Guidelines for governance

1st Edition 2021

Table of content

0. Introduction

This aim of this English language translation of the Norwegian Guidelines for governance is to reach a wider audience by making them accessible to English speaking employees in Norway, as well as to a wider international audience of public and private sector. These may be management and employees, academics, auditors and consultants with a professional interest in guidance in this area.

0.1 The objective of the Guidelines

Any enterprise, whether it operates in the private or public sector, will need to tackle frequent changes in the framework conditions in which it operates. These changes take place with an increasing frequency and enterprises are faced with the challenge of crises, disasters, business scandals and global pandemics. Systematic, efficient, and effective governance is critical to an enterprise's ability to achieve its goals, and these Guidelines identify components which are key to an enterprise's good management, survival, and success over time. For each component a suggested practical approach to successful treatment is described. The thinking behind the components is that they contribute to the creation and maintenance of a robust and durable enterprise with the ability to adapt itself to meet various and changing framework conditions.

The Guidelines are not a tutorial, neither are they fashioned to address all the detailed requirements of a given industry and sector specific laws and regulations. The components will address many of these requirements but not necessarily all of them. Users of these Guidelines must therefore adapt the various components to the detailed requirements of their own industry and sector, as well as to the enterprise's size, complexity, culture etc. The guidelines allow for flexibility in their use. Adherence to the components should be a goal, but some components can have limited relevance in certain situations and especially for smaller enterprises. As an enterprise grows in size and complexity, the need will grow for a clarity of structure, objectives and planning processes as well as risk management and control. The suggested practical approach should assist in this development process.

0.2 Relationship to other frameworks and guidance

A number of corporate governance codes have been developed internationally[1]. These are, in general, applicable to quoted public limited companies, and place emphasis on the execution of corporate power, the division of power between the respective owners as well as the organisation of high-level corporate governance. An example of this is "The Norwegian Code of practice for Corporate Governance" issued by The Norwegian Corporate Governance Board ("NUES"). These Guidelines for Governance, published by IIA Norway, have drawn inspiration from these frameworks but are distinguished by the fact that their primary focus is on "internal" governance, and only to a limited extent on the exercise of power by the owners and the interplay of responsibilities between the owners, governing bodies and executive management.

IIA Norway has previously published specific Guidelines for both the risk management and compliance functions, which delve deeper into two subjects which are key to governance and these Guidelines.

0.3 Terminology and definition

The original document ("Veileder for virksomhetsstyring") discusses a number of issues relating specifically to communicating governance terminology appropriately in the Norwegian language. The discussion has

[1] *For example: KING IV Code on Corporate Governance, G20/OECD Principles of Corporate Governance, ASX Corporate Governance Principles and Recommendations, The Dutch Corporate Governance Code and the Swedish Code of Corporate Governance*

no relevance to this English language version and is therefore not included in the English translation. There are however certain other choices of wording that had to be made in this English translation.

Firstly, concerning the title of these guidelines there was a question of whether to use the words “governance” or “corporate governance”. Many of the international guidelines we referenced use the phrase “corporate governance” however, strictly speaking, the word “corporate” refers to an incorporated entity or limited company which would imply that other entities for example in the public sector are not covered by these guidelines. The content of these guidelines should however be relevant to the public sector and non-profit making entities as well as commercial businesses. For this reason, the choice was made not to modify governance with the word “corporate”, and this is also incidentally in line with a neutral word choice in the Norwegian original.

Secondly, the Norwegian original uses a word to describe an entity which does not qualify whether the organisation is commercial or not. When translating this word for entity into English the choice lay between using the word “entity”, “organisation” or “enterprise”. After some deliberation the word “entity” was rejected for not conveying directly the concept of an administrative unit as is communicated by the word “organisation”. Organisation was felt to not cover adequately the concept of a dynamic entity which is focussed on achieving a specific mission and objectives. It was, therefore, decided to use the word enterprise. Although enterprise suggests by its name a commercial venture we find its usage has been expanded over the last 20 years to describe the concept of holistic risk management in the phrase “Enterprise Risk Management” (ERM) so that it does not appear inappropriate to talk about ERM also in the public sector. In conclusion, we have more or less consistently used the word enterprise in this document to describe an entity with a mission and objectives whether it is in the public or private sector, commercial or non-commercial.

0.4 The private and public sectors – differences in terminology and responsibility for governance

Different terminology may be commonly used within a number of the subjects which are key to these Guidelines depending on whether they are referring to the public or private sectors. Differences may also arise as to the type of governance bodies which are established and applicable to governance. The guidelines have been made sector independent as far as possible, and where there are differences this is generally noted. If, however, descriptions and practical approaches in these Guidelines are felt to be lacking in relevance because of differences in the way sectors operate, then these should be tailored in the manner described in chapter 0.1 above.

One particular matter should be emphasised, and that concerns the overall responsibility for internal governance. In the private sector this responsibility lies with the Board of Directors, but many enterprises in the public sector do not have a Board of Directors and accordingly the responsibility will lie elsewhere. It was felt that the presentation in these Guidelines would be laborious and not very reader-friendly if there was a repetitive listing of all the potential bodies or positions that hold the overall responsibility, e.g. Secretary General (in the national government), Chief Administrative Officer (in a local authority), Business Director, Board of Representatives etc. For this reason, these Guidelines consistently use the word Board to describe either the enterprise’s highest decision-making body or the highest position responsible for internal governance.

0.5 Risk management and internal control as elements of governance

Risk management is an important component of governance and is described further in section 3.3 below. Risk management requires that risks are evaluated and addressed both in the enterprise’s strategy and performance processes as well as in the daily operational tasks aimed at achievement of the enterprise’s goals.

COSO[2] defines internal control as follows: 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. In Norway we find that a frequently used expression is "internal management and control", as internal control is concerned both with managing the business and controlling it. It might have been considered natural to identify internal control, in a similar way to risk management, as a separate component in these Guidelines. The decision was however made not to do this as the components of internal control (as per COSO; Control environment, Risk assessment, Control activities, Information and communication and Monitoring activities) are key elements of both risk management and of many other components in these Guidelines. If internal control were to be defined as a separate component, it would have led to much repetition and the use of many cross references in this document.

Risk management leading to the achievement of objectives encompass the totality of the enterprise's system of internal control. In practice however, many people may define elements of internal control as lying outside risk management in so far as the systematic and planned risk management activities are concentrated on the most material and risk exposed areas and activities, based on a cost/benefit analysis. Where an enterprise has succeeded in integrating risk management to be an embedded element of the daily operations at all levels, internal control will also conceptually be a part of risk management.

Risk management and internal control overlap when we talk about identifying and treating risks affecting the achievement of goals within the following categories:

- Operations objectives – effectiveness and efficiency of operations
- Reporting objectives – reliability of reporting
- Compliance objectives – adherence to laws and regulations.

In addition to these, there is within risk management a fourth category of objectives, defined as strategic objectives, also often called high-level objectives. Risk management of these strategic objectives results in decisions about overall and strategic plans and activities which will not normally give rise to concrete internal control activities. To summarise, risk management and internal control are key elements of governance.

