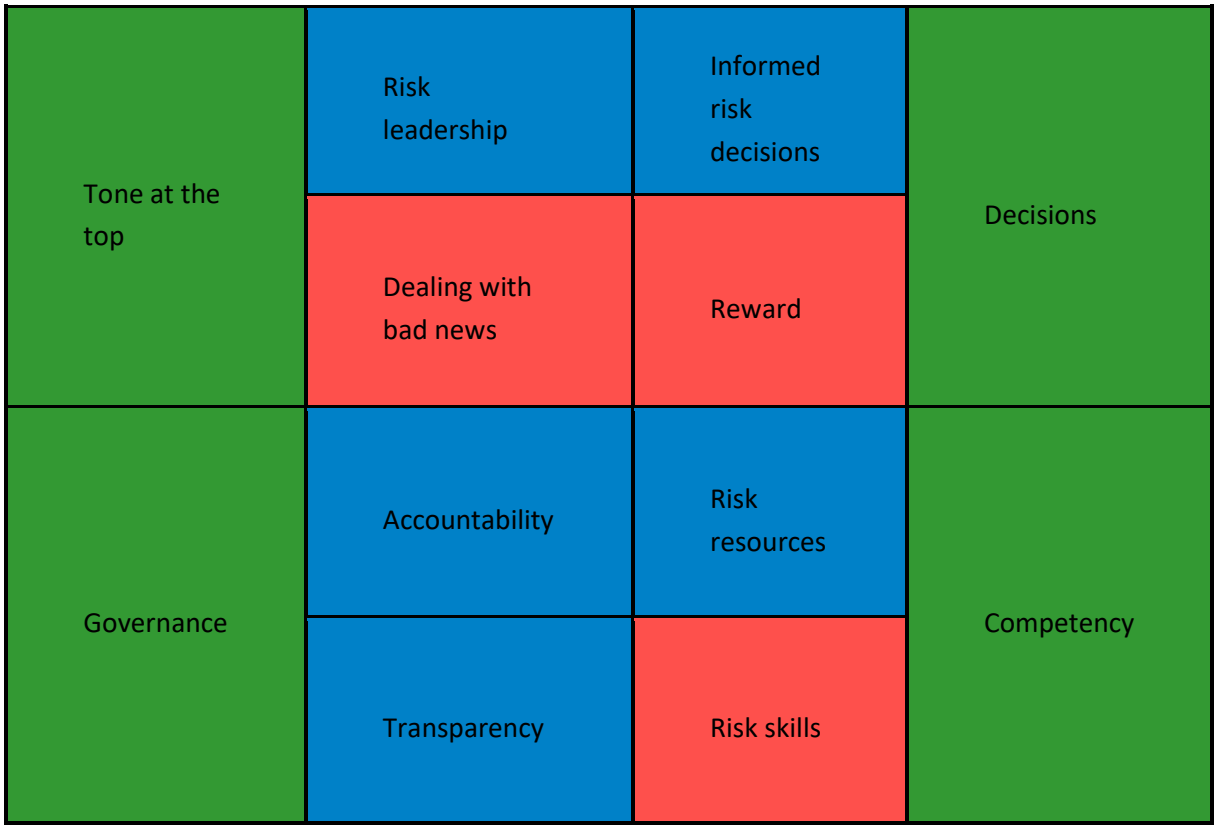


**Figure 5:** Model for risk culture. Kilde: *Institute of Risk Management* (IRM)

Effort should be invested in building a sound risk culture in the organisation, which should then be characterised by a positive attitude to risk management and a structured approach to risk management tasks.

## 3.2 Methodology

The CRO is responsible for choosing a relevant framework/standard which the organisation will use to manage risks and achieve sound business decisions. The starting point may be to choose COSO ERM or ISO 31000:2018 as a basis. A generic framework/standard will, however, always need to be adapted to the specific

organisation it will apply to as well as any external requirements made by public authorities, industry standards etc. The methodology should be evaluated at a minimum annually to reflect changes in the organisation and its market as well as new requirements from public authorities.

