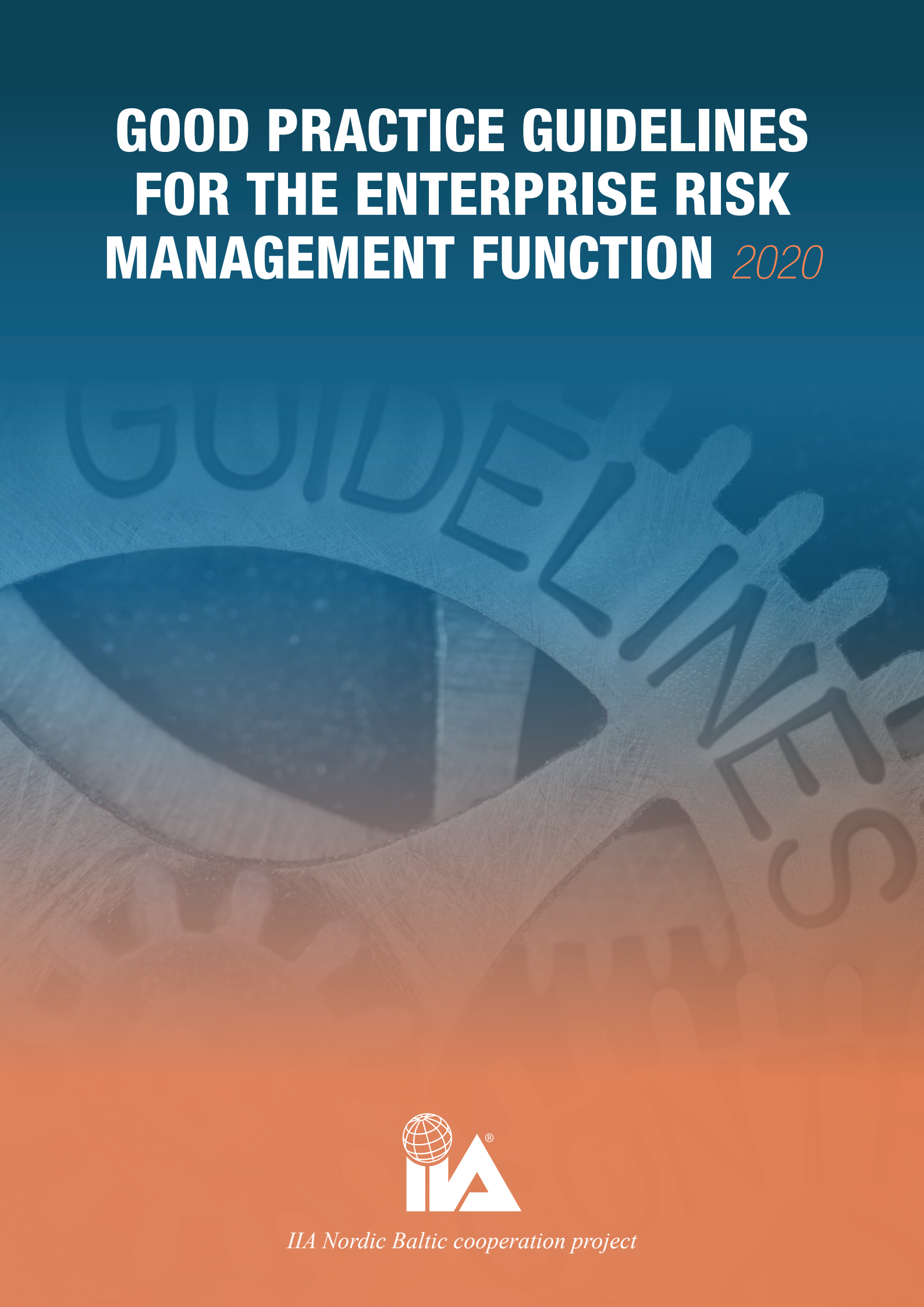
GOOD PRACTICE GUIDELINES FOR THE ENTERPRISE RISK MANAGEMENT FUNCTION *2020*



IIA Nordic Baltic cooperation project

PREFACE

The "Good Practice Guidelines for the Enterprise Risk Management function" has been developed by a steering group drawn from the institutes of internal auditors for the Nordic and Baltic countries. The target group for these guidelines is organisations that would like to either establish an Enterprise Risk Management function or develop their existing risk management function further. The principles in this guidance may also be useful for organisations without a discrete Enterprise Risk Management function, but where responsibility for Enterprise Risk Management is assigned to another function with enterprise-wide responsibility.

The main motivation for internal auditors' involvement in defining what is good practice for Risk Management is that Enterprise Risk Management has developed over the last 15 to 20 years to become a vital element in good corporate governance. Unlike the profession of internal auditing which has had a unifying global body defining principles and standards the Institute of Internal Auditors (founded in 1941) there is currently no equivalent worldwide body representing the profession of Enterprise Risk Management. In the Nordic and Baltic countries the profession is characterised by a number of formal and informal associations, some of which are members of a European representative body FERMA. The primary aim therefore of this good practice guideline is twofold, firstly to set a common benchmark which it is believed may strengthen the development of the risk management profession in the Nordic and Baltic countries and second, to facilitate the internal audit function to discharge more effectively its responsibility according to the professional standard requirement that "the internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes" [1].

The active members of the steering group for the publication of this document were:

Martin W. Stevens, IIA Norway (Chairman)
Auðbjörg Friðgeirsdottir, IIA Iceland
Karlis Majevskjis, IIA Latvia
Kim Stormly Hansen, IIA Denmark
Roman Laidinen, IIA Estonia
Žana Kraučenkienė, IIA Lithuania

The steering group members have also formed local working groups bringing together both internal auditors and risk managers in reviewing the documents. Special thanks are therefore made to:

Risk managers' club, Latvia
Risk management association, Lithuania
FinnRima (Finnish Risk Managers' Association), Finland and IIA Finland
for their contribution to the project.

The steering group expresses its gratitude to IIA Norway for taking the initiative for this project and allowing the use of Guidelines prepared by their Network for Risk Management and additional appended material. Specifically thanks go to following members of the Risk Management Network of IIA Norway:

Ayse B. Nordal, Undervisningsbygg Oslo KF
Janne Britt Saltkjel, KPMG
Martin Stevens, Gjensidige Forsikring
Ole Martin Kjørstad, Bank of Norway
Petter Kapstad, Equinor
Randi Bolsøy Hardy, Forsvarsstaben
as well as to Inger Jennings for editing the English text.

Copyright IIA Norway version 1.0 published 1st February 2020

[1] *IIA performance standard 2020* https://global.theiia.org/standards-guidance/mandatory-guidance/Pages/Standards.aspx

CONTENT

EXECUTIVE SUMMARY

Enterprise Risk Management (ERM) is now seen as an essential part of good internal governance. 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. To ensure the operation and implementation of sound risk management in a holistic fashion it has been found necessary to have a person or function dedicated to this activity.

These guidelines delineate core criteria that will guide the establishment of this function, and these are (ref. to relevant chapters in the document):

1. Risk management is a line management responsibility, however the ERM function contributes to the identification, evaluation and treatment of risks (uncertainty of future outcomes). (cf. 3.1 and 3.2)

2. The ERM function ensures the integration of risk management into decision-making at all levels. (cf. 2.6)

3. The ERM function maintains clear and open communication with executive management and the Board as well as with other control and assurance functions. (cf. 2.6)

4. The ERM function has a clearly defined mandate. (cf. 3.4)

5. The employees in the ERM function should be organised independently of operational responsibilities and demonstrate professional integrity. (cf. 3.3 and 3.5)

6. The ERM function should have access to all information relevant to the performance of its activities. (cf. 3.6)

7. The ERM function's remuneration should not contain significant financial performance-based components that could lead to conflicts of interest and influence the objectivity of the staff working in the function. (cf. 3.7)

8. Remuneration in the ERM function should be sufficient to attact and retain staff of sufficient seniority and professional and business knowledge. (cf. 3.7)

In appendices to this document we have provided additional practical guidance to the operation of risk management.

1 INTRODUCTION

1.1 The purpose of this guidance

The need to establish an Enterprise Risk Management (ERM) function may arise across all organisations both in the public and private sectors. Drivers for establishing the ERM function will 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, poor health and/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 an ERM function as an essential element of sound governance.

In this guidance, we have tried to describe «good practice» for the ERM 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 will need to make individual adaptations depending on its nature, size, complexity and organisational culture.

This Good Practice Guideline seeks to provide some clarification and delineate the organisation of an Enterprise Risk Management function. This includes the distribution of roles and responsibilities between the different control and assurance functions of an organisation, such as internal audit, the Enterprise Risk Management function and the Compliance function.[2]

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

Risk management must take place at all levels of the organisation. These Guidelines describe the function of ERM. The principles which are described may also have some validity for those working with risk management within a more limited and specialised area of an organisation.

1.2 The concept of risk

The taking of risk is a natural part of running any enterprise[3], however it is often not explicitly stated in the formulation of business decisions. The expression «risk» has often been exclusively

[2] 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.

[3] 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.

associated with unwanted events, and risk management has been defined as analysing and restricting the probability and impact of undesirable events. This is only one dimension of the total picture. Evaluating positive outcomes is just as important a part of ERM as is evaluating negative outcomes because ERM is concerned with the whole picture and evaluating risk strategy in relation to a portfolio of risks.

1.3 Enterprise Risk Management (ERM)

The tasks of ERM and strategy are integrated and iterative processes. The objective of ERM is to ensure the correct amount of risk exposure, as evaluated against both the expected and desired level of achievement of the organisation's objectives and in line with the risk appetite and business strategy of the Board[4] and Executive Management. It is concerned with ensuring both the achievement of objectives as the enterprise develops and the appropriate management of the organisation´s assets, including human resources, reputation as well as the avoidance of losses or waste as a result of undesired events. This will include 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 using ERM will ensure 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 - see appendix 3 for further details. 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.

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

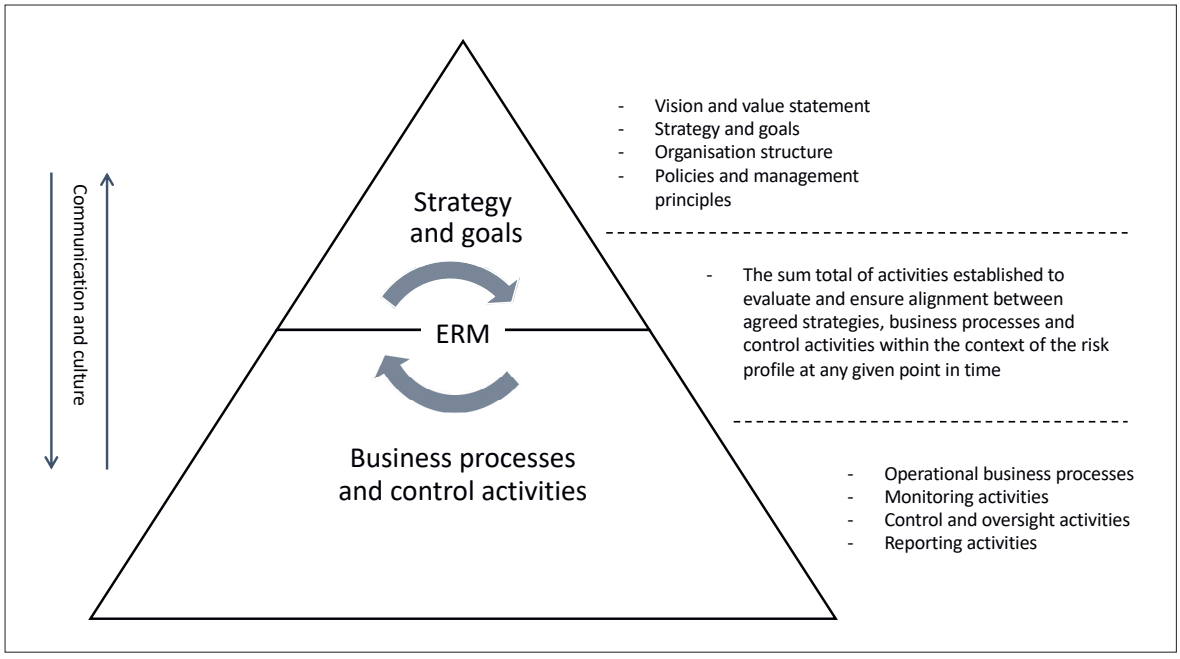


Figure 1 The interrelationship between ERM and governance

[4] *«Board» is used throughout these Guidelines to describe the highest decision-making body of the organisation.*

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 (e.g. exchange rate and currency risk);
- Analyse developments in the organisation, its environment (internal and external) and the risk profile over time;
- Proactively initiate activities which steer development in the required direction;
- Build a culture which enables every employee to make simple and complex risk-based decisions contibuting to the implementation 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.