0.6 External context

Various events and activities which arise external to the enterprise, in addition to the demands and expectations from public authorities, markets and other stakeholders, are often described as the external context. Examples of these can be laws and regulations, generally accepted accounting principles, listing requirements, business norms, societal expectations, new competitors in the market, changes to grants and external financing etc. These conditions lie outside the organisation, which can only to a limited extent control or influence them, but they result in important requirements and lie behind assumptions for choices the enterprise makes and the activities it occupies itself with. A regular and systematic review of the external context is therefore essential. This will need to be followed up further with concrete activities where deviations or the need for adjustments are identified.

[2] Committee of Sponsoring Organizations of the Treadway Commission: Internal control – an integrated framework (2013)

0.8 The components of governance

Governance is about providing a means for management and other employees to take care of their responsibility and their activities for the achievement of the enterprise's objectives, plan for sound internal control and risk management activities, support efficient and effective operations with the required level of monitoring and reporting, as well as establishing effective independent control and assurance.

The figure below shows the components which form the basis of these Guidelines, grouped according to the subjects of Objectives and direction, Structure, Implementation as well as Learning and improvement. Having taken into account the external context these components will contribute to the enterprise's ability to create value and achieve goals. The order of these subjects (1 to 4) is aligned with well-established process methodology and management circles such as Deming's circle. However, it should be stressed that the figure does not illustrate a "painting by numbers" solution where an enterprise starts with the components linked to objectives and direction and thereafter works its way down through the list component by component until arriving at "continuous learning and improvement". Governance is dynamic, and the components are highly integrated one with the other, are performed simultaneously and will influence one another.

The components of governance

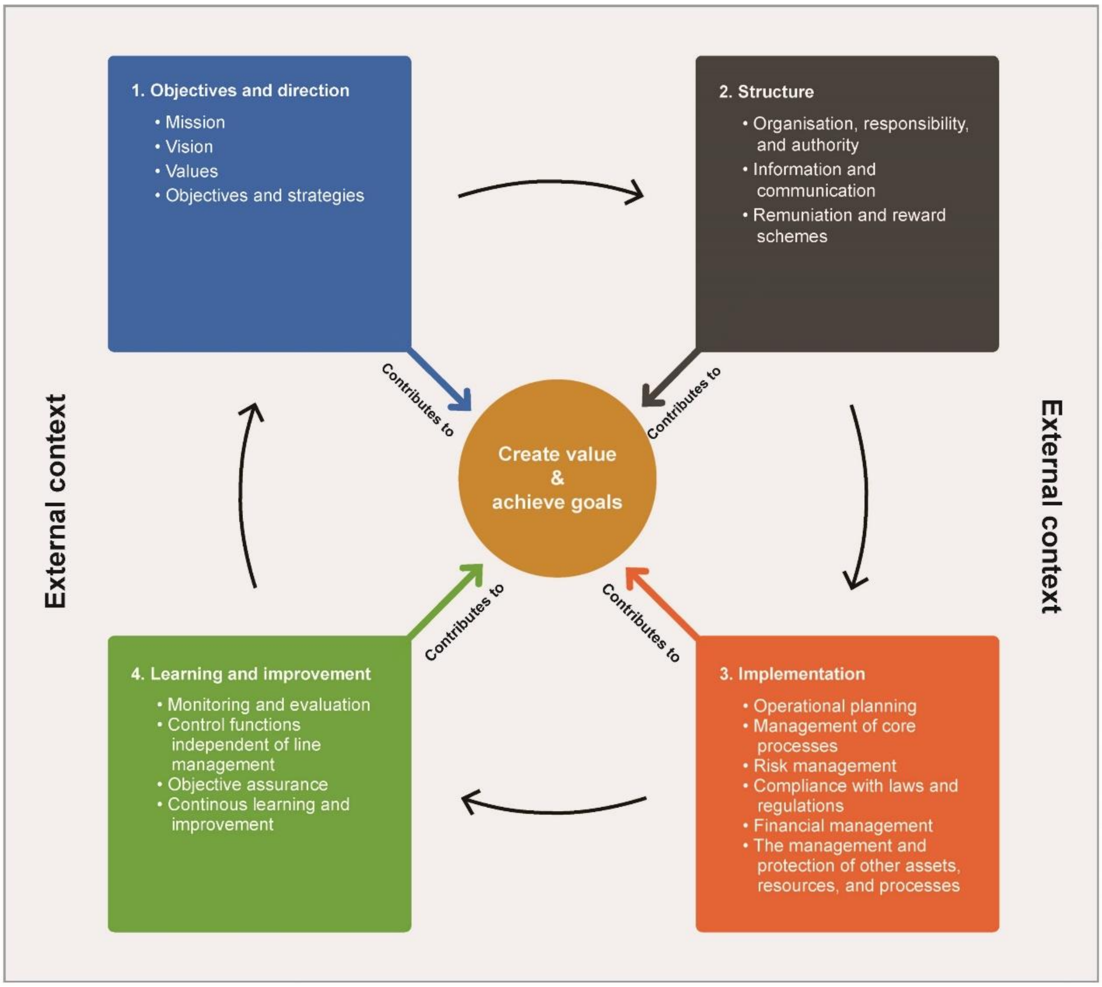

1. Objectives and direction
• Mission
• Vision
• Values
• Objectives and strategies
2. Structure
• Organisation, responsibility, and authority
• Information and communication
• Remuniation and reward schemes
External context
External context
Contributes to
Contributes to
Create value & achieve goals
Contributes to
Contributes to
4. Learning and improvement
• Monitoring and evaluation
• Control functions independent of line management
• Objective assurance
• Continous learning and improvement
3. Implementation
• Operational planning
• Management of core processes
• Risk management
• Compliance with laws and regulations
• Financial management
• The management and protection of other assets, resources, and processes

Figure 1: Chapters corresponding with the components of governance

1 Objectives and direction

Before a structure for the enterprise can be raised that caters for ordered, efficient and effective operations, a foundation needs to be laid comprising the established mission, vision, values, objectives, and strategies of the enterprise. The identification and formulation of these components are important, not least to motivate and inspire all employees to work in alignment.

1.1 Mission

The mission describes the enterprise's reason for existence as well as delineates the bounds of its operations and activities

The mission describes the enterprise's reason for existence as well as delineates the bounds of its operations and activities. It defines the parameters to the use of resources for development and improvement, for this reason it is important that the definition of the mission also includes the enterprise's planned and future activities. Activities which are not aligned with the mission should be corrected or discontinued, or alternatively lead to the revision of the mission. The mission is the basis for the enterprise's vision, values, objectives, and strategies. It is the responsibility of the owners to define the enterprise's mission. In the public sector mission may be qualified by the word social e.g. social mission.

Practical approach
The mission should:

- explain the reason for the enterprise's existence
- define the mandate requirements to be met
- be formulated with a clarity that may be readily comprehended by internal and external stakeholders

1.2 Vision

The enterprise's vision expresses the idea over the longer term of what the enterprise aims to achieve and forms the basis for objectives and strategies

The vision should represent a desired future image or state which the enterprise strives to achieve. It expresses an ambition, indicates a direction, and visualises the end state. It can be expressed for example in terms of achieving the position of industry leader in the country, of retaining the position of the supplier of choice for a given type of goods or services in the region, of realising profitable operations in a new foreign market, of being the most attractive employer in the community, of being appreciated as a socially engaged and reliable contributor, of being an attractive local government area to work in etc. The vision should be aligned with the mission and should ideally be supported by a set of concrete objectives, see chapter 1.4.