## 3.3 Risk appetite, risk capacity and risk tolerance

Risk appetite is defined as “the types and amount of risk that an organization is willing to accept in the pursuit of its strategies and objectives”. Risk appetite is thus the level of risk the organisation is willing to take to achieve its objectives, whereas the term “risk capacity” expresses the level of uncertainty that the organisation has the capacity to treat and the term “risk tolerance” is defined as “acceptable variations in performance related to achieving objectives”.

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, risk appetite being the level of risk that the organisation wishes to take in order to achieve its objectives. Risk capacity expresses the level of uncertainty that the organisation can bear. Risk tolerance is the maximum level of risk that the organisation is willing to accept – ref. the example illustrative example in figure 6.

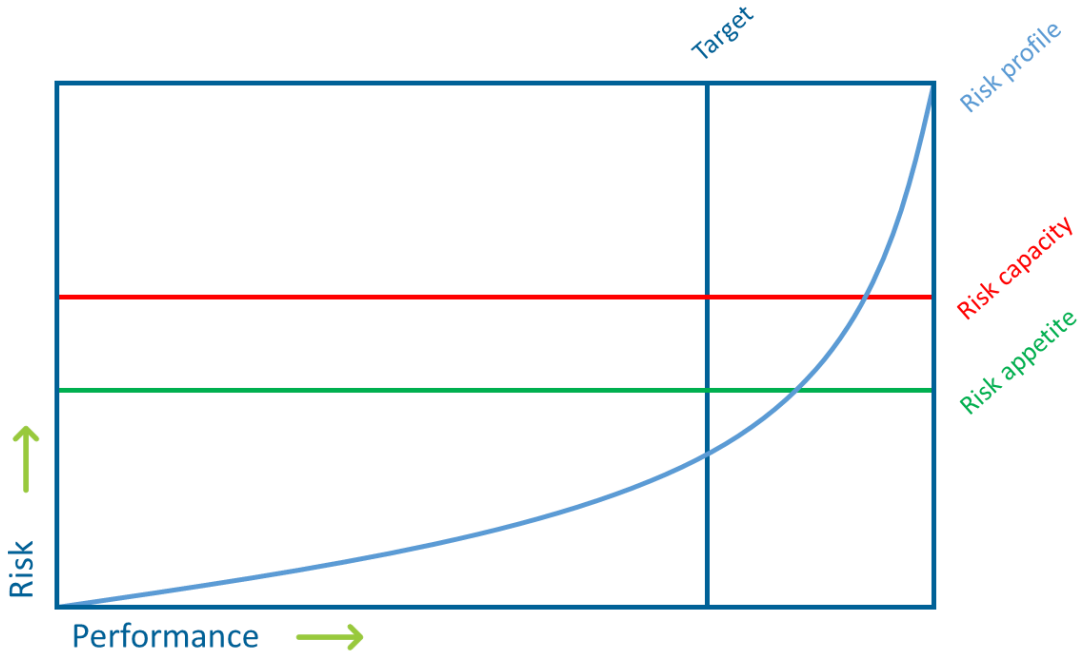


**Figure 6:** Illustration of the relationship between risk appetite and risk capacity.
Source: COSO ERM 2017

## 3.4 Risk gaps

"Risk gaps" is an expression often used to describe an imbalance that can occur between actual risk exposure and expected return on investment (including societal gains). This is especially evident where the probability for a given event is low, but the impact is high.

An important task for the CRO is to identify such gaps and ensure that these are communicated to Executive Management and the Board.