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 can be achieved through a conscious attitude to an acceptable level of risk and the desired risk exposure. For further details see appendix 1 - A practical approach to ERM and tools for developing risk management in an organisation.

1.4 The risk management responsibilities of governing bodies and organisational levels

"Dealing with risk is part of governance and leadership, and is fundamental to how an organization is managed at all levels." — International Organization for Standardization.

Executives should ensure that the risk management process is fully integrated across all levels of the organisation and is strongly aligned with objectives, strategy and culture. Risk management takes place at various levels of the organisation and its governing bodies 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 «individual» risk management. The totality of individual 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 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 2.

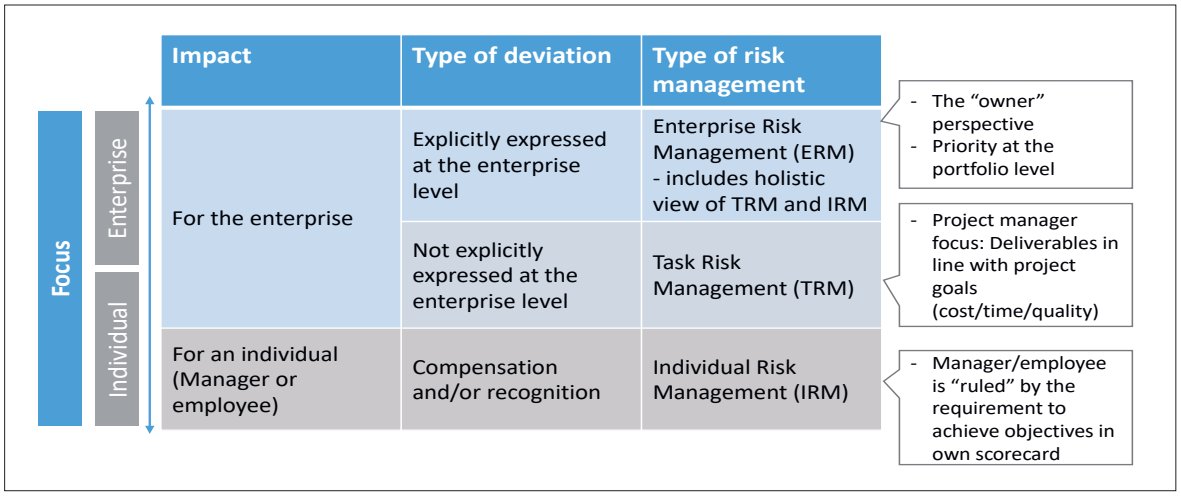


Figure 2 Types of risks and risk management[5]

1.5 The relationship between risk management, internal control and governance

Risk management and internal control are concepts that are frequently mentioned in conjunction. However, the concepts are often perceived too narrowly and separate from 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[6]. The same foundation also provided a definition of ERM in 2004 which was updated in 2017 under the title "Enterprise Risk Management – Aligning Risk with Strategy and Performance".[7] Both definitions are given in figure 3.

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 the culture, capabilities, and practices that organizations integrate with strategy-setting and apply when they carry out that strategy, with a purpose of managing risk in creating, preserving, and realizing value.[6]

Figure 3 COSO definitions

Furthermore, the COSO ERM 2004 definition[8] reads as follows "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."

Based on these definitions, it is clear that internal control is an element or sub-process of ERM. As expressed by COSO *"A strong system of internal control supports the achievement of the organization's business objectives and therefore good internal control is a way of managing risk. However, enterprise risk management is much broader than internal control. In addition to supporting management's efforts to achieve business objectives, it aligns risk management with strategy setting and aids a company's ability to assess whether the organization is accepting risk appropriately."* [9]

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. ERM contributes to value creation via reduced sub-optimisation as well as a reduction of uncertainty related to the achievement of objectives; both those which affect future cash flows and nonfinancial objectives. Therefore, this work should also be harmonised with other management activities such as strategy and performance scorecards.

[5] *http://onlinelibrary.wiley.com/doi/10.1111/risa.12375/full*
[6] *Internal Control – Integrated Framework, May 2013 http://www.coso.org/.*
[7] *Enterprise Risk Management – Aligning Risk with Strategy and Performance, June 2017 http://www.coso.org/.*
[8] *Enterprise Risk Management – Integrated Framework, September 2004 http://www.coso.org/.*
[9] *ERM FAQ D.3 https://www.coso.org/documents/ERM-FAQs.pdf*

2 IMPORTANT ELEMENTS OF THE ERM FUNCTION

2.1 The ERM function´s tasks and responsibility

In these Guidelines we have used the expression the "ERM 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 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.

2.1.1 The highest decision-making body

In an enterprise, it will be the highest decision-making body (hereinafter referred to as the Board) that will ensure that the enterprise has established adequate risk management and internal control systems. In accordance with the requirements of national Codes of Practice for Corporate Governance this responsibility encompasses amongst others 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, ethical guidelines and guidelines for corporate social responsibility. The Board sets strategy, the risk appetite statement and risk tolerance limits and should perform an annual review of the organisation's most important areas of exposure to risk and its internal control arrangement. The board of directors takes risk-based decisions and this fact must be documented.

Furthermore, it will often be a requirement that the Board must provide an account of the main features of the organisation's internal control and risk management systems as they relate to the organisation's financial reporting.

2.1.2 The Chief Executive and management

The Chief Executive has the 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.

2.1.3 Chief Risk Officer

The senior person responsible for the ERM function will often bear the title Chief Risk Officer or CRO. As mentioned in 2.1 above it may not be appropriate to have a discrete CRO position and these responsibilities may be assumed by another position, however in these guidelines CRO will be used to identify this senior position.

The ERM 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 – so called «emerging risk».The CRO should have the 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 operational units and to the management and Board of the organisation as well as to external parties where appropriate.

Relevant responsibilities for 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 and assists risk owners[10] in defining planned risk exposure.
- Communication of *risk related information* to the organisation, including making expert pronouncements.

Reporting lines should be established 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 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 cause material risk. In addition, the CRO shall monitor that the above-mentioned processes are performed in practice and react if a situation should arise where these are inadequate.

2.1.4 Chief Compliance Officer

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

In addition to a centralised Enterprise Risk Management function led by a CRO (which is part of the second line of defence) an increasing number of organisations have established a separate position of CCO to monitor risks related to breaches of legal regulations and internal and external regulations (including fraud risk). The CCO will normally report directly to senior management. There is a presumption that the Compliance and Enterprise Risk management functions will work closely

[10] *A risk owner has responsibility for the profits and losses associated with the defined risk.*

together, especially in respect of the areas of legal risk, reputation risk, establishment of a sound risk culture and monitoring of ethical guidelines.

2.1.5 Other risk functions and the CRO's ERM role

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

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 CRO 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 considered and included as a part of the work with ERM.

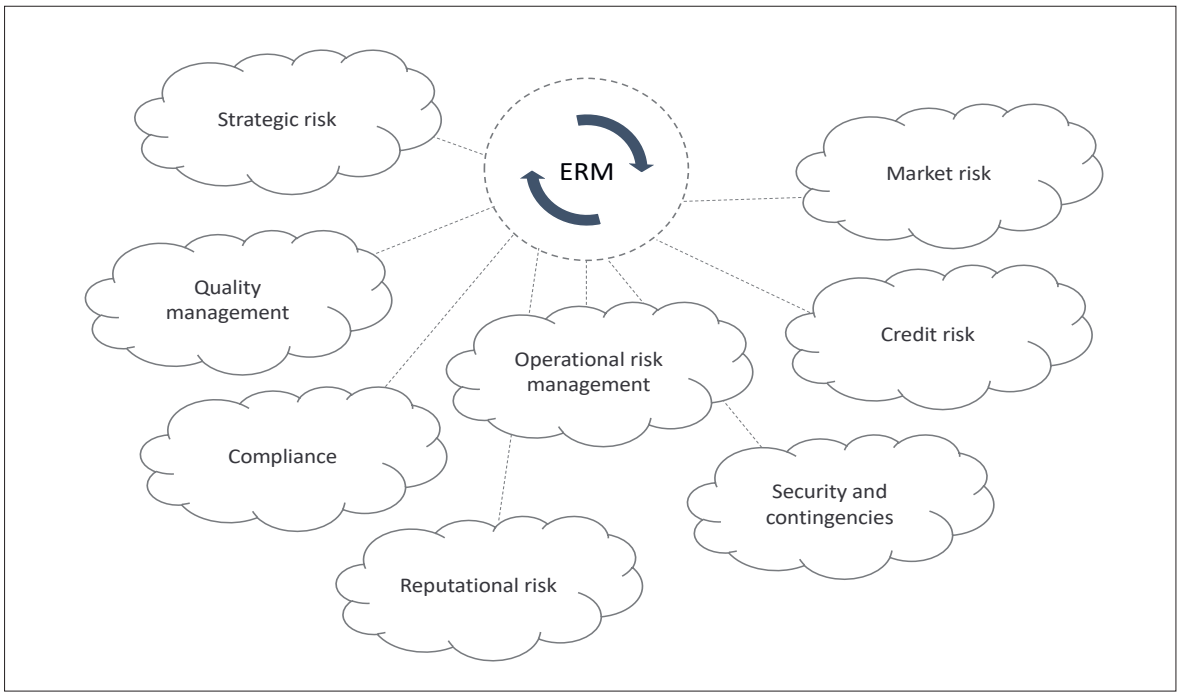


Figure 4 Example of the CRO coordinating role and the management of various risk areas

2.2 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. 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 levels within risk tolerance limits[11].

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

It is preferable that the CRO is able to report directly to the Board. This can be organised in various ways, for example, the CRO 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 an independent and unadulterated reporting to the Board in respect of the organisation´s risk profile.

2.3 Grounded in the Executive Management

The Chief Executive is responsible for the establishment and performance of sound risk management and internal controls with 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. In organisations with objectives that are not quantifiable in financial terms it is nonetheless important to connect uncertainty to a scale which expresses the potential effect on the degree of achievement of objectives. An example of this can be in relation to a public mandate or achievement of a social mission, or risk tolerance related to an organisation's reputation.