Practical approach
The vision should:

- provide direction and inspire
- be inclusive and unifying
- be readily understood

1.3 Values

The enterprise's values express the values that the enterprise wishes to uphold and will form the basis for building a cultural identity

The values express what the enterprise wishes to stand for and forms the basis for building and maintaining a cultural identity. These values must instruct day-to-day decision-making and actions. The expressions "values" and "core values" are often overlapping in daily use. In these Guidelines values are used as a collective term for core values, ethics, social responsibility and transparency. The subcategories taken as a whole, should help the enterprise to stand with integrity, act ethically and promote a sound culture.

1.3.1 Core values

Core values represent the enterprise's underlying values. How these values are defined, communicated, and complied with is crucial to constructing the enterprise's culture. A core value statement should be a guiding articulation of how the enterprise wishes to operate in order to achieve its goals in both an internal and external context. Examples of core value statements can be that the enterprise is future driven, sustainable, innovative, or places importance on diversity.

Practical approach
Core values should:

- define the behaviour which is to characterise the enterprise's desired culture
- inspire, so that people wish to live up to them
- be formulated so that any dissonance between them is avoided

1.3.2 Ethics and social responsibility

There is an expectation that an enterprise shall act in an ethically responsible manner and demonstrate social responsibility over and above a compliance with the letter of the law and legal regulations (cf. chapter 3.4 below). Living up to this expectation is of major importance to the enterprise's reputation and can impact the enterprise's achievement of goals, its competitiveness and long-term survival. As an example, society in general will expect enterprises to evaluate risks related to sustainability and the environment and establish processes over and above the minimum legal requirements in this area.

The Board and senior management should have a conscious approach to ethics and balance sustainability and social responsibility with more short-term financial interests.

Practical approach
The enterprise should:

- provide clear ethical rules and guidelines and operate in line with these
- prepare rules and guidelines for how external considerations are to be integrated with value creation
- put in place concrete preventative, detective and reactive activities targeting corruption, misconduct, fraud, discrimination, mobbing etc.
- establish a secure whistleblowing channel for the reporting of criticisable issues

1.3.3 Transparency

Transparency concerns the need for openness in the enterprise about how decisions are made, how activities are performed, and the results that are achieved. Internal and external information should be made available and be appropriate to the needs of the stakeholder, contribute to a better understanding of the enterprise's development and be adequate as a basis for decision-making (see also chapter 2.2 below concerning information and communication).

Practical approach
The enterprise should:

- document decisions and the basis for these decisions
- ensure the quality, timeliness and integrity of information provided to internal and external stakeholders
- share all relevant information related to the enterprise and decisions made with internal and external stakeholders
- ensure that the Board members and employees are aware of any potential conflicts of interest that might arise and appraise the need to absent themselves from the decision-making process (cf. chapter 2.1 below)

1.4 Objectives and strategies

Objectives and strategies support the enterprise's vision and values

An objective describes a desired future state, and an enterprise will normally have both strategic objectives and operational goals. The strategic objectives, often approved by the board, will reinforce the enterprise's vision and values, and will often be realised in the longer term. The more short-term operational goals will be approved by management (cf. chapter 3.1) and should support the strategic objectives. They are typically more tangible and concrete, and their achievement will be based on tailor-made action plans. Operational goals will, as a general rule, be defined for the various business areas and at various levels of the enterprise.

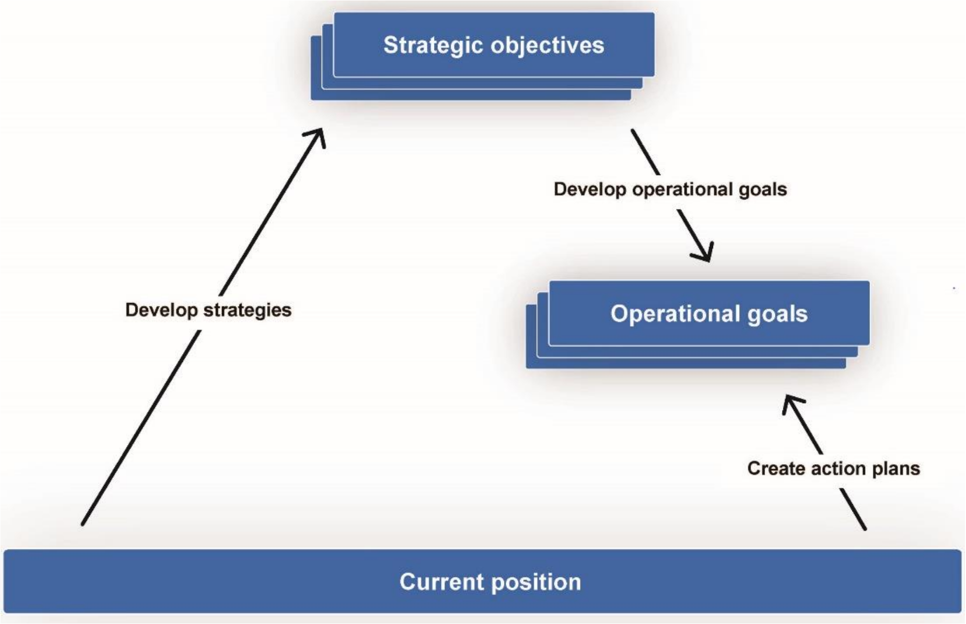


Figure 2: Objectives and strategies

When developing strategies, it is important to understand where the enterprise is today i.e. its current position, both in relation to external and internal factors. This will often require a thorough analysis. The strategies describe further the choices the enterprise makes to proceed into the future and achieve its objectives. The strategic objectives and planned strategies to achieve the future state will usually be approved by the Board, whilst operational goals and action plans will usually be approved by management. It is important that the state of achievement of strategic objectives and operational goals be evaluated regularly, and the planned course be adjusted as required (cf. also chapter 3.3 Risk management and 3.5 Financial management).

Practical approach

The enterprise should:

- define clear strategic objectives for key areas of activity within the areas of operational effectiveness and efficiency, safeguarding of value and assets, compliance with laws and regulations as well as accurate reporting
- carry out a required analysis of the current situation e.g. a SWOT-analysis[3] which provides an oversight of strengths, weaknesses, opportunities, and threats
- prepare various scenarios for possible future development including an evaluation of the related risks
- identify critical success factors (matters, assumptions or prerequisites that must be addressed to achieve success)
- approve and document the strategy and plans required to achieve the strategic objectives
- approve operational objectives with related action plans (cf. chapter 3.1)

[3] *SWOT = Strengths, Weaknesses, Opportunities and Threats*

2 Structure

A sound structure, with viable decision-making processes, clear division of responsibility and authority, appropriate information and communication processes as well as remuneration and reward schemes, is key to an enterprise being in a position to achieve its strategies and objectives. The establishment of the described structure presupposes clarity as to the enterprise's objectives and strategies, values, behaviour and culture, and that external conditions are identified and taken into account as described in sections 0 and 1 above.