## 3.5 Strategic risk management

The reason for material falls in the market value of listed companies have been analysed in respect of four types of risk:

1. Strategic risk
2. External risk
3. Operational risk
4. Compliance risk

The conclusion from two American surveys and one Norwegian survey was that material falls in the market value of listed companies were overwhelmingly the consequence of strategic risk. In USA the material loss in value caused by strategic risk was calculated in the survey published in 2012 to 81% of the companies surveyed (Booz & Co.) and to 86% in a later survey in 2015 (Harvard Business Review). In a similar exercise performed by Hermann Christensen in 2018 the cause of value loss related to strategic risk was calculated at 63% with external risk as the number two factor. Most of us will also recall

companies such as Kodak and Nokia as extreme examples of companies which did not manage to revise their strategies in a timely manner with a resultant negative hit to the Companies' equity.

We live today in a world with, amongst other things, rapid technological development and manmade climate change. It is therefore important that risk management techniques are taken on board. These will be able to add value to the strategy setting process. The professional use of stochastic techniques may be supplemented with facilitation in performing scenario analyses as well as analyses of current and emerging risks. Some organisations choose to combine strategy setting responsibilities with the Risk function.

## 3.6 Decision-making and risk quantification

The many major and minor decisions taken at all levels in an organisation will influence the organisation's development trajectory and performance. Most of these decisions will involve a degree of uncertainty. Whilst minor decisions may be based on intuition and experience, more important and major decisions that affect the organisation require more thorough analysis as well as discussion of the 'pros' and 'cons' associated with the decision.

The Risk function will, generally, possess the organisation's primary expertise on statistical calculations and data modelling. It will, therefore, be natural that the ERM function contributes with its knowledge and experience in the quantification of possible outcomes. The first challenge will be to identify the data to be used in the evaluation of possible outcomes.

The underlying data can fall into one of the following three categories:

1. The organisation has adequate and reliable data available
2. The organisation does not have relevant data available.
3. The organisation has relevant data available but there are grounds to question whether the data provides a relevant basis for evaluating possible future outcomes.

Where an organisation has data series of past trends, and where there is every reason to believe that historical trends will recur in the future, forecast outcomes can be made using normal distribution techniques – so called "Value at Risk".

Where the organisation lacks historical data, or it is held that that the historical data does not reflect a probable future development, data series will need to be constructed. This may be done by identifying comparative situations or by adjusting the historical data to reflect the new conditions. Thereafter it will be possible to create normal distributions and "Value at Risk" forecasts.

In situations with inadequate or non-existent data series, but where it is possible to use

judgment to estimate the outer limits of a normal distribution, Monte Carlo simulation may be used to create data as a basis for analysis. According to this method an artificial data series can be created as a replacement for empirical data by using a random number generator. Monte Carlo simulation may also be utilised to create models of the effect of incidents with low probability and high outcome, such as is typical of catastrophic disaster.

Where the organisation has no clear idea of future trends different scenarios may be used as the basis for the risk evaluation. This can be a relevant technique to increase the understanding of how potential geopolitical or technological developments may influence products and/or markets. Normal practice is to choose 3-4 scenarios and create data series for each scenario in the manner described above.

An organisation may use scenarios to test the soundness of the strategy and identify potential changes needed to keep the business on a sound footing. The advantage of thinking the unthinkable (i.e. mapping the effect of circumstances outside the expected normal business development) is that it increases the knowledge and understanding of the organisation's vulnerabilities. In this way it may also be possible to identify potential red flags timely and have the time to adjust the strategic direction.

The Risk function does not possess a crystal ball, but it does have techniques which can assist the organisation in strengthening the basis for the decisions that are made. There will always be uncertainty attached to the Risk function's analyses and for this reason the assumptions underlying each separate analysis should be provided.

There is however a type of risk that appears out of the blue and that no one had the imagination to consider possible. These events are often called "black swans". If such an event or events unfold, some comfort may be drawn from the mapping and analysis of comparable scenarios which will, therefore, be seen to have contributed to the organisation's resilience.