The organisation, responsibilities, activities and authority of the CRO should be determined by the CRO's job description as well as by the Enterprise Risk Management function's mandate approved by the Chief Executive. 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 equate to the responsibilities, tasks and authority.
- Access to information.
- Reporting responsibility.

2.4 Risk appetite

Risk appetite expresses the level of uncertainty an organisation is willing 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 statutory 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 capacity» which may be defined as an absolute limit to the level of risk an organisation can take.

See further appendix 4 Risk appetite.

2.5 «Risk gaps»

«Risk gaps» is an expression which may be used to describe an imbalance that can occur in the risk picture for example:

1. in the difference 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.
2. in the situation where the internal control system is not strong enough to mitigate the inherent risk to a level where the residual risk is below the risk appetite.

An important task of the Enterprise Risk Management function is to identify such gaps and ensure that these are communicated to Executive Management and the Board.

2.6 Risk management, Executive Management and decision-making

Executive management will take decisions in respect of the organisation's future. Very few decisions can be made which do not include a degree of uncertainty. Risk management's field of expertise is in evaluating and communicating the uncertain elements so that there is a fully informed basis for taking a decision.

Figure 5 describes five distinct types of future uncertainty that risk management may encounter and how they can be analysed.

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 5 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 be 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[12]. The organisation may prepare itself for such events by scenario exercises performed in connection with contingency planning. An example of this can be a cyber attack over the internet.

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»[13] describes this type of event. The event, the outcome and relevant variables are completely unknown to the organisation.

In connection with strategic risk it may be helpful to imagine 2 or 3 possible scenarios dependent on possible future developments in framework and market conditions and technologogical innovation. Each of these possible futures could then be analysed further by risk management for their possible impact on the enterprise. Even if none of the scenarios are in fact realised the exercise will in itself add to management's awareness of critical elements in the organisation and the ability to monitor trends so that appropriate and timely action can be taken.

See Appendix 3 Risk in decision-making for further detail.

[12] 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.
[13] Nassim Nicholas Taleb, The Black Swan 2007, Random House.

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 organisation's overall risk management and internal control structure.

The Enterprise 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 6) provides a high-level overview of the roles and responsibilities for internal control and risk management. Even in organisations where a formal risk management framework or system does not exist, the model can help improve understanding of the organisation´s ERM and internal control.

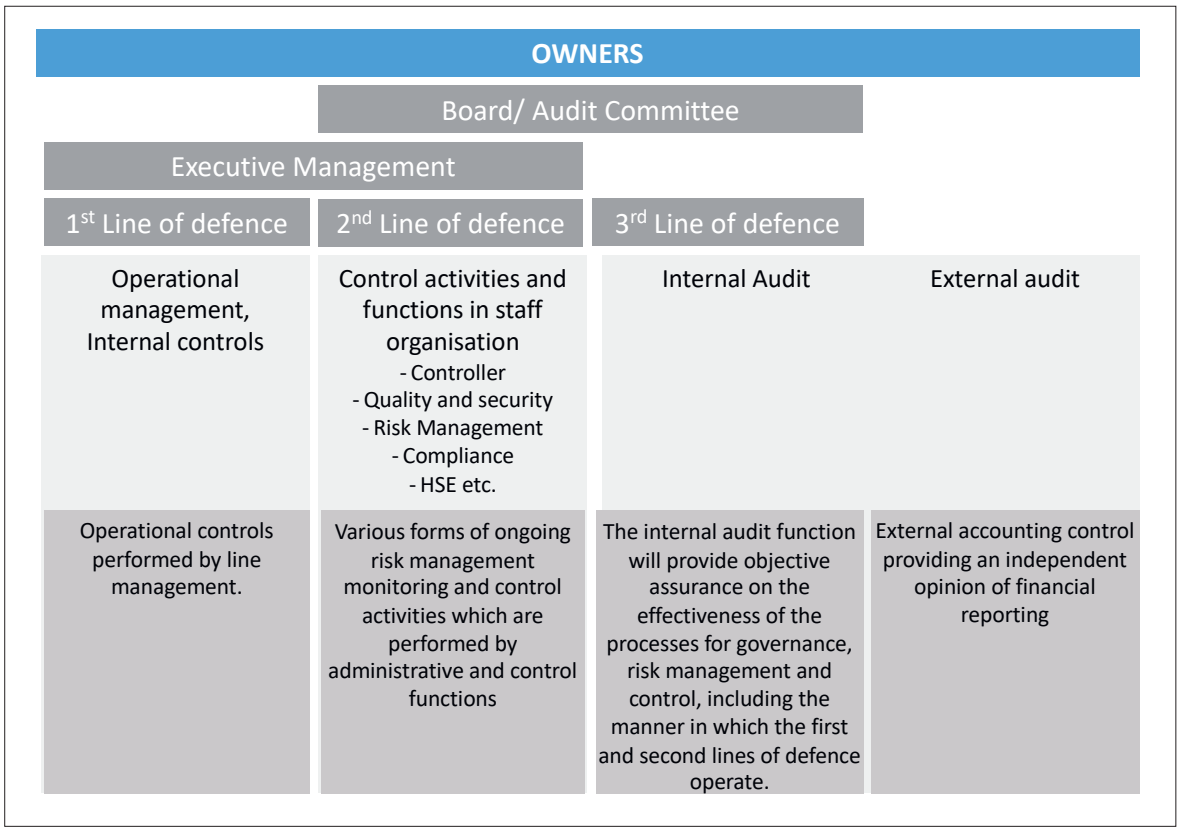


Figure 6 Description of the three lines of defence

The model distinguishes between three groups (or lines) that are involved in effective internal control and risk management:
- Functions that own and manage risk (first line)
- Functions that exercise oversight over risk (second line)
- Functions that provide independent assurance (third line).

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 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.

The support and control activities in the second line are, for example, performed by IT security, Finance, Compliance, Risk Management, Health and Safety, Legal and Quality Management. The specific functions will vary by organisation 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. The activity includes assessing whether the first and second lines of defence are working efficiently and effectively, and are contributing to the organisation'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 Co-operation between 2nd and 3rd lines of defence

Functions in the 2nd and 3rd lines of defence 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 Chief Audit Executive is required to "establish a risk-based plan to determine the priorities of the internal audit activity"[14]. Internal audit will in this context need to understand the risks the organisation faces and an important input to this process will be the documentation provided by the Risk Management and Compliance functions.

To facilitate communication with the executive management and the board it is important that both Risk Management, Compliance and Internal Audit functions develop a common vocabulary and taxonomy as far as this is practicable.

A relationship built on openness and trust will mean that internal audit will be better able to focus its efforts in those areas where monitoring by the Risk Management and Compliance functions are weaker. By challenging the CRO and CCO the head of internal audit will provide an important element of quality assurance to those functions.

3.3 The position of the Enterprise Risk Management function in the organisation

The Enterprise Risk Management function´s organisational positioning will vary depending on the characteristics of the organisation and its maturity level in respect of ERM. (See further Appendix 2 Risk Maturity). Many frameworks recommend that the Enterprise Risk Management function shall report to Executive Management without specifying its positioning in greater detail.

In some organisations, the responsibility for risk management is assigned to a separate unit independent of line management and with a reporting line directly to the Chief Executive. 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. If the Enterprise Risk Management function reports administratively to a lower management level than the CEO e.g. to the CFO, it is important to ensure an independent and direct reporting of risks to the CEO, allowing for an objective evaluation of all activities including those reporting to the Enterprise Risk Management's administrative superior manager (e.g. the CFO).

In order to ensure a well-functioning Enterprise Risk Management function, it is necessary that both the Enterprise Risk Management 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.

[14] *IIA performance standard 2010*

The Enterprise Risk Management 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.

These examples show that there is no one right answer as to where the Enterprise Risk Management function should be positioned in the organisation. Before deciding where the Enterprise Risk Management function should be positioned Executive Management should assess; what will be the function´s areas of focus, with what other parts of the organisation the Enterprise Risk Management function will interact to achieve synergies and professional co-operation, and what level in the organisation will lead to the Enterprise Risk Management function exercising its responsibilities in a satisfactory manner.

3.4 Mandate, authority, competency and resources

The organisation should appoint one person with the overall responsibility for the Enterprise Risk Management function. That person and all people performing tasks within the Enterprise Risk Management function must 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 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.

3.5 Independence and integrity

People employed in and responsible for the organisation´s Enterprise Risk Management function, should as far as possible be organised independently from operational 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 affect the business operations. Persons employed in the Enterprise Risk Management function shall equally not work in units that they themselves are responsible for monitoring.

Some, and especially smaller organisations, will not be in a position to establish a separate and independent 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 Enterprise 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 Enterprise 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 Enterprise Risk Management function must possess, in addition to a relevant professional competency, a high level of professional integrity. Additionally, the function head must have adequate authority and experience to take responsibility for the development and communication of the risk management framework. Professional integrity is decisive to achieve confidence in the function and the function´s value contribution. 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 Enterprise 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 Enterprise Risk Management function´s responsibilities and tasks, as well as an organisation, access to information and reporting that supports this mandate.

3.6 Access to information

The Enterprise Risk Management function should have access to the required information regarding the organisation´s operations and its decisions. 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 Enterprise 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.

3.7 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 Enterprise Risk Management function should not contain significant financial 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.

3.8 Reporting requirements

Irrespective of how the Enterprise 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.

3.9 Outsourcing the ERM function

If management chooses to outsource all or part of the Enterprise Risk Management function, it must ensure that the fundamental requirements of an Enterprise 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.

APPENDIX 1

A PRACTICAL APPROACH TO ERM AND TOOLS FOR DEVELOPING RISK MANAGEMENT IN AN ORGANISATION

1 Framework and standards

First identify risk management frameworks/standards including those which relate to your business field.

There are two relevant general standards/frameworks which are internationally accepted. These are:

1. ISO 31000:2018 - Risk Management –Guidelines

ISO 31000 Risk Management –Guidelines is an international standard which was last updated in 2018. It describes the *principles, framework* and *process* of risk management. These components may already be established in the organisation, but there can be a need to tailor and improve them in order to achieve an efficient, effective and consistent risk management.

According to the *principles* the purpose of risk management is defined as being the creation and protection of value which shall contribute to improved performance and innovation as well as support the achievement of objectives. Risk management shall be integrated, structured and comprehensive, customized, inclusive, dynamic, provide the best available information, take account of human and cultural factors as well as be based on the principles of continual improvement.

The *framework* for risk management consists of integration, design, implementation, evaluation and improvement.

The risk management *process* consists of the following elements: definition of scope, context and criteria, the identification, analysis, evaluation and the treatment of risk. The process takes place within overall requirements for communication and consultation, recording and reporting as well as monitoring and review.

The overall objective of ISO 31000 is to integrate risk management into a strategic and operational management system. In the 2018 version emphasis is placed both on the role of management and the central principle of value creation and protection.

The standard underpins a disciplined decision-making process in respect of activities, which affect risk and return and thereby it contributes to the organisation´s achievement of planned objectives. The standard is applicable irrespective of sector, type and size of organisation.