2.1 Organisation, responsibility, and authority

The organisational structure with a clear delineation of responsibility and authority is appropriate to the enterprise

An effective organisational structure consists of a system of delegation of responsibility and authority which balances and distributes the roles, responsibility, and authority in the organisation. The relationship between superior and subordinate should be clarified, from owners and out to the individual employee, and rules of impartiality which secure adequate objectivity in decision-making processes should be established.

The Board has a supervisory role helping to support value creation and avoid loss of value. This implies responsibility for approving the overall organisation of the operations, including an efficient and value creating management structure. Management at various levels are responsible for establishing, maintaining and further developing an appropriate organisational and governance structure in alignment with the Board's decisions.

The Board should hold the senior management accountable for compliance with the authorised responsibility and authority structure and that it functions as intended. Any serious breaches should be reported to the Board. The Board is also responsible for hiring, evaluating and determining the remuneration of the CEO as well as potential dismissal. There is a comparable responsibility in respect of managers of supervisory, control and assurance functions. The Board should approve guidelines for the remuneration of executive managers (cf. further chapter 2.3).

Practical approach

The enterprise should:

- prepare and approve the Board Charter and have a plan for the work of the Board which includes frequent evaluation of the functioning of its own activities
- establish and document a clear and appropriate responsibility and authority structure e.g. by way of a matrix for responsibilities and authorities
- prepare and approve written mandates, job descriptions etc.
- establish management structures which address, coordinate and prioritise portfolios, programs, projects and cross operational processes
- ensure necessary and regular training, awareness raising, and follow up and monitoring of roles, responsibilities and authorities
- ensure all decisions can be traced back to the person or persons responsible for the decision
- establish rules for handling conflict of interest which are communicated to all relevant parties and ensure their compliance.

2.2 Information and communication

Relevant, reliable, and sufficient information is made available and timely communicated

Relevant, reliable, timely and sufficient information in an appropriate format is a prerequisite for the management and development of an organisation. Information must be made available to those who can make use of it both within and outside the organisation. This requires the establishment of processes and criteria for the identification of who is the recipient of what type of information, and the decision is made as to when and how information is to be sourced or obtained. Typical elements in an enterprise's information and communication processes are communication plans, descriptions of responsibilities, stakeholder matrices (relevant stakeholders and type of information to be communicated) and various communication channels.

Practical approach
The enterprise should:

- define target groups and interested parties for information and communication
- put in place governing documents for dealing with internal and external communication, as well as defining responsibility, roles and tasks
- establish action plans with a detailed description of how information-gathering and communication shall be carried out also in a crisis situation
- ensure that information to the Board, management and external stakeholders has an appropriate scope, accuracy and level of detail, and is formed in a way that can be understood by the recipient

2.3 Remuneration and reward schemes

Remuneration and reward schemes support the enterprise's objectives and values

Remuneration and reward schemes should include all employees and reinforce the enterprise's objectives and values. The schemes should reward an employee's contribution to long-term and ethical value creation as well contribute to the avoidance of unnecessary conflicts of interest.

Practical approach
The enterprise should:

- adopt remuneration and reward schemes which will be considered reasonable, ethically sound with a long-term focus and balancing the relationship between fixed and variable remuneration for positions where this is relevant
- have specific, Board approved rules for the remuneration of managers, possibly also for other employees with special work tasks and responsibilities
- ensure transparency concerning the remuneration and reward schemes by publishing openly the key principles and criteria for fixed and variable remuneration as well as adjustments made
- establish routines for dialogue between management and union representatives when changes are made, or a new remuneration or reward scheme is proposed

3 Implementation

The enterprise's objectives and strategies should be rendered into concrete actions plans at an operational level. Comprehensive and co-ordinated management of the core processes translates into efficiency and quality in the operational phase, and they are supplemented by support processes, such as financial and risk management. At the same time, laws and regulations must be complied with, and organisational values maintained and protected.

3.1 Operational planning

Strategic objectives are rendered into specific goals and action plans

The enterprise's strategic objectives must be rendered into specific goals and action plans for organising and implementation. The plans should provide clear direction as to how the strategies are to be implemented and the goals achieved, whilst ensuring that organisational values are taken into account and realised in practice. The achievement of goals is monitored in relation to plans made and the desired progress.

Practical approach
The enterprise should:

- develop operational goals which are realistic, meaningful, relevant and as far as possible measurable
- prepare action plans that describe responsibilities, roles and deadlines for the various actions and activities
- establish a set of measurement indicators or criteria as a basis for monitoring progress as well as the degree of achievement of objectives, and as a basis for corrective actions in the case of adverse development

3.2 Management of core processes

Core processes are defined, managed and documented

Typically, an enterprise's core processes will often consist of the production and distribution of goods and services with a given quality in the most efficient way. Processes that normally encompass many different departments and systems in the organisation should be defined, managed, and documented. This will ensure targeted and coordinated processes and activities leading to the best results possible and which will provide a basis for knowledge transfer and quality improvement.

Practical approach
The organisation should:

- define its key processes and describe them in governing documentation
- formalise processes and routines which are necessary for the production and distribution of the organisation's goods and services
- ensure integration with support processes (see sections 3.3 to 3.6 below) thereby contributing to successful execution as well as management and control of the core processes
- systematically seek to identify weaknesses and implement improvement measures in the core processes (see section 4).

3.3 Risk management

Risk management assists in the management of uncertainty in respect of the achievement of the organisation's objectives

Risk management is a tool to manage and control uncertainty in respect of the enterprise's ability to create, protect and realise value as well as to achieve its goals. By uncertainty is meant in this context both possible unplanned negative outcomes as well as potential positive outcomes.

The risk of failure to achieve objectives is often split into "downside" risk and "upside" risk. Downside risk describes the risk for negative and undesired events. This risk will always be important and traditionally has been something that organisations are aware of and mitigate by establishing controls. Upside risk is the risk for the organisation not identifying or exploiting opportunities, something which can have a negative impact on value creation. An organisation's risk management should encompass both upside and downside risk.

Risk management should be an integrated part of governance. Established good practice is that risk management should have a holistic perspective ("Enterprise Risk Management") which is integrated across the organisation and harmonised with other management activities.

An enterprise's willingness and ability to take risk (its risk appetite and risk tolerance) should be described and quantified as far as is practically possible. This will provide the enterprise with a management criterium and a measurement point both for the type and quantity of risk that the organisation is willing to assume or believes it can tolerate, and for the risks which have already been absorbed.

Sound risk management is reinforced by the organisation's systematic development of a sound culture and attitudes which should be integrated into its processes at both a strategic and operational level. Risk management must contribute to a best possible basis for decision-making at different levels, ensuring that the decisions made support the enterprise's various goals. It is important to have sound mechanisms for continuous monitoring and implementation of mitigating activities in response to changes in the risk profile.