## 3.7 Best available information

Quantifying the risk profile entails estimating potential future outcomes based on informed judgments about the likelihood of specific scenarios occurring. The underlying data should reflect the best available estimates, drawing on factors such as historical trends, analogous situations, and—critically—expert judgment. There is always a balance to be struck between the precision of the analysis and the time and resources required to obtain the necessary data. In certain cases, a well-founded expert intuition may suffice for a preliminary assessment. Engaging multiple experts can enhance the credibility and robustness of the risk evaluation by reducing individual bias and broadening the perspective.

## 3.8 Communication and consultation

In order to maintain the Risk function's objectivity, the CRO should not be responsible for taking business decisions and initiating transactions outside the remit of the function. The exception may be where time is of the essence to close an exposure to avoid material losses and where the responsible line management is unavailable. For the organisation to derive benefit from the insights the Risk function has built up from its work it is important that the risk profile and perception of the possibilities of realising positive or avoiding negative outcomes is communicated clearly and in a timely manner to the executive management and the Board.

It will be reasonable to expect that the CRO's job description also includes a duty to report promptly if the CRO identifies matters that can have a material effect on the organisation's performance.

The risk function represents a professional capacity with insight in all business areas. It is therefore to be expected that Executive Management and the Board will want to utilise the CRO's advice and judgment in connection with important business decisions.

## 3.9 Operational risk and risk response

ERM processes should identify potential risks which are critical to the organisation's value creation as a basis for monitoring both the risk profile and actions taken to reduce negative impact and strengthen positive performance.

Traditionally, the monitoring of the operational risk profile has focused on verifying that key controls are both established and functioning effectively. This is often achieved through Control Self-Assessment (CSA) procedures, where first-line employees confirm that required controls are being applied in practice. These insights are valuable not only for line management to avoid losses but also serve as a foundational input for second- and third-line assurance functions.

Historically, control activities have been retrospective in nature—such as sample testing. However, advancements in artificial intelligence have opened new possibilities for automating these controls. This could enable real-time, cost-efficient monitoring of all transactions and accounting entries. Nevertheless, where decisions still rely on human judgment, sample testing remains relevant—particularly for purposes such as employee training and development.

Another important outcome of operational risk evaluation may be the identification of actions to mitigate the risk of errors. For example, replacing manual processes with fully automated solutions. In such cases, it is considered good practice for the organization to actively monitor the implementation of these actions—tracking progress in terms of timeliness, cost, and effectiveness. Status updates should be reported through line management and reviewed by the risk function to ensure the intended improvements to the risk profile are achieved.

IIA Norway has prepared and published the document An Introduction to Operational Risk Management - IIA which defines a framework for the management of operational risk.

# Chapter 4: Organisation and performance of the Risk function

## 4.1 The three lines 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, 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 organisation's overall risk management and internal control structure.

