IIA Norge

Board Guidelines on Risk Management 2025

Governance

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

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

Risk management

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

Compliance

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

Internal auditing

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

"Questions the Board should raise about Risk Management"

Guidelines for Board members of Norwegian organizations

Norwegian law requires that all Norwegian organizations headed up by a Board have a responsibility to ensure that the organization has established risk management processes according to recognized good practice. This applies to organizations in both the private and public sector.

These guidelines contain a set of key questions in respect of the organization's risk management processes. This set of questions should be viewed as a whole and are interrelated. Together the questions aim to strengthen the understanding of both the Board and management as to how the organization's risk management functions today as well as how it might be developed further.

What are the characteristics of "Enterprise Risk Management"?

These guidelines reflect accepted good practice for "Enterprise Risk Management" (ERM) based on the framework "COSO ERM (2017)". This type of risk management is built on the following three pillars:

1) Risk is defined in neutral terms as "the management of uncertainty in respect of the achievement of the organization's objectives".
2) Relevant risks are viewed holistically in order to understand the organization's enterprise-wide risk profile and thereby exploit the potential for value creation.
3) Risk management processes should be structured in such a way that they strengthen the basis for important decisions at all organizational levels and in that way provide a basis for increased value creation.

This view contrasts with a more traditional view of risk management, where:

1) Risk is viewed exclusively as an event which can have a negative impact on the business. Therefore, the aim of risk management is defined as avoiding negative surprises which can weaken the organization's financial results,
2) Risk management builds on a periodic practice of collating a list of relevant negative risks applicable to the organization, followed by an evaluation as to whether these risks are being managed by the organization. Thereafter, in the situation where controls are viewed as insufficient, an action plan is put in place to reduce the identified risk.

The more traditional method of approaching risk management does clearly have a value, and can contribute to strengthening the management of operational processes and avoid unnecessary losses. However, with ERM organizations can additionally achieve proactive

management leading to increased value creation. The question for all operational organizations it is not whether to take risk, but rather to choose to obtain the best possible outcome from the existing risk profile. As the expression goes: "No Risk – No Reward"!

The requirements for risk management are detailed in a number of laws and regulations applicable to different types of organizations. The overarching principles both in respect of the arrangement of risk management and the Board's responsibility for it are however in essence the same. It is IIA Norway's opinion that there is a benefit to be gained from high-level, comprehendible guidelines for ERM regardless of entity type, sector and industry.

Although the guidelines are primarily aimed at Board members, they will also be of use to other players with governance roles such as executive management, line management and the risk function. Furthermore, they will assist in strengthening risk management in organizations which do not have a Board – for example in departments and agencies in the public sector.

These guidelines have been developed by IIA Norway's Network for Risk Management under a working committee consisting of Petter Kapstad (Equinor), Martin Stevens (Gjensidige), Esben Jensen (risk veteran) and Wilhelm Kavli (IIA Norway secretariat).

The questions are structured in a simple table divided into five subject areas:

A. The Board's role in risk management
B. The organization's goals for risk management
C. The organization's risk profile
D. The organization's methodology for risk management
E. The organization's risk function.

A	***The Board's role in risk management***	
A-1	*Do we as Board members understand what role the board shall perform in the risk management of an organization?*	Board members should have a general overview of the legal requirements applicable to Board members in an organization applicable to risk management – including a good understanding of the Board's administrative and oversight responsibilities. Furthermore, Board members should appreciate the relevant legal requirements applicable to the organization's sector and industry.

A-2	*Do we in the Board possess sufficient professional knowledge of risk management?*	The Board should ensure that they have sufficient knowledge of the subject of ERM. When considering the composition of the Board, the owners should ensure that Board members are appointed with strong practical experience of risk management processes. These persons will then be able to provide appropriate support to the Board's decision-making process.
A-3	*Do we in the Board have the ability and motivation to raise constructively critical questions and not lay the questions to rest before we have received satisfactory answers?*	Based on its solid understanding of its role in governance, the Board should be open to asking specific critical questions, creating and maintaining a culture of unbiased critical discussion about the organization's activities and risk profile. In addition, the Board should establish a procedure for the regular evaluation of the quality of the Board's own activities.
A-4	*Do we in the Board understand the organization's value chain, strategy and the main risks affecting the value drivers?*	The Board should expect to receive a comprehensive visual presentation of the organization's value chain which can support an evaluation of the organization's most critical risks. In order to better understand the risk situation, the Board must first understand the strategic and operational value drivers and those risks which can influence the organization's production. This information will provide the Board with a basis for adequate insight into the organization's tactical and strategic choices and the reasoning behind these. Through this work, the Board should achieve an understanding of the link between results and risk capital ensuring the balance between these is justifiable and expected.
A-5	*Does the Board ensure that the organization's risk evaluations strengthen the basis for decision-making at the management and Board level?*	Board members should experience that risk evaluations strengthen the basis for strategic and other important decisions. In the situation where risk evaluations are insufficient, flawed or non-existent, the Board should request that appropriate risk evaluations be performed as the basis for decision-making.