The organisation of risk management is the responsibility of line management with ultimate responsibility lying with the Board and executive management. In those instances where the organisation has established an independent risk management function such function should not have a decision-making responsibility at the operational or business level.

Practical approach
The organisation should:

- have a board approved mandate and guidelines for risk management
- consider the establishment of a risk management function[4] with responsibility for establishing and maintaining a risk management framework, methodology and process
- ensure that the risk management process operates at all relevant levels of the enterprise e.g. at strategic and operational levels and in projects
- describe and quantify risk appetite and risk tolerance
- identify responsible risk owners who decide, manage and accept risk exposure including the implementation of controls or other activities as required

[4] *Cf. Good practice guidelines for the Enterprise Risk Management Function - IIA Nordic Baltic Cooperation project 2020*

- establish sound systems and activities allowing for the continuous identification, analysis, evaluation, management, monitoring, communication and reporting of developments in the risk profile
- continuously evaluate and follow up on risks arising from major changes, events and projects in the enterprise
- identify and evaluate new and emerging risks and their potential positive and negative outcomes e.g. by way of scenario analysis
- document how key control activities are performed, how they are expected to affect the risk profile, who is responsible for implementation and performance as well as how the results are to be reported

3.4 Compliance with laws and regulations

The organisation operates in compliance with laws and regulations

The Board has the overall responsibility to ensure that the organisation operates in compliance with external and internal regulations and has an oversight role which contributes to this. Senior management has the operational responsibility to ensure compliance by monitoring their areas of responsibility by identifying any compliance gaps and implementing necessary measures to close these gaps. The risk of non-compliance is an operational risk and work with this type of risk should be coordinated with and assessed as a part of the organisation's operational risks.

Practical approach
The organisation should:

- consider establishing a compliance function[5] with a defined mandate, organisational position, and defined reporting lines
- establish a system adapted to the organisation's characteristics, size and complexity which promotes compliance with laws, regulations, other regulatory requirements as well as internal and external instructions. Such a system should encompass:
  - an overview of key laws, rules and guidelines, which is regularly updated
  - routines for monitoring and reporting compliance between the organisation's activities and applicable laws and regulations as well as internal instructions and resolutions
  - regular assessment of the risk of non-compliance
  - communication, training and providing advice aimed at preventing non-compliance
  - notification procedures for compliance violations
  - follow-up of deliverables from a compliance function (if such has been established)

[5] *Cf. Guidelines for the Compliance Function - IIA Norge 2015*

3.5 Financial management

Financial management supports decision-making and contributes to the organisation’s access to and use of resources

The organisation should consciously manage the inflow and use of resources in order to achieve its objectives. The planning of inflow and use of resources is expressed in the budget and financial forecasts, while the financial statements reflect what has actually happened The budgets and financial statements are an important support for decision-making by the board, management and other internal and external stakeholders.

Practical approach
The organisation should:

- establish a finance function with a defined organisational position, tasks, reporting lines and -responsibilities
- establish a structure for planning, budgeting, accounting and reporting which reflects the organisation’s activities and areas of responsibility and complies with applicable regulations
- prepare short-term and long-term budgets and/or forecasts in line with the organisation’s objectives and action plans
- ensure reliable accounting in line with applicable regulations including generally accepted accounting principles
- measure and report actual development in relation to budgets and plans, including informative key figures, and take action where this is necessary

3.6 The management and protection of other assets, resources, and processes

Other assets, resources and processes are identified, managed and protected

There will normally be other important processes in an organisation in addition to those mentioned in chapters 3.1 to 3.5 above, and the organisation will also have additional assets and resources to those mentioned in chapter 3.5 under financial management. These processes and resources must also be managed, and their value advanced and protected. The subchapters below are not exhaustive but discuss some important areas which are relevant to most organisations.

3.6.1 Project, program and portfolio management

Project, program and portfolio management is a means by which to identify, prioritise and manage projects and programs. By identifying and managing these across the organisation the possibility of achieving objectives and realization of benefits will be enhanced, amongst other things by reducing the risk for sub-optimalisation, lack of coordination and unnecessary use of resources.

Practical approach

The organisation should:

- establish a governance structure with roles, responsibilities and authorities which facilitates holistic management, co-ordination, and prioritisation within the portfolio as a whole and each sub-portfolio with programs and projects

- prioritise in a systematic way the commencement, progress and possible discontinuance of projects and programs in the portfolio, based on established criteria for management and prioritisation including for example, resource limitations, deadlines, bottlenecks, skills requirements etc.
- put in place routines for the regular evaluation of existing and any new programs and projects, so that the need for changes, improvements or other adjustments can be identified early and necessary actions taken

3.6.2 IT-management

Information technology (IT) management should lead to the achievement of maximum value from investments in IT and should address risks that might arise from the application of IT (IT risk). Management of IT must be performed in interaction with both strategic tasks and daily operations, and will affect almost all of the organisation's activities and processes, including organisation, IT design, data processing, data and information security, data privacy, implementation of new technical solutions and training. There are significant risks associated with maintaining an overview of the type of data/information the organisation has, and to handle problems concerning quality and integrity as well as access, rules for data usage and ownership. The use of established frameworks[6] can ensure that IT-service deliveries support the organisation's objectives and that IT risks are handled systematically.

Practical approach

The organisation should:

- establish IT-roles, responsibilities, and authorities
- approve an IT strategy with objectives aligned with the organisation's overall strategy and mission
- establish a culture of IT security under which all employees understand their role, are aware of the risks in their own field and know how to prevent and deal with these
- apply an established framework (e.g. ITIL or COBIT) to provide quality assurance over IT management and the handling of deviations

3.6.3 Contingency management and continuity planning

The organisation's system for contingency management and continuity planning comes into operation when serious, unwelcome events threaten or occur. These events may be external e.g. a pandemic, terrorist attack and sabotage, fire, electricity outage and natural catastrophe, or they may be unwelcome internal events. Contingency management and continuity planning contribute by both preventing such events and by reducing their consequence by ensuring the continuance of operations. These plans are an important tool in assisting management and employees at all levels in the organisation in preparing for and dealing with these types of events in the best possible way.

Practical approach

The organisation should:

- approve and inform about roles, responsibilities and authorities for the organisation's contingency preparedness and continuity efforts

[6] *A number of frameworks have been developed within the area of IT-management which can be used. Examples of these are ITIL ([https://www.axelos.com/)](https://www.axelos.com/) and COBIT ([https://www.isaca.org/resources/cobit)](https://www.isaca.org/resources/cobit) which represent international standards in this area.*

- perform frequent risk and vulnerability analyses to identify potential events which may lead to an extraordinary burden on the organisation
- prepare and regularly update the required planning documentation, including contingency and continuity plans with details of actions to be taken and responsibility for these
- implement preventive actions and adjust planning documentation and routines when weaknesses are identified
- perform regular exercises that test and improve preparedness and planning

3.6.4 Safeguarding of assets

Assets which the organisation owns or disposes of will fall into various categories and they can be impaired or destroyed for a number of reasons and in very many different ways. Thus, there is a great variation in how assets can be maintained and protected or developed. Many of the components mentioned above in these Guidelines relate either directly or indirectly to the protection of value, but the subject matter is so all-encompassing that it should be specifically addressed. It is not possible to address all the possible reasons for impairment or loss of value, but a few variants will be mentioned in order to illustrate the breadth of the challenges faced: Inappropriate use and/or inadequate maintenance of buildings, machinery, equipment, fixtures and vehicles, theft or embezzlement of cash, goods, art etc., loss of inventory, failure to maintain legal claims on account receivables, losses due to fluctuating exchange rates and the value of securities, destruction due to fire and natural disasters, sabotage on real estate and equipment, failure to register or protect immaterial values such as trademarks, patents and copyright, as well as unauthorised access to (and use of) internal information and business secrets. Various forms of collusion with third parties can also result in the loss or impairment of the organisation's assets. The same applies when an employee is an independent party in the development of ideas, concepts or products.