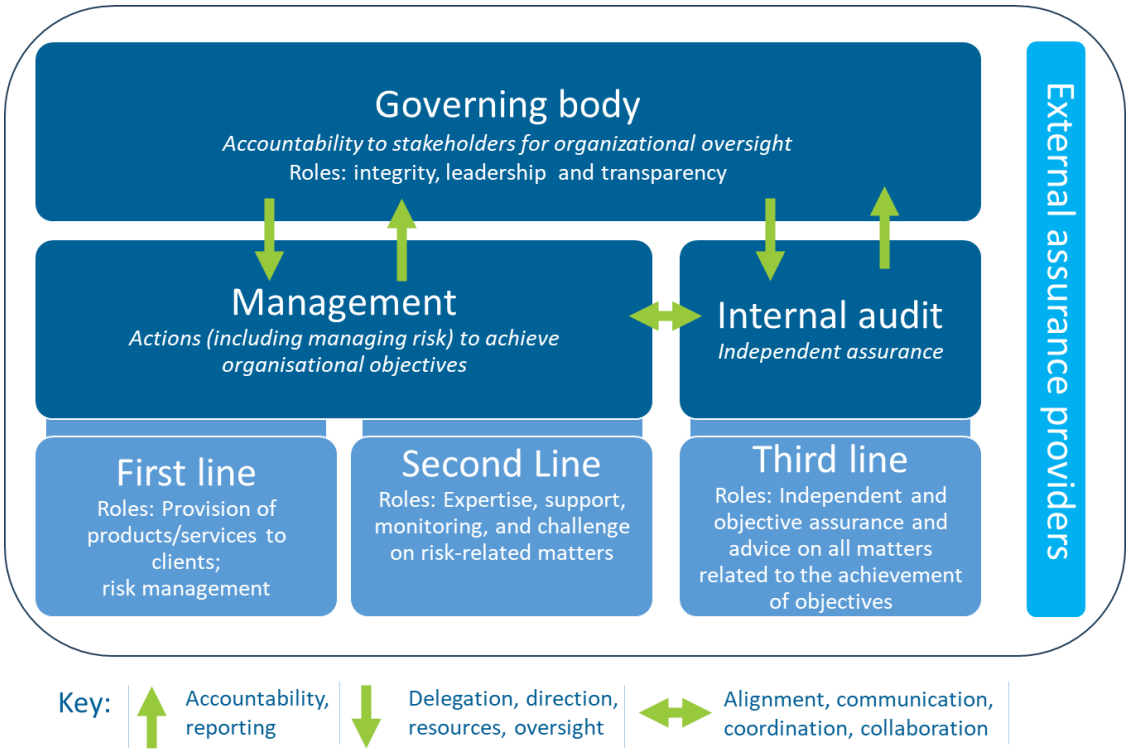


**Figure 7:** The IIA's three lines model. Source: *The IIA's Three Lines Model – An Update of the Three Lines of Defense* (as of Sept. 2024)

The IIA's three lines model provides a high-level overview of an organisation's governance and control structure including roles and responsibilities for risk management and internal control. 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.

The ERM function is a second line role and one of the support and control functions in the organisation, similar to amongst others the Finance, Compliance, IT-security and HSE functions as well as the Legal and Quality Control functions. The specific functions in an organisation will vary by organisation and sector.

The second line roles are 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 control work is to identify matters deviating from the expressed risk appetite and desired development, and to ensure that the organisation focuses on and reacts to these issues.

It is important to be aware that the functions in the second and third lines 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 to put the company in a position 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.

## 4.2 Cooperation between second line functions

Today, more and more organisations have established a compliance function to monitor breaches of legal requirements and internal guidelines (including fraud risk). Such a function may not be organised as a separate function, but the responsibilities may be covered by someone in a related position. This guidance will use the term Chief Compliance Officer (CCO) when referring to this function.

The CCO usually reports directly to Executive Management. It should be taken as granted that the CRO and CCO work closely together, especially in the areas of legal risk, fraud risk, social dumping, whistleblowing, reputational risk, risk culture and the monitoring of ethical guidelines.

The CCO and CRO, as well as the heads of other second line functions, have their respective areas of responsibility and/or work tasks which border on one another's. Even though these functions are independent of one another, it is important to foster open communication lines between these functions to ensure an efficient use of resources. Furthermore, consideration may be given to gathering the functions organisationally with the aim of strengthening the level of professional cooperation and the ability to carry out the several tasks.

## 4.3 Cooperation between the second and third lines

Second and third line functions have a similar characteristic in that they are not responsible for the day-to-day operations of the organisation. Both functions have as their objective that the organisation they work for should develop successfully and sustainably.

The Global Internal Audit Standards requires that "the chief audit executive must create an internal audit plan that supports the achievement of the organisation's objectives". The plan shall build on an assessment of the organisation's strategies, objectives and risks. In this process it will be necessary for internal audit to understand the risks the organisation is faced with. An important source of this information will be the documentation prepared by the ERM and compliance functions.

