



MATURITY MODEL FOR GOVERNANCE

1st Edition 2022

Table of content

1.	Introduction.....	3
1.1.	The purpose of the Maturity Model.....	3
1.2.	Relationship with Guidelines for Governance	3
1.3.	Structure of the maturity model	3
2.	Use of the Maturity Model.....	4
3.	The Maturity Model	5

1. Introduction

1.1. The purpose of the Maturity Model

This Maturity Model for Governance (the Maturity Model) is intended as a governance tool to be used in mapping the level at which the organisation is managed. Using the model may provide insight into the organisation's current situation and create a basis for improvement, and thus contribute to the organisation's achievement of goals.

1.2. Relationship with Guidelines for Governance

The Maturity Model is based on the IIA's Guidelines for Governance (The Guidelines) from 2021. The Maturity Model is aimed at the same target group as The Guidelines, i.e., everyone with responsibility for governance in the private or public sector, as well as others who have a role in the governance area or an interest in the topic.

The Guidelines state that governance is about facilitating management and other employees in the fulfilment of their responsibilities and tasks to achieve the organisation's goals, plan for good risk management and internal control, facilitate efficient and appropriate operations with the necessary follow-up and reporting, and establish effective, independent controls and assurance. The Guidelines break governance down into 17 components divided into four subjects, and this Maturity Model follows the same pattern.

1.3. Structure of the Maturity Model

The Maturity Model outlines five different maturity levels for each of the 17 components identified in The Guidelines. For each component, suggestions are given as to how the maturity can be assessed and sorted under each individual level. In practice, there will be no sharp distinctions between the levels, but the model's description of the various levels provides guidance for assessment and positioning. The five position levels are defined as Random, Started, Established, Developed and Optimised. The levels may be understood as follows:

Level	Name	Description of what characterizes governance at this level
1	Random	Governance does not appear to be formalized and / or is random.

2	Started	Governance is deficient, but under development. There are to a limited extent comprehensive solutions and common definitions.
3	Established	Governance is satisfactory. Comprehensive solutions and common definitions have been established.
4	Developed	Governance is well-functioning. Work is done systematically, and improvement measures are assessed / implemented.
5	Optimised	Governance is subject to continuous improvement, rationalisation and ongoing follow-up. This is integral to the culture.

For the model to be as simple and user-friendly as possible, the text in levels 3-5 are mainly derived from each other, avoiding the repetition of text in levels 3 and 4 at the next level.

2. Use of the Maturity Model

The Maturity Model provides a practical approach in assessing the maturity of governance and may be a useful tool for both first-, second- and third-line functions.

The advantage of a number scale (1-5) is that you are given an immediate indication of the level of maturity, and a visual image that is easy to communicate and provides a basis for further assessments. However, the choice of level should always be justified. The figures themselves, without an accompanying justification, give less value.

A qualitative aspect is the basis for placement at levels 1-5. If it is desirable to improve the quality of a component, the text at the next level will provide suggestions for improvement goals that can help raise the level of governance. For example, the maturity in governance for component “4.3 Objective confirmations” may be increased from level 3 to 4 by fully applying IIA's standards. However, the results of a survey can also conclude that governance is at the desired level, e.g., because the cost of achieving a higher level is believed to be greater than the benefit this provides. This must be evaluated in each case and may be dependent on many different factors. The Maturity Model must, like The Guidelines, be adapted to industry and sector, the organisation's size and complexity, organisational culture etc.

The model is flexible in use. It can be used for all or parts of the organisation, and it is not necessary to consider all the components at the same time. As mentioned in the introduction, the model may be used to assess maturity within a limited part of the business, e.g., a department or a larger project and it is not necessary to evaluate all the subjects or components of the model at the same time. Perhaps one just wants to consider some of these, e.g., the component “Objectives and direction”, or the components “3.4 Compliance with laws and regulations” and “3.5 Financial management”. With such limited use of the model, there may be a need for adaptation, e.g., a project may lack a fully developed vision, but can have both overall and operational goals. When choosing to evaluate only a single component (or a few components), the model may be used as a checklist. In this case the term "Governance" may be somewhat misleading. A limited assessment may still provide some value to the user.