It is a very demanding task to protect and maintain all these types and varieties of assets and, if possible, increase their value. It is for this reason crucial to have a well-functioning system for risk management cf. chapter 3.3 above. In the risk management process the various assets should be identified and their risk evaluated so that tailor-made actions may be initiated to protect them.

Practical approach

The organisation should:

- establish and make known the roles, responsibilities, and authorities in the relevant areas
- perform risk assessments and implement control measures when the organisation obtains possession of new physical or immaterial assets
- regularly review, identify and assess risk for the organisation's material and immaterial assets with the help of personnel with the requisite professional knowledge
- implement new control measures and as necessary remove or tweak already established controls, where this is called for by the risk assessments performed
- ensure that measures for the protection of values are also implemented by third parties
- enter into binding agreements and ensure that the parties are agreed as to ownership in those cases where employees or external parties are involved in projects or development work

3.6.5 Human resource and competency management

The enterprise implements systematic activities to identify, recruit, build and retain the appropriate competence to perform its tasks and achieve its objectives. This requires knowledge as well as understanding of the organisation's current and future need for expertise.

Practical approach

The organisation should:

- regularly perform gap analyses to identify current status of skills and those required in the future and devise strategies and plans to close the gap
- put in place processes to recruit, develop, maintain, and hire the required skillsets in sufficient quantity
- have measures in places that ensure skills transfer and experience-based learning
- identify and develop potential managers and professional experts, and plan for any loss of persons with key skills
- establish a system to address health, safety, and environmental requirements, including employee satisfaction

4 Learning and improvement

An enterprise which has established structures and processes for planning and daily operations will need to supplement this with satisfactory processes for learning and improvement. The external context and internal conditions will be frequently changing, and it is therefore important to have satisfactory processes for continuous learning and improvement so that the organisation will be well prepared and equipped for the future. Learning and improvement takes place at all levels in the organisation. In chapter 0.7 above it was emphasised that the various components of governance will to a large extent interconnect, take place simultaneously and influence each other. As illustrated in figure 3 below, this will be particularly applicable to the components of Learning and improvement.

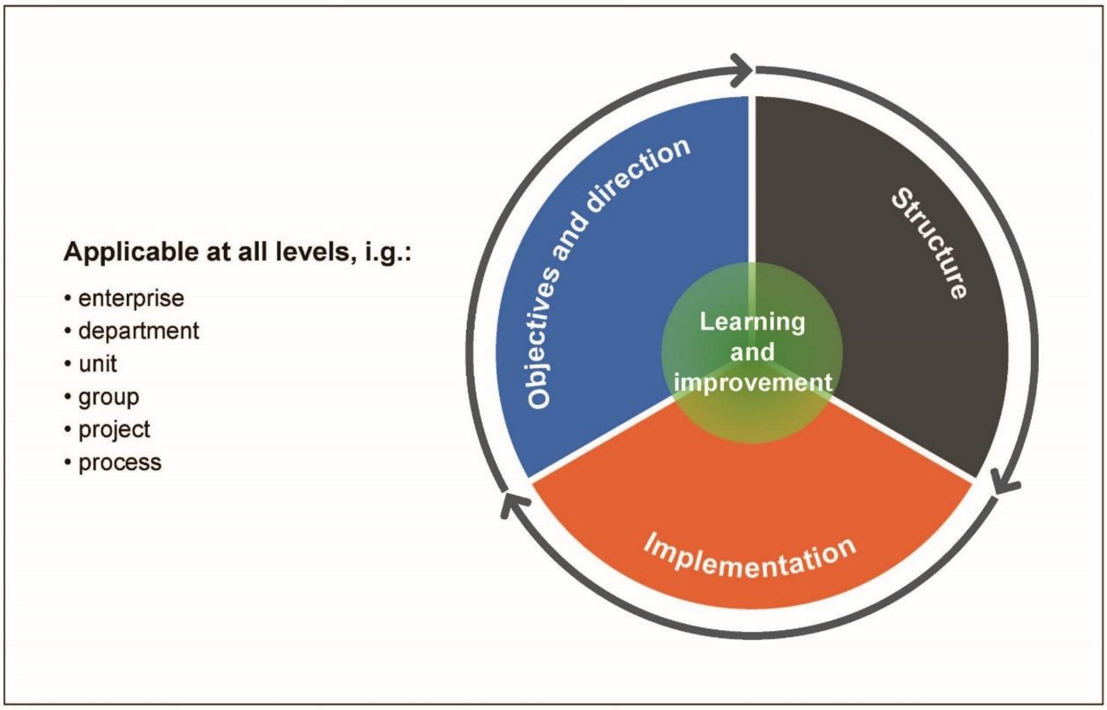


Figure 3: Learning and improvement

Learning and improvement will arise out of evaluations from the implementation phase or the comparison of an analysis of data and results against the desired development and objectives. This should provide the basis for identifying and taking decisions on improvement actions at all levels of the enterprise. Evaluations independent of line management, as well as controls and objective assurance from those not responsible for the day-to-day operations, will strengthen the basis for learning and improvement in the organisation.

4.1 Monitoring and evaluation

Systematic monitoring and evaluations are established for all key activities so that deviations and undesired trends may be discovered and mitigated

Weaknesses and errors or the potential for improvement will always be present both in how the basic activities in the enterprise are performed and how control activities function. It is therefore important to have in place systematic, continuous monitoring and assessment of the enterprise. This is defined here as "monitoring and improvement". Monitoring and improvement will enable the early detection of deviations, undesired trends, and possibilities for improvement. Monitoring will also form the basis for the evaluation of risk areas, follow up at appropriate levels and the timely implementation of mitigating actions.

Practical approach

The enterprise should:

- ensure that major activities and risk exposed areas identified by deviation reports, risk management or other processes, are continually and systematically monitored
- evaluate deviations and undesired trends arising from monitoring activities, i.e. by analysing them and evaluating whether there are risks which need to be mitigated by actions
- clarify whether the responsibility for monitoring and evaluation should, in certain areas, be assigned to a staff- or support function

4.2 Control functions independent of line management

Control functions independent of line management contribute to the development and improvement of the enterprise's governance and operations

In a number for industries and sectors there are official requirements as to the establishment of control functions independent of line management, often called second line functions[7]. Even when this is not an imposed requirement, enterprises of a certain size will often find such functions useful. These second line functions should be independent of the operational activities and function as controlling and advisory entities for the enterprise. They should have an open dialogue with the rest of the enterprise and have access to all information of importance to perform their tasks. The control functions can be important contributors to the development of governance and decision-making principles and the administration of frameworks for governance and control. They can also contribute by providing advice, guidance, and suggesting improvements in control activities, as well as the identification of deviations from the desired development and help the enterprise focus on and react to these. The control functions should report to a management level with executive authority.