2. COSO: Enterprise Risk Management – Aligning Risk with Strategy and Performance, June 2017

It was explained in chapter 1.5 of these Guidelines addressing risk management and internal control that COSO published a framework for ERM which builds further on the framework for internal control. The aim of the 2004 publication was to help organisations to improve protection as well as value for stakeholders. The underlying philosophy was that value is maximised when management sets a strategy and objectives which achieve an optimal balance between goals for growth, return and related risks, and the utilisation of resources.

The updated version of COSO ERM which was published in 2017 emphasises the importance of evaluating risk both in the strategy process and in activities aimed at the achievement of goals.

It is stated that ERM is as much about understanding the implications of strategy and the possibility of non-alignment of strategy as it is about managing risks to set objectives. The organisation's management of risk is therefore the basis for identifying strategic opportunities and opens for the development of important characteristics of the organisation.

The framework delineates five components which together constitute ERM:
1. Governance and culture
2. Strategy and objective-setting
3. Performance
4. Review and revision
5. Information, communication and reporting.

These five components are supported by a set of 20 principles. These principles cover everything from governance to monitoring. They are manageable in size, and they describe practices that can be applied in different ways for different organisations regardless of size, type, or sector. COSO maintains that adherence to these principles can provide management and the board with a reasonable expectation that the organisation understands and strives to manage the risks associated with its strategy and business objectives.

2 Designing a framework in practice

Every organisation should adopt its own risk management framework. The complexity of the framework must be proportionate to organisation's maturity level. (see appendix 2).

A common denominator for the current standard and framework is the understanding 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 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 by using 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 organisations 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 of 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 organisation's 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 policy and appetite. The Chief Executive appoints a head of the risk management function. Risk owners are identified for all risks.
- Risk owners determine meaningful and measurable objectives and control mechanisms which are accepted throughout the organisation.
- A centralised Risk Management function is responsible for establishing, maintaining and developing 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 promoting 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.

3 High-level risk assessment in 3 steps

Analyse your organisation's strategic objectives regarding risks. A risk analysis should start by taking a high-level objective and breaking it down into more tactical, operational performance indicators. Use the strategy document, financial model, business plan or the budgeting model to determine key assumptions made by the management.

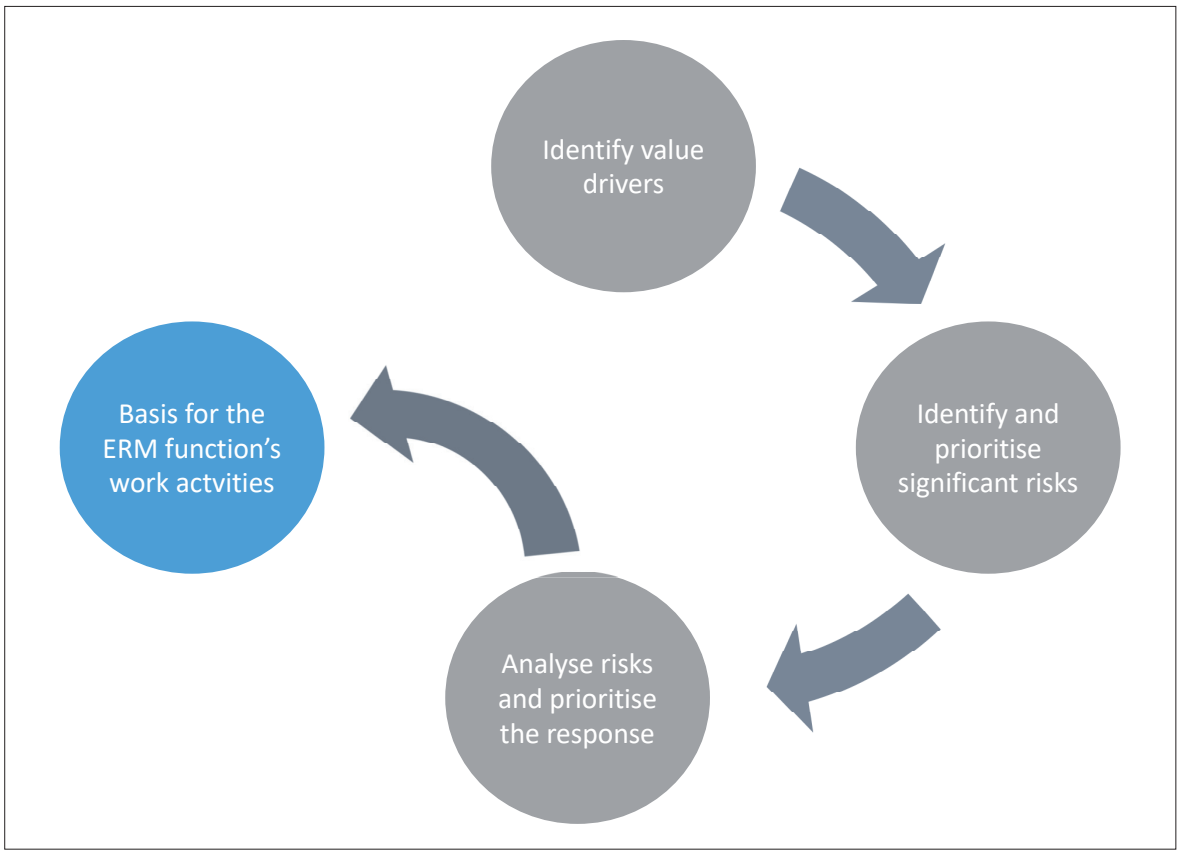
An organisation which has never previously performed a high-level risk assessment may do this through a simple three-step process (cf. app.1 figure 1):

1. Identify and define the organisation's value drivers i.e. ask the question «why does this organisation exist, and what can influence the achievement of objectives in both a positive and negative direction? » In this regard «value» can be interpreted widely. It can, for example, include life and health or the fulfilment of a public mandate, as much as costs and value in monetary terms.

2. Identify, evaluate and analyse major uncertainty which can have an effect on the value drivers. This includes both those elements that can lead to a more positive outcome than expected as well as those that can lead to a more negative outcome. All risks should be evaluated as to whether

they should be managed (by actively addressing and monitoring), shared (by sharing the risk exposure with another party or by purchasing insurance) or avoided (by changing operational activities or fully insuring). As a part of the management of risk, it is possible as an alternative to consciously increase the risk exposure.

3. Uncertainty may be quantified in terms of likelihood and impact, and should be the basis for the work to be performed by the Risk Management function. When using such a measure it is important to clearly define the criteria for the various levels of likelihood and impact. In this respect impact should be defined in respect of various categories, such as finance, achievement of objectives, health and safety, and reputation. Likelihood can also be evaluated in respect of uncertainty which it is not possible to calculate based on historical experience by performing a qualitative evaluation of the probability of such a situation occurring at some time in the future. Organisations that do not measure the achievement of objectives in monetary terms should define intervals for impact based on degree of impact on objectives/mandates.



App.1 figure 1 3-step process for performing a high-level risk assessment

4 A 17-point plan for the establishment of a risk management function in the organisation

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

1. Prepare a mandate and job description for the function and define the role in the organisation as well as reporting lines. Ensure the Risk Management function has support and is understood at the Executive Management and Board level, their support will provide the "tone at the top" for the whole organisation.

2. Appoint a person to lead ERM initiatives with the appropriate experience and competency. Ensure there is provision of resources to build a function that has the required level of integrity.

3. Create a Roadmap (implementation plan) which describes steps to be taken for creating an ERM function.

4. Approve a policy for the implementation of risk management, including the framework to be used, responsibility and reporting. Risk management should be defined as a responsibility for all employees in the organisation.

   Evaluate the need to buy/ develop a support system for enterprise risk management which can facilitate the establishment of the entity´s risk profile and the management of risks.

5. The ERM function should encompass all types of risk including uncertainty in strategy and decision-making, operational and financial risks, political risk, regulatory risk etc. The function should also focus on actions taken to treat risks based on adverse events e.g. adequacy of insurance coverage and «business continuity management».

6. All major decisions of an organisation (for example making an investment, entering into a contract etc.) and key processes (for example procurement, asset management etc.) should be identified as the basis for the identification of risks relevant to those decisions and processes. Every major decision should include and take account of a comprehensive risk analysis.

7. The Board and Executive Management defines risk appetite for every risk category and describes how an organisation can ensure that risks are kept within agreed parameters and where relevant upper and lower limits.

8. Communicate the implementation plan to the organisation and perform risk evaluations, starting from a risk-based evaluation of the organisation's strategic goals. Decide on the principles for the management and measurement of risk.

9. Include risk discussion into the agenda of the board of directors and top management meetings.

10. Consider the creation of a risk committee to address the risks associated with important investment, project and other decisions and to evaluate major risks and mitigation plans.

11. 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 for education and experience, as well as describing a development path.

12. For better risk identification cooperate with persons responsible for related functions such as Quality, Health, Safety and Environment, LEAN, financial controlling etc.

13. In larger organisations, it may be effective to establish also Risk Management in the first line in addition to a centralised function which is concerned with the enterprise taken as a whole (the ERM function).

14. Perform regular communication of the status of risk culture, risk exposure, risk appetite, risk evaluations and any emerging risks as well as changes to existing risk profiles.

15. Risk communication should as far as possible be pro-active and it is important that all risks have an owner.

16. A structure should be established to ensure that the centralised risk management unit works closely with the strategy function and business management.

17. Report regularly to the Board (preferably on a quarterly basis) and plan activities for the following periods.

5 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 the following:

Reason for failure	Why/how to challenge that
1. Lack of understanding that any organisation is exposed to risks, thus needs a risk management function	All operational activities, service provision and business ventures involve risks. Awareness of this fact should lead to informed decision making processes (i.e. using risk management techniques) and will increase positive and reduce negative outcomes for the organisation
2. 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.	Common goals within a culture of constructive challenge will improve the ability to attain overall objectives.
3. Lack of a link between strategic objectives and risk management.	Risk management informs the ability to utilise resources efficiently in the achievement of strategic objectives.
4. Imprecise mandate leading to lack of understanding of the role of the Enterprise Risk Management function and the division of responsibilities.	It is important that risk management is understood to be a responsibility of all members of the organisation. The ERM function facilitates effective risk management and provides insight into decision-making at a global level within the organisation.
5. Formal risk management regulations are too complicated which leads to ineffectiveness of the ERM	There needs to be structure to the management and reporting of risks, however it is important not to lose sight of the fact that the objective is to achieve an overall picture of risk enabling effective decision making.
6. The CRO 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 CRO should have an executive management understanding of the business in addition to an essential understanding of the concept of risk management. These skills and knowledge should be combined with a creative mindset open to new ideas and solutions. The organisation should allocate resources to a risk management training budget.
7. The CRO does not understand the activities of the organisation.	A lack of a fundamental understanding of the business can lead to decisions being made that harm rather than enhance the business.