It will often be required to make a summary assessment based on the assessments made of individual components / subjects, but then it is not certain that pure quantitative methods provide the best and most credible answer to where the overall level of maturity lies, and mathematics must be supplemented by use of professional judgment. Furthermore, in the assessment of the individual component, it will often be found that certain elements indicate one level, while other elements / conditions "belong" at another level. In such case it is equally important to perform a discretionary assessment.

3. The Maturity Model

Level	1	2	3	4	5
Description	Random	Started	Established	Developed	Optimised
Objectives and direction	Basic prerequisites for structuring the organisation and for efficient and appropriate operations				
1.1 Mission <i>The mission describes the organisation's reason for existence as well as delineates the bounds of its operations and activities</i>	The organisation lacks a formal mission or has a defined mission that is misleading in relation to what it is intended to do.	The mission does not provide a precise description of the purpose of the organisation. There is little knowledge about the mission in the organisation.	The mission describes the purpose of the organisation and what needs are to be addressed and suggests the framework for its operation and activity. The mission is adopted by the owners, it is known in the organisation and is available to external stakeholders.	The mission is clearly formulated and provides a precise description of the framework for the organisation's operations and activities.	There is a regular assessment of whether operations and activities are within the mission of the organisation. If this is not the case, the mission will be adjusted, or the operations / activities will be amended or discontinued.
1.2 Vision <i>The organisation's vision expresses the idea over the longer term of what the organisation aims to achieve and forms the basis for objectives and strategies</i>	The organisation has no expressed vision.	The vision is deficient, or vaguely worded.	The vision is clearly formulated, and in accordance with the purpose of the organisation. It gives a clear indication of what the organisation will achieve in the long run.	The vision is a suitable basis for the organisation's work on objectives and strategy. It is inclusive and unifying and is well known and rooted in the organisation.	The vision signals a high level of ambition and is inspiring.
1.3 Values <i>The values express what the organisation wishes to stand for and forms the basis for building</i>	The organisation has not adopted, defined, or described its core values and ethical guidelines, social responsibility, and maintenance of	The organisation's core values, ethical guidelines, social responsibility, and transparency are deficient or not clearly defined.	Values have been defined and rules and guidelines have been established in all significant areas related to behaviour, ethics, social responsibility, and openness. These are to a large	The values are fully incorporated and are part of the organisation's culture.	Regular assessments are made of whether the set values are maintained at the desired level, and complied with in daily operations.

Level	1	2	3	4	5
Description	Random	Started	Established	Developed	Optimised
<i>and maintaining a cultural identity</i>	transparency regarding decisions, activities, and results.		degree known and implemented in the organisation.		
1.4 Objectives and strategies <i>Objectives and strategies support the organisation's vision and values</i>	The organisation lacks overall and formal objectives.	The organisation's strategic / overall objectives appear to be deficient and unclear and are to a lesser extent known in the organisation.	Strategic / overall objectives have been adopted in key areas, and are known and understood in the organisation. They build on the organisation's vision and values, and a strategy has been adopted for how they are to be achieved	The strategies are based on critical success factors and on internal and external analysis of the current situation and cover all significant organisation areas.	Different scenarios for future development with associated risk assessments are prepared. The organisation's overall objectives and strategies are adjusted accordingly.
Structures	Structures for decision-making processes, responsibilities, and authority, etc. form the basis for the organisation's implementation of strategies and fulfilment of its goals				
2.1 Organisation, responsibility, and authority <i>The organisational structure with a clear delineation of responsibility and authority is appropriate to the organisation</i>	The organisation lacks responsibility and authority structure.	The organisation's responsibility and authority structure appear to be fragmented and / or unclear. It is to a limited extent documented, known by and anchored in the organisation.	The organisation has a clear responsibility and authority structure that is documented, known, and anchored in the organisation. Mandates, instructions, principles of probity etc. have been prepared for some functions and areas.	The responsibility and authority structure are at all times adapted to the organisation and covers all its levels. Mandates, instructions, principles of probity, etc. have been adopted for all important functions and areas, and the organisation's decision-making processes are traceable.	The responsibility and authority structure are continuously and systematically evaluated and updated. Separate management structures have been established to manage, coordinate, and prioritize portfolios, programs, projects, and processes across the organisation.
2.2 Information and communication <i>Relevant, reliable, and sufficient information is made available and timely communicated</i>	The organisation lacks an overview of target groups and stakeholders for information and communication. The need for information is not defined, nor who is to collect and communicate the information.	The overview of the organisation's stakeholders, and their information needs is deficient. It has not been clearly clarified who is responsible for information and communication, and how this should be communicated.	The organisation has an overview of stakeholders and their information needs. The division of tasks, as well as the time and manner of communication, have been clarified. Routines have been communicated to the organisation.	Responsibilities, roles, and tasks related to information and communication are clearly defined and well known in the organisation. Action plans have been adopted for the information activity, including the handling of crisis situations. Appropriate information to the board, management and other stakeholders is provided at the right time.	The organisation's overview of stakeholders is regularly re-evaluated and updated. Ongoing supervision is carried out to ensure that information and communication are handled in accordance with decisions and guidelines. Information and communication are regularly discussed with external and internal stakeholders.