Practical approach:

The enterprise should:

- consider establishing control functions independent of line management e.g.:
  - a risk management function with responsibility for establishing and maintaining a framework, methodology and processes for risk management (cf. chapter 3.3)
  - a compliance function to monitor compliance with applicable laws and internal rules and resolutions (cf. chapter 3.4)
  - a controller function which monitors and analyses performance development, profitability, and the achievement of objectives in general
  - functions in other areas such as for example health, safety, security and environment, quality systems and misconduct

[7] *Cf. attachment 2: The Three Lines Model*

- consider whether the control functions independent of line management should have a responsibility for courses and training
- approve a placement in the enterprise for the control functions independent of line management which ensures independence from those parts of the enterprise being controlled
- approve reporting lines which give the functions both the right and duty to report to a management level with executive authority

4.3 Objective assurance

Objective assurance and advice provide the Board and management with a more reliable and sufficient basis for decision-making

It is of critical importance that the Board and management can rely on the fact that the information they build their assessments and decisions on is relevant, reliable, and sufficient. The degree of comfort experienced will increase if the systems, controls, and information is confirmed from an independent source not having any responsibility for the day-to-day operations. Internal audit is one such function, also often called a third line function[7]. The establishment of such an independent, objective assurance and consulting function is required by the authorities in many industries and sectors, but even when there is not a requirement many organisations find it useful to establish an internal audit function.

Internal audit shall contribute to enhancing and protecting organisational value by providing risk-based and objective assurance, advice, and insight. It evaluates the established governance- and control activities and contributes to their improvement. The function's independence and authority are strengthened when the head of internal audit is appointed by and reports directly to the Board.

Internal audit is a profession which operates under a code of ethics, standards and guidance which is published by the international organisation "The Institute of Internal Auditors (IIA)" and by the national institute "IIA Norway". These delineate how the internal audit function should maintain its independence, objectivity, and professionalism as well as how the work should be managed and planned, including requirements in respect of analysis techniques, documentation, and reporting. Internal audit personnel can be employed by the enterprise and will thereby build up in depth knowledge of it, knowledge which will be retained within the organisation. The function may also be outsourced giving the enterprise increased flexibility and access to expert knowledge. The two variants may also be combined.

Many bodies external to the enterprise may have the authority to scrutinise the organisation's activities and issue confirmations, instructions and advice that will be of importance to governance. For example, the external auditor responsible for the financial statement audit and various inspection and supervisory authorities who perform controls in the area of their responsibility (for example in the areas of food safety, public health, financial institutions, employment and competition law). In the public sector instructions and recommendations will be issued after local and government audits. These external functions/ control bodies are however not a part of the internal governance and the Board or management cannot themselves decide whether or when these objective inspections will be carried out. They will therefore not be addressed in any further detail in this document.

[7] *See attachment 2: The Three Lines Model*

The suggestions to a practical approach of the subject provided below will therefore only apply where the Board has approved the establishment of an internal audit function, a resolution which should be explained and minutes.

Practical approach

The enterprise should:

- approve an internal audit instruction in conformity with the IIA-standards
- evaluate whether internal audit personnel shall be employed in the enterprise or whether the function shall be outsourced either in whole or in part
- emphasise the need for the head of internal audit to have the requisite integrity, authority, and professional skills
- establish a reporting system whereby internal audit will give regular and relevant information to the Board and executive management
- address to what extent internal audit may carry out consulting activities for the Board and management, including issuing confirmations

4.4 Continuous learning and improvement

The need for improvement and learning is continually identified and actions are implemented

Errors, unwanted events and the need for improvements to the activities of the enterprise will often be detected and corrected through the internal control measures established, but in that case only those directly involved in the matter will normally be informed and learn from it. Learning should not stop there but also be disseminated to others who might experience similar challenges and to those who have the responsibility and authority to implement necessary changes. The enterprise’s ability to establish continuous learning and improvement may be crucial to future development and survival. The satisfactory solutions of yesterday will not necessarily be the best for tomorrow, so willingness to change and the ability to “work smarter” are crucial both in respect of formal, structured processes and more informal matters.

The enterprise may discover the need for change and improvement by performing evaluations and analyses (cf. chapter 4.1), from reports from second- and third line functions (cf. chapter 4.2 and 4.3) as well as from other information collected and received. The need for learning and training will best be addressed through a well-structured and robust system for learning and improvement, with effective channels for disseminating information, good structure to required courses and training, and the allocation of sufficient time and resources.

Practical approach

The enterprise should:

- emphasise the need to create a culture for continuous learning and improvement
- put in place systems which identify the need for change and improvement
- ensure that identified needs for change and improvement are reported to those responsible
- verify that resource requirements related to learning and improvement activities are included in the enterprise’s budgets and plans
- establish routines for implementing learning and improvement activities