To facilitate communication with the Executive Management and the Board it is important that both the ERM, Compliance and Internal Audit functions develop a common vocabulary and taxonomy as far as this is relevant.

A relationship between the second and third lines should be built on openness and trust. This will mean that Internal Audit will be better able to focus its efforts in those areas where monitoring by the ERM and Compliance functions are weakest. By challenging the CRO and CCO, the head of Internal Audit will contribute to the quality of those functions.

## 4.4 Important considerations regarding organisation of the Risk function

The ERM function´s organisational positioning will vary depending on the characteristics of the organisation and its maturity level in respect of ERM (see further the ERM maturity model published by IIA Norway). Many frameworks recommend that the Risk function should report to Executive Management without specifying its positioning in greater detail.

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

The Risk function shall perform an active role in monitoring the holistic risk picture and the relationship between the achievement of objectives and/or financial returns. The position shall provide the Chief Executive and the Board with clear recommendations and proposals in respect of strategic developments.

There is no one right answer to where the Risk function should be placed within the organisation. Before deciding on the positioning of the Risk function, management should amongst other matters consider:

- The extent of the function's areas of focus

- What other areas the Risk function will interface with and thus can achieve synergies and professional cooperation with
- The organisation's need to have in place a professional environment for risk management and internal control
- The organisational position which is most likely to facilitate the effective performance of the Risk function's responsibilities.

It is highly recommended that the CRO has a reporting line and can communicate directly to the Board or a Risk or Audit Committee of the Board. The goal of this reporting is to ensure, as may be necessary, the possibility for independent and comprehensive reporting directly to the Board of matters concerning the organisation's risks.

## 4.5 Mandate, authority, competency and resources

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

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

## 4.6 Executive management responsibility

The CEO is responsible for establishing and maintaining an effective framework for risk management and internal control. This includes issuing a policy statement and defining a clear mandate, aligned with the Board-approved guidelines and risk appetite. This responsibility remains equally important even when the risk appetite is difficult to quantify. In organisations with objectives that are not financially quantifiable -such as those with a public sector mandate, a social mission, or a strong focus on reputation - it should still be possible to assess uncertainty using a measure that reflects the potential impact on the achievement of objectives.

The organisational position, responsibilities, activities and authority of the CRO should be outlined in the CRO's job description and the Risk function's mandate. This is then approved by the Chief Executive. The following main elements should be described:

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

## 4.7 Independence, objectivity and integrity

People employed in and responsible for the organisation´s Risk function, should as a second line function be organised independently from the units over which they perform monitoring and control activities. This should not preclude the Enterprise 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 directly affect the business operations. Persons employed in the Risk function shall equally not work in units that they themselves are responsible for monitoring.

Some, and especially smaller organisations, will not have the possibility to establish a separate and independent position for working with risk management issues. In such circumstances, it is important that the function description addresses this issue. A mix of roles may weaken the Risk function's independence.

The organisation should earmark sufficient resources to ensure a well-functioning and independent Risk 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 function must possess, in addition to a relevant professional competency, a high level of professional integrity. Additionally, the CRO must have adequate authority and experience to take responsibility for the development and communication of the risk management framework. Professional integrity is critical to achieving confidence and realising the function´s value proposition. Integrity is perceived through the objectivity, consideration and responsibility accompanying the tasks performed. Integrity can be compromised through biased, unethical and illegal acts.

Employees in the Risk function must 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 function´s responsibilities and tasks. This mandate should be supported by the organisational structure, access to information and reporting requirements.

## 4.8 Understanding context and access to information

The Risk function should have access to the required information regarding the organisation's operations and decisions made. This right of access to relevant information can be defined in the function description and include for example access to computer systems, governing documents, physical property and employees, as well as documents from governing bodies. In addition, the Risk function should have the right to participate in internal meetings, as necessary.

## 4.9 Remuneration and incentive system

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

## 4.10 Reporting

Irrespective of how the Risk 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.

## 4.11 Outsourcing the Risk function

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