Level	1	2	3	4	5
Description	Random	Started	Established	Developed	Optimised
<p>2.3 Remuneration and reward schemes</p> <p><i>Remuneration and reward schemes support the organisation's objectives and values</i></p>	The organisation lacks clearly defined remuneration and reward schemes.	Remuneration and reward schemes have not been adopted for all relevant staff groups. No routines have been established to ensure that union representatives are involved in the establishment or change of remuneration and reward schemes. The schemes are inadequately communicated and not well known.	The organisation has established remuneration and reward schemes for relevant staff groups. Trade union representatives participate in the planning and decisions and there is openness about the schemes, which are communicated to the organisation.	<p>The remuneration and reward schemes support the organisation's goals and values. There are board approved rules for the remuneration of managers and other employees with special tasks or areas of responsibility.</p> <p>The remuneration and reward schemes are assessed and updated regularly.</p>	The schemes reward contributions to long-term and ethically sound value creation and are designed with the aim of avoiding conflicts of interest.
Implementation	Strategic objectives are rendered into specific goals and comprehensive and co-ordinated management of the core and support processes				
<p>3.1 Operational planning</p> <p><i>Strategic objectives are rendered into specific goals and action plans</i></p>	Specific goals and action plans with indicators have not been developed.	Some specific goals and action plans have been defined and are, to some extent, being used for developing action plans and indicators. These are partly in line with the organisation's strategic goals and current situation.	Specific goals that are realistic, meaningful and measurable have been developed and implemented and are supporting the strategic goals. Most of the specific goals have been rendered into action plans.	Action plans includes action points with set responsibilities and deadlines. Progress is monitored based on relevant indicators.	The specific goals, action plans and indicators are monitored, assessed, and adjusted on a regular basis.
<p>3.2 Management of core processes</p> <p><i>Core processes are defined, managed, and documented</i></p>	Key processes are not defined or documented.	Key processes are defined and documented in governing documents.	Key processes are defined and documented in governing documents and include integration with support processes. The processes are being managed and implemented as planned.	There are procedures for regularly assessing if the core processes are appropriate and efficient. If the development of indicators shows the need for adjustments, actions are taken to address this.	There is systematic follow up that all core processes are implemented as planned. Deviations are reported and addressed.
<p>3.3 Risk management</p> <p><i>Risk management assists in the management of uncertainty in respect of the achievement of the organisation's objectives</i></p>	There are no governing documents or processes for risk management and risk management principles have not been implemented.	The implementation of risk management is not systematic or is fragmented.	The board has set the mandate and guidelines for risk management in line with good practice, which are complied with by most of the organisation. Relevant personnel have adequate	Throughout the organisation's strategic and operational levels risk management is implemented. The implementation of internal controls, and the effect of these, are documented. The	Risk management is reinforced by the organisation's systematic development of a sound culture, and holistic organisation risk management is integrated in all governing processes and activities. Risk