Reason for failure	Why/how to challenge that
8. The risk management concepts are not understood or are misunderstood.	A focus on only downside risk can lead to a false perception that the ultimate goal is the elimination of all risks. Such an objective will surely prevent the organisation from achieving its objectives.
9. Lack of ownership of the system tool used.	A risk management tool to be effective must be appreciated as a practical way to achieve good management and effective business decisions.
10. A tool is used without understanding its weaknesses and limitations.	A tool will never be able to give a full picture of the organisation's risks, therefore limitations must be understood to enable a critical focus to decision making.
11. There is insufficient focus on developing and implementing a sound risk culture. Discussion is not encouraged, and 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».	A culture of openness and constructive criticism will build a resilient organisation.
12. Lack of prioritisation of significant risks.	Blind spots in respect of certain significant risks can have material adverse consequences for the organisation.
13. Lack of understanding/ knowledge of correlation between risks.	There is a risk of sub-optimisation of risk management and even worse increasing risks when believing they are being reduced.
14. There is no understanding of what decisions should be made as a result of a systematic risk analysis	Risk management should inform sound decision-making at all levels.
15. Lack of management/ monitoring of IT risk	Information is a valuable and vital component of any organisation. Risk management plays a crucial role in understanding risks and advising the investment decisions in respect of information security.
16. Lack of focus on change in the risk profile and emerging risks.	All organisational activities exist in a changing environment and it is important to be aware when established truths may no longer be valid in order to improve decision-making.

Reason for failure	Why/how to challenge that
17. The organisation is not convinced of the value of risk management efforts resulting in a lack of commitment.	As all employees in organisation make decisions on a daily basis that involve risk taking, the quality of those decisions can only be enhanced by a better understanding of the role of risk management-
18. The organisation and responsibility are unclear between the Head of Enterprise Risk Management and the risk owners.	The Enterprise Risk Management function should be clarified as being a facilitator to improve the decisions of risk owners as well as assisting in appropriate decisions at a global level in the organisation.
19. Personal risk management dominates over ERM.	If managers are making decisions solely based on their area of specific expertise, then there is a risk that those decisions may be sub-optimal for the organisation taken as a whole.
20. Work performed by the various control functions is uncoordinated.	An organisation may have a number of specific control functions e.g. quality, compliance, risk control, financial control, information security. It is important that there is a common understanding of the role of control within Enterprise Risk Management and that ineffective approaches and the duplication of tasks is avoided.
21. There is damaging competition/ professional rivalry between the Head of Risk Management and related functions e.g. Quality Management, Compliance and Internal Audit	It is important to have common shared goals for the objective of these functions and avoid sub-optimisation
22. 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.	Risk evaluations should as far as possible be quantified to achieve a common and comparable measure. There will always be uncertainty as regards the reports made but it is important to strive to achieve a "best estimate" figure as a basis for discussion and decision-making.
23. Risk evaluations (both in respect of upside and downside risk) lack clarity and precision in their formulation. Adjectives such as "satisfactory", "sufficient", "reasonable", "optimal" are used, which will be understood and interpreted differently from one person to another.	Qualitative risk evaluations should as far as possible be further defined, preferably in monetary terms, or failing that by reference to a benchmark for materiality.

Reason for failure	Why/how to challenge that
24. Lack of quality assurance measures in respect of analyses/evaluations.	As analyses and evaluations will be relied upon in the decision making process it is important to have in place a quality assurance process in respect of all reporting. Best practice would be also to achieve an annual review of a risk analysis/evaluation model for every risk category in every structural unit.
25. Lack of a holistic view to reporting where differing formats for risk evaluation hinders aggregation at a higher level.	The CRO should create a model for consolidated risk reporting. It may happen that one type of risk can be assessed at a different level for different structural units (for example, subsidiaries). However, in absolute figures risk levels are the same. For example, for a larger subsidiary a loss of € 100.000 may be considered a low risk, but for a smaller subsidiary it can be an extreme risk. Failure to apply a correct aggregation model may mean that a particular risk category (for example, IT-risk) could be shown as high for a whole group of companies, whereas the risk is in fact low.
26. Poorly identified internal and external sources of information needed for risk identification. Such sources can be, for example, different financial and management reports, incident reports, client feedback sheets, LEAN reports, reports from the quality department, external auditors etc.	Enterprise Risk Management is concerned at assisting top management to understand the organisation's activities and the uncertainty of the achievement of goals taken as a whole, for this reason the picture presented should be informed from a multitude of sources.

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

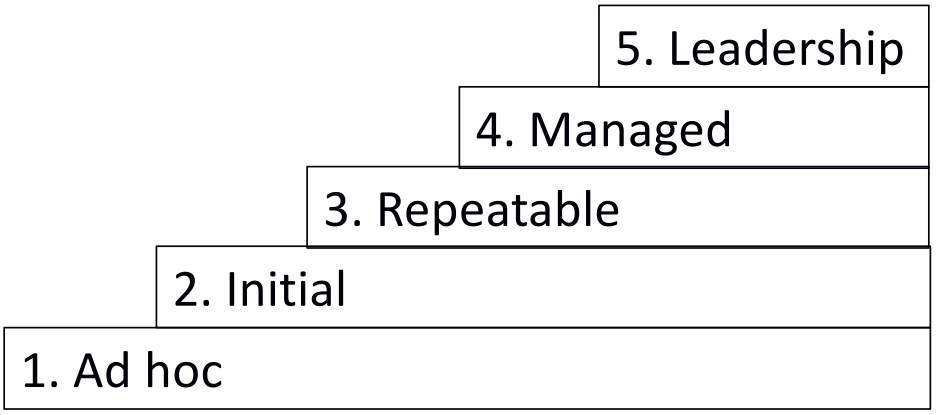
APPENDIX 2

ERM MATURITY IN AN ORGANISATION

1 Traditional approach

The traditional approach to developing a maturity model is to see the development as a set of steps in a ladder where one maturity level, after further development and refinement, leads to attainment of the next level before the ultimate goal is reached. The "Capability Maturity Model"[1] was originally developed as a tool for objectively assessing the ability of US government contractors´ processes to implement a contracted software project.

A maturity model for ERM has been developed by "RIMS, the risk management society". The model was named the RMM[2] (Risk Maturity Model) Approach and it allows for the following 5 maturity levels from Ad hoc to Leadership:



App.1 figure 1 Maturity levels in the RIMS maturity model

The model is comprehensive and is based on seven key attributes:
1. Adoption of ERM processes
2. ERM process management
3. Risk appetite management
4. Root cause discipline
5. Uncovering risks
6. Performance management
7. Business resilience and sustainability

[1] *M.C. Paulk, B. Curtis, M.B. Chrissis, and C.V. Weber, "Capability Maturity Model, Version 1.1," IEEE Software, Vol. 10, No. 4, July 1993, pp. 18-27*
[2] *https://www.riskmaturitymodel.org/rims-risk-maturity-model-rmm-for-erm/*

Each attribute includes a set of competency drivers which outline the key readiness indicators (or activities) involved in achieving each driver. There are in total 25 competency drivers and 68 key readiness activities in the model. These driver/indicator pairs cover the entire risk management process including administration, outreach, data collection and aggregation, and analysis of risk information.

A maturity score is provided for each driver as well as an overall maturity score for the entire risk management program. Scoring is based on a 5-level scale, with Level 1 indicating the lowest risk maturity and a Level 5 representing the highest maturity.

The model is freely available and may be accessed online allowing an organisation to use the model to calculate its own ERM maturity.

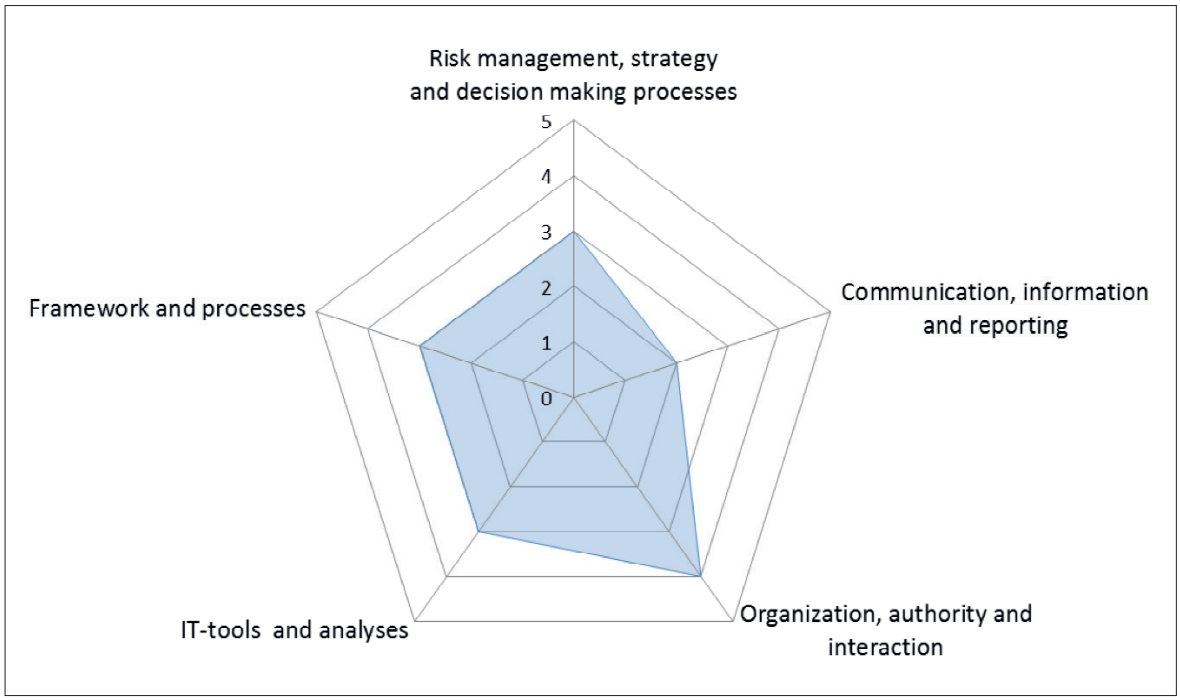
The traditional approach has two important assumptions:
a) The risk maturity process is a "progress". An organisation does not fall back to lower maturity levels. Many organisations experience organisational and technical changes or market constraints which do not allow such progress.
b) A maturity level is uniform and applies to all aspects of the organisation. In reality an organisation for instance may be good at IT- procedures and reporting but may not have the same degree of achievement at communications.

2 A fresh approach to risk maturity

Ayse Nordal and Ole Martin Kjørstad, members of IIA Norway's Risk Management Network, developed in 2017 an alternative and simplified approach to risk maturity[3]. Fundamental to this approach was a realisation that ERM development is seldom linear. At times certain aspects of ERM can develop well whereas at other times they can stagnate and even regress. In this proposed new model, the focus is not on maturity levels but rather on maturity objectives. Maturity objectives have been defined for the following 5 dimensions:
1. Risk management, strategy and decision-making processes
2. Communication, information and reporting
3. Organisation, authority and interaction
4. IT tool and analyses
5. Framework and processes

[3] *"Modenhetsmodell risikostyring" published by IIA Norway https://iia.no/product/modenhetsmodell-risikostyring/ and is available in English upon request*

Within each dimension there are a set of 10 criteria which must be fulfilled to achieve full maturity within a dimension. A score is then based on the number of criteria. The results then be shown graphically for example in a spider chart (see figure 2). This graphical presentation makes it easier to identify where efforts for improvement should be applied and show development over time. It may also be used to benchmark against other organisations where this information is available.



App.1 figure 2 Presentation of the result of a risk maturity evaluation

Since being published on the internet the proposed ERM maturity objectives model has received recognition internationally as a fresh and new approach to ERM maturity modelling.

APPENDIX 3

RISK AND DECISION-MAKING

1 Quantifying risk

All decision-making involves weighing up the consequence of a proposed course of action. The exception being in the rare case of split-second, intuitive decision-making. It is in this process of weighing up the consequences that risk management can have a role to play by applying a disciplined, structured and objective approach. Risk management techniques allow the computation of probable outcomes from a given course of action.