B	*The organization's goals for risk management*	
B-1	*Does the organization provide a comprehensive and consistent expression of how risk management shall contribute to value creation?*	The Board should ensure that risk management contributes to the organization's value creation, and is not defined exclusively as a tool to avoid negative events and situations. ERM's defining characteristic is that an organization's risk management should be structured to allow the exploitation of the potential for value creation. The Board should ensure that there is a continual and sound evaluation of the balance between risk and expected return / value creation. This should underly the Board's objective considerations.
B-2	*Has the Board established a clear level of ambition in respect of risk management?*	The Board should clearly set a level of ambition for risk management, based on an evaluation of the organization's needs. This should be based on recognized maturity models and established good practice relevant to the industry. Furthermore, the Board should ensure that the level of ambition agreed upon for risk management is sufficient for the Board to fulfil its legal responsibilities. The Board should monitor the organization's status in respect of the ambition set and, if necessary, ensure that adequate resources are allocated to achieving it. The organization's overall process for risk management should be specified in a governing document which clarifies roles and responsibilities.
B-3	*Are the organization's strategy and risk profile synchronized and coordinated.*	The Board should ensure that the organization's risk profile and strategy are synchronized so that changes in risk evaluations will impact the strategy and vice versa.
B-4	*Has the organization clearly defined how much risk can be taken to achieve the goals of value creation?*	The Board should continually evaluate the risk/reward relationship at the overall level and in respect of the various business areas.

B-5	*Does the organization have a clear understanding of what constitutes strategically important risks for the organization?*	The Board should ensure that executive management and managers generally have a clear understanding of which risks can have a significant impact on the organization and that the board is kept informed about changes in the nature of these risks. The Board should ensure that the executive management has adequate plans to maintain ongoing operations. The Board should ensure that the consequences of geopolitical developments, applicable catastrophe scenarios and other potential significant risks outside of the day-to-day expectations for future development are evaluated and, if necessary, addressed.
B-6	*Is risk management integrated into the organization's general decision-making and management processes?*	The Board should ensure that risk management does not become an add-on process but rather is an integral part of the basis for and follow up of all significant decisions.
B-7	*Does the organization ensure that all direct and hired personnel take responsibility for understanding and treating risk related to their area of responsibility?*	The Board should require a regular confirmation of the status of the organization's efforts on attitudes to risk applicable to the whole organization. This should include details of the activities of executive management in reinforcing a sound risk culture.
B-8	*Is internal audit used as a tool to provide assurance that the organization's risk management functions as intended?*	In organizations which have an internal audit function, the Board should ensure that internal audit gives an independent evaluation of the organization's risk profile. The Board's prioritization of audit engagements should reflect the Board's need for an acceptable level of confirmation of risk management and internal controls in the various organizational areas based on the risk profile. This can also mean that internal audit may be tasked with auditing selected areas of the organization's ERM system.

B-9	*Are the entity's processes and organization well-structured to provide adequate enterprise risk management?*	The Board should ensure that the organization's risk management is enterprise-wide and integrated as opposed to fragmented and/or ritualistic in nature.
B-10	*Is it clearly defined who specifically owns the organization's various risks?*	The Board should ensure that it is defined who is the responsible owner of each of the risks in the organization's risk map, and what are the applicable consequences of this ownership.
C	***The organization's risk profile***	
C-1	*Does the organization have an appropriate governance structure which ensures that the Board is provided with sound and impartial risk profile information?*	The Board should ensure that the organization has a governance structure which facilitates the risk function's communication to the Board of an impartial view, of both strategic and operational risks.
C2	*Is the organization structured in a way that facilitates the ability of the Board to monitor the risk profile and risks underlying each and every decision to be made by them.*	The Board should ensure that they are provided with an adequate basis to monitor changes in the risk profile. This should be based on a periodic review supplemented by extraordinary reviews as a result of unforeseen incidents significantly impacting the risk profile. The risks related to each and every Board decision should be expressed in a way that provides the Board with a clear understanding of the issues involved.
C-3	*Does the Board have a regular process to monitor the organization's risk profile?*	The Board should monitor the risk profile both on a regular basis and as may be required. This should include a deep dive into significant areas. Estimates of the potential consequence of risks in the future should be measured in terms of the potential effects on equity and liquidity. The Board should ensure that insurance is viewed as a tool in the management of the organization's risk profile, in line with other possible risk-reducing activities. The organization's policy and practice for insurance should be based on the organization's risk profile and form an integral part of risk management.