Level	1	2	3	4	5
Description	Random	Started	Established	Developed	Optimised
			competence. The risk assessments are used for making decisions at different levels in the organisation.	need for a separate risk management function has been assessed.	appetite and tolerance are defined and (as far as possible) quantified. There are procedures for continuously identifying and assessing emerging risks.
<p>3.4 Compliance with laws and regulations</p> <p><i>The organisation operates in compliance with laws and regulations</i></p>	<p>There is no overview over applicable external and internal regulations. Compliance with external and internal regulations is not monitored or risk assessed.</p>	<p>The organisation's documented overview of important laws, rules and internal guidelines, and the control that such laws, rules and guidelines are followed, is deficient. The system for risk assessing compliance and following up identified requirements for improvement is fragmented.</p>	<p>There is a documented overview over all key internal and external regulations. These are integrated into governing documents. Risk assessment and controls are being carried out and contribute to compliance with internal and external regulations.</p>	<p>The documented overview over all key internal and external regulations is continuously updated. The risk of non-compliance is systematically assessed, and in key business areas, compliance is continuously monitored. Employees are systematically trained and continuously informed about relevant regulations. The need for a separate compliance function has been assessed.</p>	<p>The organisation systematically monitors and assesses opportunities to improve and streamline systems and routines related to compliance. Development and maintenance of a culture with a conscious and positive attitude to compliance is included in the organisation's ongoing work with values (see component 1.3).</p>
<p>3.5 Financial management</p> <p><i>Financial management supports decision-making and contributes to the organisation's access to and use of resources</i></p>	<p>There are no functions or structure for financial management.</p>	<p>The financial management system and structure is fragmented.</p>	<p>The financial management system complies with the legal requirements and reflects the organisation's activities. The financial management function's place in the organisation, tasks, responsibilities, and reporting lines are defined.</p>	<p>Long-term plans, budgets and forecasts are prepared in accordance with goals and action plans. Developments in relation to budgets and plans are measured and reported.</p>	<p>Informative key financial figures have been defined, and are reported on, which provide management with a decision basis for quickly implementing measures or correcting course if necessary.</p>
<p>3.6 The management and protection of other assets, resources, and processes</p> <p><i>Other assets, resources and processes are identified, managed, and protected</i></p>	<p>Management of assets, resources and processes is missing, fragmented, or done as ad hoc activities.</p>	<p>The organisation's processes and resources are not systematically controlled, and the values are inadequately promoted and protected.</p>	<p>The organisation has defined and to a large degree implemented roles, responsibilities, and authorities for the protection of assets and for the management of important processes and resources.</p>	<p>Plans and routines for managing values, processes, and resources support the organisation's goals and strategy.</p>	<p>Plans and routines for managing values, processes, and resources are regularly (risk) evaluated and improved.</p>