A key technique will be the calculation of a set of probable outcomes based on estimated probability and estimated impact. In these calculations it will be normal to base the outcome on historical data either internal or available from the market, assuming that such data exist. If the decision involves an area where we do not have historical data at all (for instance: first time in the market with a completely new product) we can use scenario techniques and/or interviews to support our decision.

For certain risks such as high impact and low probability events it may be necessary to replace historical data with best estimates. The advantage gained by quantifying risk, even if the result of the computation is "ball park" rather than millimetre accuracy, is that it allows the entity to compare alternative courses of action in a neutral medium (i.e. currency value). This can be especially important when deciding how much to expend on risk mitigation techniques in a cost-effective manner.

It is common to colour code (green, yellow, red) especially in the area of operational risk assessment based on impact and probability. In this case it is important that the relative seriousness of impact is also defined in monetary terms. If this is not done, then it will be exceedingly difficult to measure risk for the organisation as a whole as one person's perception of materiality will likely differ from another (for example in an area of greater value of monetary transactions).

2 Decisions and risk management involvement

Decision-making in an organisation may be categorised into a number of areas:

1. Day-to-day decisions (operational decisions)

A lot of the decisions made on a daily basis in an organisation will be based on established parameters e.g. pricing and discount policies, procurement policies etc. The risks associated with this business will be delineated in advance and monitored after execution based on approved budget as well as risk appetite establishing and monitoring processes.

In addition, there will arise certain and more complex business decisions involving a greater risk exposure for the organisation. In these circumstances there will often be a pre-requisite for the direct involvement of risk management techniques in analysing the risks and evaluation of possible outcomes. It will also be natural that these decisions will require a number of experienced persons and specialists to be involved in the process.

2. Strategic decisions

Strategic decisions may be further sub-divided into short to medium term (1-5 years) or longer term.

Short to medium term decisions (tactical decisions) can encompass everything from modelling of budget development for the next 5 years to acquisition of a business or investment in a new IT system. The role of risk management in this process will be to assist in an evaluation of the possible outcomes based on historical information combined with the application of expert judgment. Unlike a financial forecast that may typically present one version of future development, risk management should normally be in a position to provide a range of possible results based on probability of outcome. This will allow key decision-makers at the executive management and Board level to weigh up the possible outcomes and make an informed decision.

Longer term strategic development will involve a greater degree of uncertainty and perhaps never more so at the present time with digital development and innovation combined with the possible upheavals caused by climate change and global political rivalries. In these circumstances risk management will also have a role to play. One role is through acting as a radar to pick up on emerging risks and communicate these to senior management and the Board. Furthermore, this insight can be brought into the development of possible strategic scenarios. Each scenario being a separate "story" of a plausible future development. The risk manager can contribute in quantifying the outcome of a scenario. Even if the scenarios developed do not arise in practise they will increase the understanding of the vulnerabilities of the organisation and the awareness of adverse signals as they appear.

3. Contingency planning

Not all risks can be managed and especially in the case of high impact and low probability events the only mitigating action will be to set contingency plans which may apply in response to extreme events such as caused by natural disasters and computer hacking. Risk management's role may be to help in the identification of these outlier events and help the organisation ensure that relevant contingency plans are developed. The general awareness of contingency actions may contribute to rapid reaction time as they become reflex actions of the organisation.

3 Conclusion

Risk management through its area of expertise will be rightly involved and contribute to decision-making at many levels in the organisation. Risk management in an ERM framework will bring a holistic version of risk taking account of the consequences and impact for the organisation taken as a whole and the CRO should be an important advisor to the organisation at all levels as well as to the Board.

APPENDIX 4

RISK APPETITE

1 Risk appetite vs risk tolerance

Risk appetite expresses the level of uncertainty an organisation is willing to take on in order to carry out its activities and realise its goals. Risk appetite should always lie within the organisation's tolerance limit to absorb risk. Risk tolerance may therefore be defined as the level of risk an organisation is able to absorb without significantly impacting the achievement of its strategic objectives. This means that risk appetite can be decided by the management and the board, while risk tolerance is more of a given based on the organisation's financial robustness, the enforcement by authorities, or other external factors determining the impact when a risk materialises.

Both risk appetite and risk tolerance normally increase with a commercial organisation´s performance. Firstly, because profits require investment and action, and neither is possible without also taking risk – hence the ambition for higher profits requires a higher risk appetite. Secondly, profits increase a commercial organisation´s financial robustness and hence also increase the level of risk tolerance.

We experience that many organisations do not distinguish between risk appetite and risk tolerance in their ERM model, but operate only with one of the terms, more often risk appetite. However, we believe it is useful to be aware of the difference.

As risk appetite is actively decided and can be subject to changes based on strategic choices, companies with advanced ERM normally manage by risk appetite limits. We therefore choose to focus on this term in this document.

2 Setting the risk appetite profile

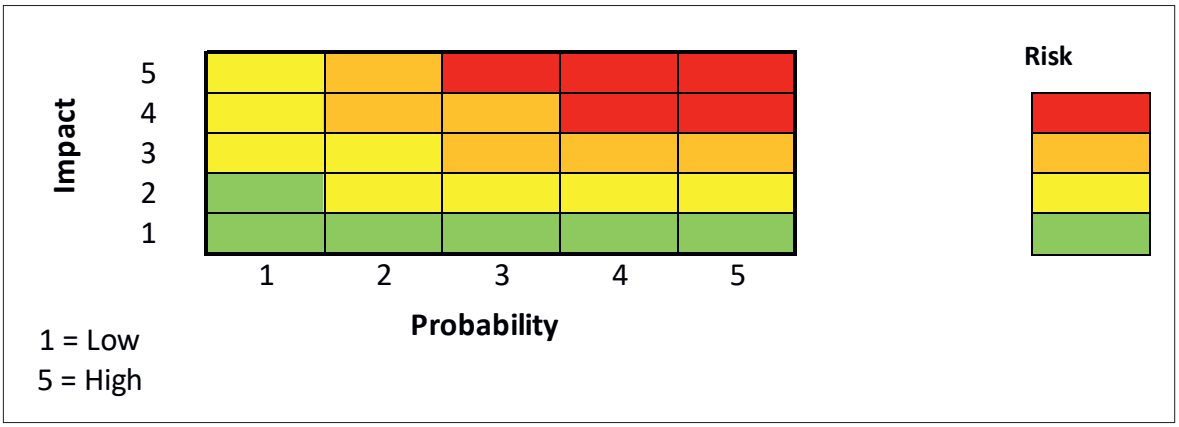
The nature of an organisation's risk appetite depends on the type of risk the organisation has appetite for. Quantitative risk types can be monitored and managed by measurable limits; not more than x % or Y million of credit loans (which can be lost) can be provided to certain segments, not more than x % of the organisation´s annual investments (which can be lost) shall be within certain markets and so on.

For non-quantitative risk, such as compliance risk, one may still operate with certain measurable criteria; for example the organisation may decide that it cannot accept the occurrence in the course of the year of any major violation of the General Data Protection Regulation (GDPR), but may accept 10 minor violations of the same regulation. If the organisation is to enter into new business segments or is to run a cost efficiency project, requiring implementation of new systems and new processes, the organisation may be willing to accept a certain increase in operational risk, measured by customer complaints within a limited time horizon.

However, in many cases, the risk appetite is not set in numbers or at very granular levels, but limited to low, medium or high. Also, some companies may set the risk appetite level for certain risk categories based on the impact; e.g. any activity that may be associated with a potentially critical impact, regardless of likelihood, is outside the organisation´s risk appetite. For example, an organisation may wish to minimise the risk of corruption as a corruption case may have a severe

impact on the entire organisation, and hence the organisation may wish to have a presence in certain markets or regions where corruption is part of the business culture.

The illustration in app.4 figure 1 shows an organisation's risk profile set as a balance between the performance and the risk level. The green area defines the desired performance and given risk appetite. For a bank, the risk could be the amount of loans going into default the bank expects given a certain performance level, for a technology company it could be R&D-investments potentially failing to reach a certain profit level. While the latter may be harder to measure within a short time span, it might still be useful to apply the risk appetite approach when making decisions on which projects to invest in – what is the likelihood of a project failing and how much money the organisation is willing to risk losing.



App.4 figure 1 Risk matrix

APPENDIX 5

QUESTIONS A BOARD MAY ASK TO UNDERSTAND HOW AN ORGANISATION CONTROLS ITS RISKS

RESPONSIBILITY FOR RISK MANAGEMENT

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

The aim of this appendix is, through the presentation of a set of questions, to give a better understanding of the most important risks which can influence an enterprise and how these may be managed.[1]

Reading the financial statements will seldom give sufficient information to understand the key drivers of an organisation´s bottom-line results. An understanding of the enterprise´s risk profile and how this is managed is an approach which can give valuable insight into the business. The definition of «risk» used in this appendix is «the effect of uncertainty on objectives» and «the effect» is defined as a «deviation from the expected — positive and/or negative» (cf. the definition used in the ISO standard on Risk Management[2]).

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

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

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

[1] For further information regarding the objective and practical performance of risk management cf. Guidelines for the Risk Management function published by IIA Norge in 2017 (in both Norwegian and English translation)
[2] ISO 31000:2009 - Risk Management – Principles and Guidelines

GOVERNANCE

- How is the organisation´s Risk Management function organised? Is it organised per business area and only thus, or is there an ERM function which looks at the enterprise as a whole.

Background: It is important to understand if the organisation manages its activities based on a holistic view of the risks the organisation is exposed to or only a partial view.

- How does risk management carry out its reporting? Does it report exclusively to the Executive Management or to the Board including Risk and Audit committees or to both of these stakeholder levels?

Background: If the board is to be in a position to place reliance on the robustness of risk management it is essential that there is a high degree of professional integrity amongst those who are responsible for the function and moreover that there is a facility for directly communicating with the Board should the situation arise that the Risk Management function does not share Executive Management´s view in respect of a critical situation/case etc.

- Are the organisation´s risk management and internal control processes aligned with the organisation´s goals and policies?

Background: It is vital that both policies and processes are aligned with the strategy and associated risks.

- Is the adequacy of resources in the Risk Management function regularly evaluated against requirements and compared to similar organisations?

Background: It is important that the Board understands whether the organisation has evaluated whether resources are in line with the scope and ambitions required by the risk management strategy.

RISK MANAGEMENT

- How is the competency and professional integrity of risk management employees evaluated? Is there a structure for systematic education/professional development in the risk management area applicable to both managers and staff?

Background: It is important for the Board to understand whether the organisation is able to develop the required level of competency in this professional area.

- What activities has the Executive Management initiated to support a sound risk culture? Is risk ownership clearly delegated?

Background: It is important not to encourage the failure to take responsibility, or the development of an unhealthy risk culture e.g. through bonus and remuneration systems based on sub-optimal incentives.

- Does the Risk Management function share information regularly with internal audit?

Background: It is important to have in place a frank and open dialogue between the organisation´s Internal Audit and Risk Management functions. Internal audit is required by international standards (published by IIA) to take account of the enterprise´s risk picture in the following specific areas:
– Preparation of a risk-based audit plan
– Evaluation of the enterprise´s strategies, objectives and risks
– Audit work aimed at improving processes for governance, risk management and control
– Inclusion of material risks in the reporting to Executive Management and the Board.

- Has it been considered how the risk management system shall be integrated with other parts of the internal control system and how the Risk Management function shall co-ordinate its work with other control functions such as Compliance, Quality Audit and Internal Audit?