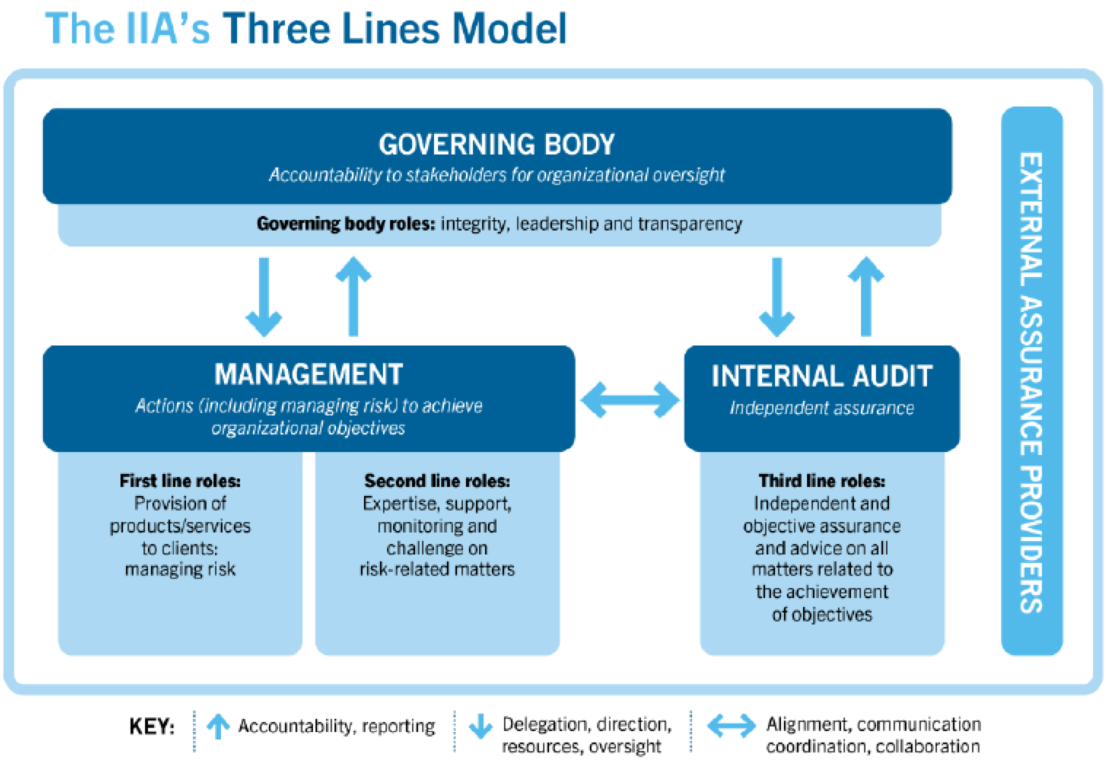
Attachment 1: Components

Objectives and direction	
Mission	The mission describes the enterprise’s reason for existence as well as delineates the bounds of its operations and activities
Vision	The enterprise’s vision expresses the idea over the longer term of what the enterprise aims to achieve and forms the basis for objectives and strategies
Values	The enterprise’s values express the values that the enterprise wishes to uphold and will form the basis for building a cultural identity
Objectives and strategies	Objectives and strategies support the enterprise’s vision and values
Structure	
Organisation, responsibility, and authority	The organisational structure with a clear delineation of responsibility and authority is appropriate to the enterprise
Information and communication	Relevant, reliable, and sufficient information is made available and timely communicated
Remuneration and reward schemes	Remuneration and reward schemes support the organisation’s objectives and values
Implementation	
Operational planning	Strategic objectives are rendered into specific goals and action plans
Management of core processes	Core processes are defined, managed and documented
Risk management	Risk management assists in the management of uncertainty in respect of the achievement of the organisation’s objectives
Compliance with laws and regulations	The organisation operates in compliance with laws and regulations
Financial management	Financial management supports decision-making and contributes to the organisation’s access to and use of resources
The management and protection of other assets, resources, and processes	Other assets, resources and processes are identified, managed and protected
Learning and improvement	
Monitoring and evaluation	Systematic monitoring and evaluations are established for all key activities so that deviations and undesired trends may be discovered and mitigated
Control functions independent of line management	Control functions independent of line management contribute to the development and improvement of the enterprise’s governance and operations
Objective assurance	Objective assurance and advice provide the Board and management with a more reliable and sufficient basis for decision-making
Continuous learning and improvement	The need for improvement and learning is continually identified and actions are implemented

Attachment 2: The Three Lines Model

The Institute of Internal Auditors (IIA) published in 2013 a Position Paper with the title *The Three Lines of Defense in effective Risk Management and Control.* The document described a model which achieved significant recognition and wide usage. However, many people felt that the use of the word defence gave an unfortunate signal that risk management and control is primarily concerned with defending the enterprise against negative incidents and not about taking offensive action and grasping the possibilities that may exist for improving the achievement of objectives. For this reason, the IIA published in 2020 an updated version of the model with the title *The Three Lines Model*. In this latest document it is emphasised that risk management is as much a matter of identifying and grasping opportunities as of ensuring control and a satisfactory defence, as described in the initial model. The mode focuses on both *upside and downside* risk cf. paragraph 3.3 Risk Management. The model can be summarised in the following figure:

IIA Three lines model


The IIA's Three Lines Model
GOVERNING BODY
Accountability to stakeholders for organizational oversight
Governing body roles: integrity, leadership and transparency
MANAGEMENT
Actions (including managing risk) to achieve organizational objectives
First line roles: Provision of products/services to clients; managing risk
Second line roles: Expertise, support, monitoring and challenge on risk-related matters
INTERNAL AUDIT
Independent assurance
Third line roles: Independent and objective assurance and advice on all matters related to the achievement of objectives
EXTERNAL ASSURANCE PROVIDERS
KEY:
Accountability, reporting
Delegation, direction, resources, oversight
Alignment, communication coordination, collaboration

Copyright © 2020 by The Institute of Internal Auditors, Inc. All rights reserved.

The model illustrates that the Board (the governing body) has the overall responsibility for ensuring the establishment as well maintaining an oversight of an enterprise's risk management and internal control. Senior management has the day-to-day responsibility for activities leading to the achievement of organisational objectives, including risk management, and that the first and second line have key roles to play in discharging this responsibility. First line roles are closely tied in with the enterprise's core activities of providing goods and services and include the roles of various support functions such as administration and HR.

The second line supports the first line by providing advice to the first line in the areas of risk management, compliance and monitoring of activities. The distinction between the first and second line may not necessarily be visible in the organisation chart.

The third line is the internal audit function which provides objective and independent assurance and advice to the Board and management in the areas of governance and risk management (including internal control).

While the first and second lines are part of line management and report to them, the internal audit/the third line will in contrast be employed by and report to the Board (the highest level of governance).

The external audit and various supervisory authorities are also included in the model (External assurance providers).

Preparation of the Guidelines

These Guidelines for governance were prepared by the Professional practice and methodology committee of IIA Norway. An exposure draft was circulated for comment and the committee expresses its gratitude to all the parties who responded and provided a valuable contribution to the final document.

The members of the Professional practice and methodology committee are experienced professionals drawn from managerial positions in internal audit and risk management and who have participated in various national and international professional bodies. IIA Norway extends its thanks to:

- **Tor Solbjørg**, Internal Audit, Helse Nord RHF
- **Rune Johannessen**, Group Risk Management, Gjensidige
- **Trygve Sørlie**, Service Provider, Trygve Sørlie Services EPF
- **Martin W. Stevens**, Group Internal Audit, Gjensidige
- **Cecilie Thorberg**, Internal Audit, Oslo University
- **Linda Lillestøl**, Internal Audit, Norwegian Refugee Council

This translation of the Guidelines was initially prepared by Martin Stevens for whom English is his mother tongue, however, all committee members have participated in a rigorous quality assurance process resulting in an accurate and appropriate translation. Some changes in content were however made to the introductory paragraphs 0.1 and 0.3 to ensure the relevance to an English-speaking public.

About IIA Norway

IIA Norway is a professional body open to all working within or with an interest in good governance and focussed on internal audit, risk management and compliance. The mission of IIA Norway is to provide members with a sound professional foundation and strengthen organisations' knowledge of management, control, and internal audit.

We have established professional and participatory networks for the sharing of experience and knowledge. We have separate networks, for finance, leaders, public sector, compliance and business ethics, risk management, and IT audit. Each network consists of committed members drawn from various organisations within or across specific industries. As a member of IIA Norway you have the opportunity to participate in all networks and have access to tools and documentation from the networks. For further information see www.iia.no.

Other relevant Guidelines from IIA Norway available in English are:

- Guidelines for the Compliance function
- Good Practice Guidelines for the Enterprise Risk Management Function
- Questions a board may ask to understand how an organisation controls its risks

IIA Norway also provides further education, leading to the following certification and diplomas:
Diplomert internrevisor
Certified Internal Auditor (CIA)
Certification in Risk Management Assurance (CRMA)