Level	1	2	3	4	5
Description	Random	Started	Established	Developed	Optimised
Learning and improvement	Identification and implementation of processes for learning and improvement				
4.1 Monitoring and evaluation <i>Systematic monitoring and evaluations are established for all key activities so that deviations and undesired trends may be discovered and mitigated</i>	The organisation has not established systematic follow-up and control of how key activities and risk-exposed areas are carried out, and the functioning of important control measures.	The organisation's follow-up and control of key activities, risk-exposed areas, and important control measures take place randomly and unsystematically. Detected deviations are not systematically analysed and assessed.	Monitoring is systematically carried out and documented, in accordance with the described routines. The organisation has assessed if an assigned staff- or support function should perform these tasks.	Deviations and developments are evaluated and analysed and form a good basis for assessing the initiation of further measures.	Monitoring takes place continuously and is largely automated. Routines have been established for automatic analysis against predefined target figures / KPIs, and for learning and improvement.
4.2 Control functions independent of line management <i>Control functions independent of line management contribute to the development and improvement of the organisation's governance and operations</i>	It has not been assessed whether there is a need or requirement for line-independent control functions in the organisation, and such functions have not been established. It may have been concluded that there is a need for such second-line functions, but these have not been established.	Line-independent control functions have been established, but roles and responsibilities are not clearly defined. The functions have an organisational position that does not safeguard the independence of the operational activities they control.	The roles and responsibilities of the control functions are defined. The organisational position gives independence from the line management being controlled. The functions report to a management level with executive authority.	The function actively contributes to keeping up to date and assures compliance with the framework and methodology relevant to the area being controlled. The functions' advisory and guidance tasks are prioritised and attended to.	The organisation has routines to ensure that those responsible for the second-line functions are always kept professionally updated. It has been assessed and decided to what extent the functions should be responsible for the training of personnel who perform tasks the functions control. It is continuously assessed whether control functions have been established in all parts of the business where this is appropriate.
4.3 Objective assurance <i>Objective assurance and advice provide the Board and management with a more reliable and sufficient basis for decision-making</i>	An independent assurance function has not been established to provide the board and management with objective assurance. An assessment has not been made of whether there is a need for, or requirement for, such a body.	The organisation has, through hiring or outsourcing, established a function with the purpose of providing the board and management with objective assurance. The assurance function, often referred to as internal auditing, is not entirely independent of the management, and does not carry out its work in accordance	The organisation has adopted an internal audit instruction and established an internal audit function (third-line function) in accordance with IIA's standards for the professional performance of internal auditing. These standards, and the IIA's ethical rules, are largely complied with. Alternatively, an internal audit function has not been established, because an	IIA's standards for the professional performance of internal auditing, with core principles, as well as the ethical rules and guidance from IIA, are fully complied with. When performing advisory services, the internal audit maintains its objectivity, and does not assume managerial responsibility.	The internal audit issues an overall statement that at an overall level discusses the organisation's governance, risk management and / or control. It considers the organisation's strategies, goals, and risks and meets the agreed expectations from top management, the board, and other stakeholders.

Level	1	2	3	4	5
Description	Random	Started	Established	Developed	Optimised
		with national and international standards.	assessment has been made with the conclusion that there is no need for, or requirement for, internal audit in the organisation.		
4.4 Continuous learning and improvement <i>The need for improvement and learning is continually identified and actions are implemented</i>	The organisation has not established processes where discovered errors and weaknesses are made known to others than those who are directly involved in the relationship, or systems which would allow the identification of the need for changes and improvements.	Errors, adverse events, and the potential for improvements that have been identified through internal control and monitoring, or by second- or third-line functions, are to a small degree registered and reported as a source for change and improvements. Arenas and routines for systematic learning and improvement measures have not been established.	The organisation has established routines for systematically registering and reporting identified needs for change and improvements. An arena and routines for systematic learning and improvement measures has been established.	Learning and improvement are put into a system in the organisation and approached in a holistic and proactive manner. The organisation has effective channels for the communication of information and good arenas for courses and training.	Culture for continuous learning and improvement is emphasized and maintained in the organisation, e.g., by using a well-functioning reporting system for deviations. Resource needs related to learning and improvement measures are addressed in budgets and plans.

Preparation of the Maturity Model

The Maturity Model for Governance has been prepared by the Professional practice and methodology committee of IIA Norway.

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:

- **Cecilie Thorberg** Internal Audit, Oslo University
- **Tor Solbjørg** Internal Audit, Helse Nord RHF
- **Rune Johannessen** Group Risk Management, Gjensidige
- **Jan-Rune Brox** Internal Audit, Vår Energi ASA
- **Merete Skjelsbæk** Quality Assurance, Norwegian Geotechnical Institute (NGI)
- **Linda Lillestøl** Ethics and integrity, Norwegian Department of Defence

About IIA Norway

IIA Norway is a professional body open to all working within or with an interest in good governance and focused 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.iaa.no.

Other relevant guidelines from IIA Norway available in English are:

- Guidelines for Governance
- Good Practice Guidelines for the Organisation Risk Management Function
- Guidance for the Risk Management Function
- Risk Management Maturity Model
- Guidelines for the Compliance 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)