Background: It is important for the Board to understand whether related professional environments co-operate to avoid duplication of work, overlapping roles, development of two conflicting sets of terminology etc.

- How is the risk picture communicated to the Board both in respect of form (quantitative/qualitative), content and frequency?

Background: It is important to understand how hands-on the Board is able to be. Is the risk information sufficient for the board to act before an unwanted outcome is reality or is the Board limited to acknowledging in retrospect that the event happened?

- How are significant emerging risks identified before they are reality; the same question applies to material control weaknesses, are these communicated and reported to Executive Management and the Board?

Background: It is important that changes in the risk picture as a result of external factors and identified weaknesses are communicated to Executive Management and the Board. It is usual to have in place a system for registering material loss events and that these events are reported to management and the Board.

COMPLIANCE

- Is the organisation´s Compliance function part of a staff unit reporting at a sufficiently high level within the organisation? If not, who does Compliance report to?

Background: it is important for the Board to understand where responsibility for the enterprise´s Compliance function lies within the organisation and whether it operates independently of the organisation´s risk management and other risk processes.

- Is the Compliance function, however organised, responsible to monitor both internal and external regulations and guidelines? What regulations and guidelines (internal and external) are included in the Compliance function´s area of responsibility?

Background: It is important that the Board understands the extent of Compliance work, who is in fact leading it if the function happens to be split as well as Compliance priorities and how these are communicated.

MANAGING BUSINESS RISK

- Does the enterprise have a high-level risk strategy and if so who is responsible for this?

Background: It is important that the Board understands whether the organisation sees risk management as a strategic and integrated part of business development.

- Has the enterprise articulated a risk appetite which is holistic and quantifiable?

Background: It is important that the Board understands both to what extent a risk appetite has been formulated if at all. If one has been formulated how much of the enterprise´s profitability and risk capital has been tied up as a result of the risk profile?

- What are the organisation´s most important value drivers?

Background: It is important that the Board understands the main source of value creation in order to appreciate the risks which can affect the value creation both in a positive and negative direction.

- Has the organisation quantified the risks which can affect the most critical value drivers and is there a reasonable connection between allocated risk capital and expected profitability?

Background: A quantitative measure ensures a common language which most people will understand. One million US dollars will mean the same to everyone whereas a yellow flag on a risk chart is more open to interpretation. A quantitative expression ensures an easier comprehension of the connection between value creation and potential loss that may arise in the process.

- What is the enterprise´s strategy in relation to the most critical value drivers both in a short-term and long-term perspective?

Background: Recent research shows that many organisations are exclusively focussed on the coming few months whilst the greatest effect on the business will be what happens to strategic risks. Strategic risks often have a major effect but still are paid little attention because they are more difficult to articulate, and it requires a degree of co-operation between the strategy unit and risk management (something which is gradually becoming more and more common).

- Have risk management and hedge strategies been developed and are these evaluated in relation to securing against fluctuations in profitability or balance sheet values? Does the organisation´s risk management also take into account taxation effects?

Background: accounting rules for hedging can be both inflexible and may not be aligned with the enterprise´s high level economic exposures e.g. from an economic perspective the management of risk should be post tax as it makes little sense to protect more of the profit than the enterprise will end up with after tax has been charged.

- Is the set up for risk communication between Executive Management and the Board pro-active or reactive?

Background: In order to understand and influence strategic development it is important to obtain forward-looking information. In this way a Board may to a greater extent be a contributor to and owner of important decisions proactively.

- Are decision making documents both to management and the Board adequately focused on shedding light on the underlying risk aspects? In critical cases the decision making document should detail both potential impact and probability based on a risk perspective.

Background: An objective a risk picture as possible is an essential element in ensuring a relevant basis for a decision.

- Does the enterprise have major positions/ exposures which can lead to major differences between the economic outcome and the accounting profit and loss?

Background: As a result of accounting requirements it is possible that major differences can arise between the economic outcome and the accounting profit and loss e.g. in respect of hedging of future income and costs in foreign currency.

MANAGING OPERATIONAL RISK

• Has the enterprise discussed which operational risks may have the greatest impact on net profit?

Background: It is important to clarify and reconcile whether there is a consensus concerning the risk picture and the implication of the various risks as well as an overall understanding of what this picture means for the organisation

• Does the enterprise have a Business Continuity Plan which is based on a risk assessment?

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

• Have catastrophe scenarios been prepared?

Background: All businesses should think through and define for themselves what a catastrophe is and what it can mean for profitability/ balance sheet values. Based on such an analysis it should be possible to identify less significant activities which nevertheless have the potential to overturn the whole enterprise even though the probability of occurrence is extremely low. A question which should then be addressed is – do we wish to continue with these activities/ does it make economic sense?

It is also important to identify these types of scenarios because normally the probability of such events is so low that they will likely fail to be included in the documentation of high level risk charts.

• How are insurance policies integrated/ included in risk management?

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

This appendix was first developed by the Risk Management Network of IIA Norway in 2017 and has been translated from the Norwegian original.

APPENDIX 6

ERM IN THE PUBLIC SECTOR

1 Background
This Good Practice guidelines document is intended to be applicable and relevant to both the public and private sectors. In this appendix will be highlighted some of the main areas that may present different challenges in the public sector than in a commercial enterprise.

2 Risk definition
Risk management in the public sector must be integrated with management of the achievement of goals and required outcomes. It is expected that all managers have knowledge of and manage risk. *Risk* is defined in relation to matters or incidents arising which may affect the achievement of goals and may have negative or positive consequences or a combination of both. In some cases, official pronouncements may define risk exclusively as negative risk, and positive risk as opportunity.

Risk Management is an important management tool and consists of two main elements – risk evaluation (risk identification, risk analysis and risk prioritisation) and *risk treatment* (identifying risk reduction efforts and risk monitoring). Risk is evaluated in respect of the likelihood of a risk occurring and the expected consequence of a given risk occurring. There are many similarities between public and private sector risk management. Risk management is often based on the same standards and frameworks such as COSO ERM and ISO 31000, but there can be differences in the detailed practice of risk management between the two sectors.

3 Managing risk reduction activities and effects in the public sector
Public sector entities are to a great extent financed by taxation and not by investors and they cannot go bankrupt as with private companies. For many of the services offered by the public sector there is no equivalent market for delivering the product/service (e.g. defence, police and justice system) to the user or society which can be used as an information source in risk management. Public sector entities are self-insured.

In the public sector there may be considerable difficulties in measuring the outcomes achieved for the user or society taken as a whole. As there will often not be a market for the public sector products/services there is no market that gives the answer to the effectiveness of activities. Pricing is not a good measure of the quality delivered and makes prioritising and allocation challenging. As there may be more than one organisational entity responsible for the delivery of a product/service it can be a challenge to place responsibility, understand cause and effect, and monitor risks, as well as explain the effect of risk reduction activities and the outcomes achieved.

Cost benefit and budget limitations
The achievement of goals in the public sector must be achieved within the limits of disposable resources and the assumptions set by the superior authority (e.g. the Parliament, the department). Cost benefit considerations will therefore underlie the dimensioning of initiatives and risk reduction activities. Goals and risk mitigation activities cannot be chosen freely as the social mission, limitations etc. are given.

4 Risk management and internal control
Public sector entities are diverse and fragmented in respect of administrative level, means, and areas of responsibility. Public sector entities have many various goals and activities, from upholding laws and carrying out inspections to various forms of welfare delivery. Understanding the specific type of activity is key to the practice of risk management. The risk management requirements set for the public sector are often expressed as high-level principles, in order to allow for variation in the type of activity. There are therefore no detailed requirements for risk management as is the case in for example the financial sector. In local authorities it can be seen that governance principles can affect risk management e.g. risk management can be based on the principles of management by trust.

Risk management and internal control are overlapping concepts as will be seen from the standards and frameworks of ISO and COSO:

5 Risk culture
The management and control environment affects employees' attitude to both risk management and internal control.

The management and control environment encompasses everything from attitudes, behaviour, values and competency, to how management has established the division of responsibility and authorities, organises work processes, and develops the organisation's human resources. The management and control environment consists both of formal and informal standards in the organisation. Formal standards include prescriptive risk management and internal control standards with which all employees must comply. Informal standards include attitudes, values and norms which characterise the organisation often called organisational culture.

Good risk management and internal control is dependent on a good fit between the formal and informal standards comprising the management and control environment. The proof of the success of this will normally be reflected in a higher quality of risk management and internal control.

6 Risk appetite
Public entities must take risk in order to contribute effectively to the development of civil society. If it were indeed possible to have zero tolerance for errors in all areas, the aim of an innovative public sector learning by trial and error would be unachievable. Zero tolerance for errors would mean an inordinate amount of resources being invested in control activities as against service delivery. It is therefore important that entities in the public sector have a conscious awareness of risks and the acceptable level of errors and acceptable outcomes.

For many managers in public sector entities it can be a political dilemma to formulate an acceptable level of failure to achieve a specific objective for example in respect of risk tolerance for death or health impairment.

Despite the difficulty in defining or quantifying risk tolerance related to overall objectives, it should be a critical subject for discussion at the top level of the entity as well as in discussion between the entity and higher authority e.g. government department.

APPENDIX 7

RISK REPORTING

1 Introduction

There is no one definitive risk report or set of reports which are applicable to all organisations and all circumstances. Risk reporting has one common goal which is to increase the understanding of the possible effect of uncertainty on the future development of the organisation. This understanding should provide a basis for improved decisions. This appendix demonstrates some of the most common types of reporting for the various types of risk that may assist in this process.

In this appendix risk will be addressed in the following main categories:

1. Strategic risk
The risk of failure to formulate and implement a strategy which enables the organisation to develop successfully.

2. Business risk
The risk of failure to develop the activities in a way which provides benefit to all stakeholders from customers/clients to investors/public authorities.

3. Financial risk
The risk of losses from failure to manage financial exposure in connection with investments, financing, foreign exchange and liquidity management.

4. Operational risk
The risk of errors and inefficiencies leading to poor product/service quality.

2 Historic or forward-looking information

Most reporting that is made regularly to the board illustrates what has happened over the past period or periods. Historical information provides the following main benefits:

- It can give comfort to the report receiver (e.g. top management or the Board) that there is no evidence of major risks that would require action to be taken.
- It can be used as a basis for identifying the responsible party in the case of higher risk
- It can be used to identify specific weaknesses in systems and procedures
- It can be used to understand better the development in the risk landscape and the direction of development in the organisation.

It is the last benefit listed which will give the most value added to the decision-making process.

3 Strategic risk

A vision of the long-term future of the organisation will direct decisions on organisation and activities in the short to medium term (strategy).