C-4	*Does the organization have an updated register of its most significant risks?*	The Board should ensure that the organization has at any point in time a comprehensive overview of those risks which are most significant for the organization's overall results, both in the short and long term. In order for the Board and Executive Management to be in a position to understand and evaluate the various risks at an enterprise level, it would be a significant advantage if risks are made comparable by their quantification. This quantification can be in monetary or other relevant terms.
C-5	*Does the organization's risk management include time-limited programs and projects within its scope?*	The Board should ensure that programs and projects are included alongside ordinary business processes. This should be done in a way which allows for the risk management of programs and projects to be an integral part of enterprise-wide risk management. The Board should ensure that management is aware of the project's risk profile as it develops through its various stages.
C-6	*Does the organization exploit the potential that lies in available data about the organization's operations and status as a basis for evaluating risk?*	The Board should ensure that risk evaluations and decisions to be made are based on reliable quantitative facts and well-founded calculations. The Board should ensure that the potential benefit of accurate, complete and timely data concerning the organization's operations and status are fully utilized.
C-7	*Is it clear what is the source of the various numerical inputs to risk calculations, and what level of uncertainty that is attached to these numbers?*	The Board should ensure that they are provided with sound explanations for the degree of uncertainty attached to numerical inputs to risk calculations. The Board should satisfy itself that the basis for the calculations of critical risks is validated by requiring a periodic quality assurance of data forming the basis of the organization's key decisions.

D	*The organization's methodology for risk management*	
D-1	*Is the organization's methodology for calculating risk in line with good practice?*	The Board should ensure that the organization's methodology for calculating risk is in line with good practice, taking account of the organization's industry and the characteristics of the relevant risks. This methodology should be documented in a set of principles. If the organization calculates return on risk-adjusted capital, the Board should be able to understand how the reported returns take account of the organization's risk profile. This should be documented in the methodology for the calculation of risk.
D-2	*Is it clear what models are applied to the analysis and evaluation of the under-lying data and what uncertainties are attached to these?*	The Board should ensure that they are provided with good information regarding what models have been used and how this has been done. Irrespective of how good a model and how well it is applied, there will always be an element of uncertainty attached to the calculations underlying the analyses. The Board should periodically require a quality assessment of the models which support the most significant decisions. This can be done by way of an independent or third-party evaluation as well as testing of the model against actual developments. Where such periodic quality assurance is regularly performed, the Board should be provided with a comprehensive report of the results.
D-3	*Does the method used include an evaluation of how alternative possible developments might affect the organization's value creation, including financial results?*	The Board should be in a position to understand how the future outcomes have been arrived at taking account of alternative developments in the risk profile and proposed actions. Relevant methodology tools can be forecasts and scenario analyses.

D-4	*Does the organization's methodology for risk management include an obligatory step for re-evaluation and learning?*	The Board should ensure that the organization has a well-functioning learning loop as an integral part of the ongoing risk management.
E	***The organization's risk function.***	
E-1	*Is the professional responsibility for the organization's risk management clearly defined and distinctly placed?*	The Board should ensure that the organization has a risk function with a mandate, integrity, competence, and capacity which permits enterprise-wide risk management. According to the three lines model the risk function is designated as executive management's tool. At the same time, the function should be in a position to present and take responsibility for the reports it presents to the Board.
E-2	*Does the risk function have a correct understanding of their role in the organization?*	The Board should ensure that the risk function takes a proactive and forward-looking role as provider of an impartial evaluation as a basis for decision-making. The function should monitor the organization's risk exposure in a holistic perspective and track the development in the risk profile in close dialogue with the organization's management.

E-3	*Does the risk function have the competence and capacity to realize the ambition the Board has articulated for the organization's risk management?*	The Board should ensure that the risk function has been established based on a solid professional knowledge of modern risk management relevant to the organization's sector and industry. It is crucial that the function possesses the ability to strengthen the basis for both strategic and tactical decisions and at all organizational levels. The Board should ensure that the organization maintains the professional knowledge of risk management and develops further both methods and techniques. There should be an updated competency strategy for the risk function, and the Board should enquire after the current status on an annual basis. The Board should ensure that the organization has prioritized the provision of sufficient resources to this function so that it is ensured good system support, sufficient quantity of resources as well as possesses professional and business knowledge in the areas of strategy, finance and operations.
E-4	*Does communication from the risk function have a satisfactory format?*	The Board should ensure that the risk function's written and oral reports to the Board have a format which is well adapted to the needs of the Board and executive management.
E-5	*Does the risk function coordinate its work with the organization's other management and administrative functions?*	The board should ensure that the risk function in larger organizations coordinates its activities with other staff and support functions such as compliance, DPO, quality and internal audit. The aim should be to optimize resource use and the combined utility value to the organization.