Visions of the future can fall into various types (see also figure below):

1. One chosen future

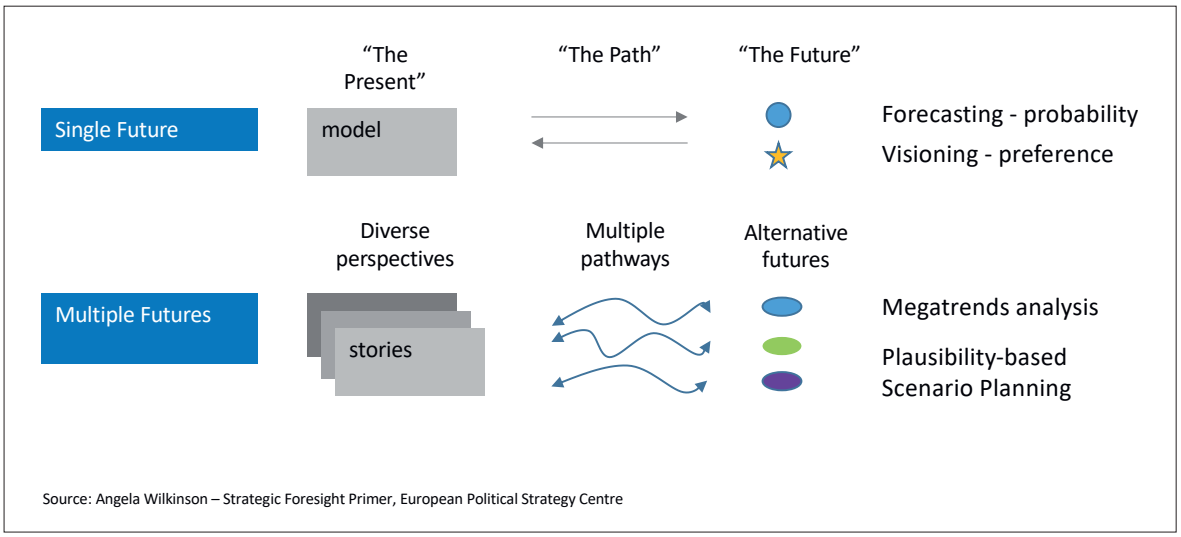
This will often result in one agreed strategy supported by a financial forecast. In this situation Risk Management can help to broaden the picture by showing the possible effects of uncertainty on the expected future results. This can give greater insights in decision making in respect of major investments/divestments.

Stochastic risk models can bring a further sophistication allowing potential outcomes to be measured against historical development. The assumption being that past development is a good measure of future development. An example of this type of methodology can be the use of Value at risk in monitoring financial activities.

2. Multiple futures

The risk management profession has identified that increasing technological, political and social development means that historical risks may not be a good measure of future risks. These future risks are often identified under the caption "emerging risks".

A good way to understand the effect of possible changes in the future is to have a creative workshop/project with the objective of arriving at a limited set of plausible stories as to future development which will affect the organisation's activities. Risk management can have a role in facilitating such clear sky thinking for thereafter to assist in the quantification of the effect of these various scenarios.



App. 7 figure 1 Comparison of methods for looking into the future

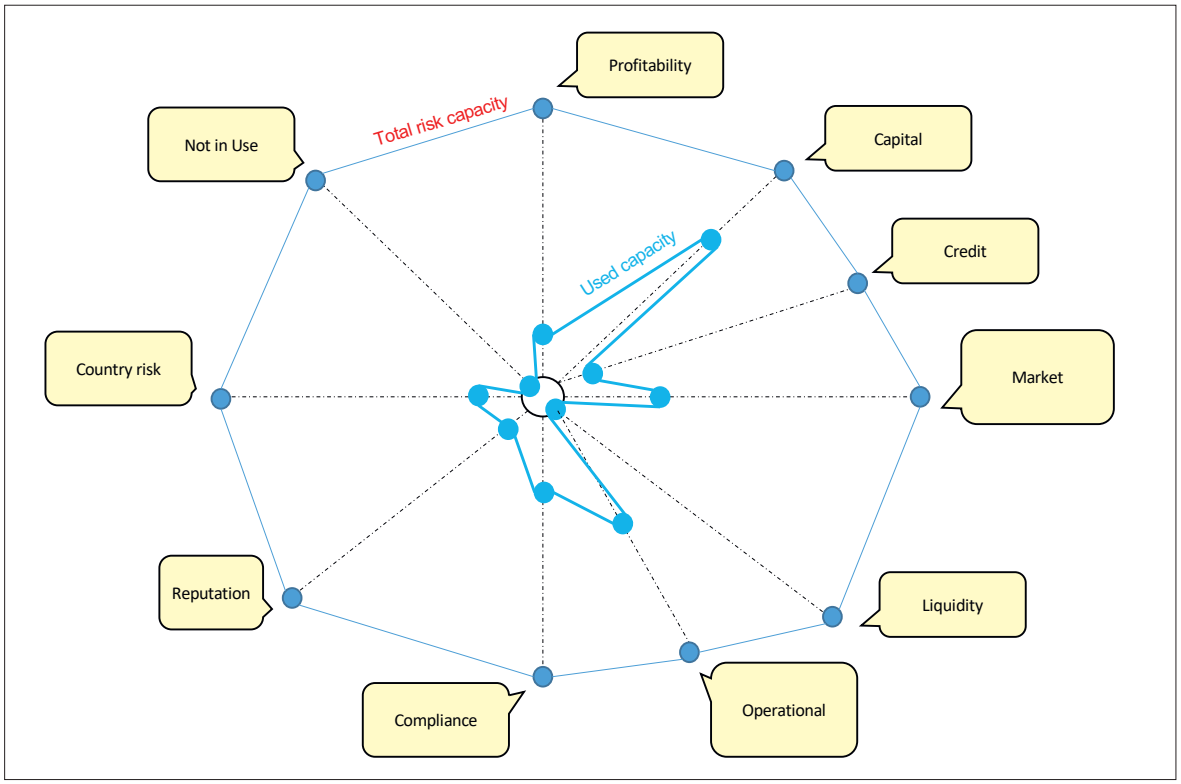
The benefits of quantified scenarios can be:
1. Increased insight into the organisation's activities and vulnerabilities.
2. They allow the timely identification of when change in strategic direction is required (so as to avoid ending in a situation similar to Kodak where the business failed due to not taking into account change in customer preference for digital rather than cellulose film).
3. The development of red flags and contingency plans allowing prompt action to be taken as and when a specific situation arises.

4 Business risk

Business risk will often be best monitored by financial measures such as development in:
- Sales
- Gross profit
- Costs
- Net profit
- Customer satisfaction
- Market share/competitor analysis etc.

These elements are often identified as Key Performance Indicators or KPIs. The trends revealed by KPIs will also mean that they will double as Key Risk Indicators or KRIs.

Risk management may also expand the understanding of financial development by identifying those areas where there is potential to take more managed risk within the given risk appetite (see figure 2).



App. 7 figure 2 Potential v. utilised risk capacity

5 Financial risk

Financial risk will typically be managed by quantifying future exposure by reference to actual exposure with reference to historic trends and risk correlation (value at risk). As these parameters are historically based this risk picture should be complemented by stressing parameters (stress testing) and the quantification of risk under a number of given scenarios based on other than historical price development and correlation of risks (scenario testing).

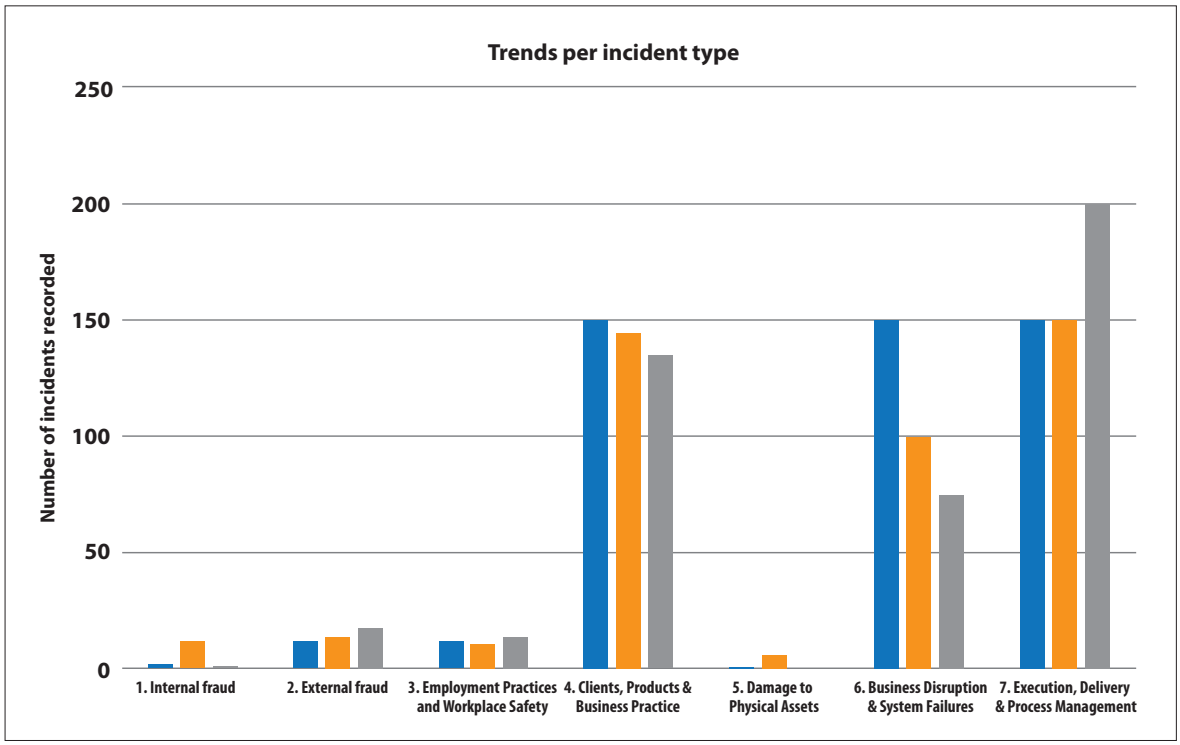
Where the enterprise has considerable proprietary trading a histogram of historical daily results may provide a way of assessing the success of risk taking from trading activities over time.

6 Operational risk

Operational reporting is concerned with showing the status and development of internal process and routine and can include:

- Status reports on the implementation of strategy with the aim of identifying any necessary reassessment of direction or activities
- Status of project risks
- Monitoring of KRIs in administrative processes e.g. processing time, customer satisfaction, error percentage, staff illness days etc. with the aim of re-evaluating, resources, systems, competency etc.
- Incidents and quality reports to encourage continuous improvement
- Staff surveys in order to identify possible weaknesses in risk culture
- Quantification of potential losses from current operational risk picture e.g. in areas with low probability and high impact such as cyber risk.

An example of operational risk incident reporting is shown in figure 3.



App. 7 figure 3 Operational incidents

7 Conclusion

There are many forms of risk reporting for the various types of risk but they all have a common objective which is to increase the level of understanding at management and board level so that better and more informed decisions can be made.

Ad hoc reports can also be an important adjunct to regular reporting. These reports can for example allow for a deep dive into a specific risk area. The resulting risk analysis can identify such issues as sub-optimalisation between organisational silos. Such analysis can lead to improvements in organisation, policy, work practices etc.

The use of traffic light reporting (red, amber, green) can communicate directly with the report reader but simple graphs and quantification of effects can add to the clarity of a message. The message can also be improved by providing verbal explanations, interpretations and comparisons with other data e.g. industry standards.

In the context of ERM it is important that the central risk management function maintains a helicopter view of the whole risk picture in order to be in a position to give sound advice to top management and the Board.

This Practice Guidelines are developed as a cooperation project between the following IIA institutes:

IIA Norway
www.iia.no

IIA Denmark
www.iia.dk

IIA Estonia
www.siseaudit.ee

IIA Iceland
www.fie.is

IIA Latvia
www.iai.lv

IIA Lithuania
www.vaa.lt

IIA Nordic Baltic cooperation project