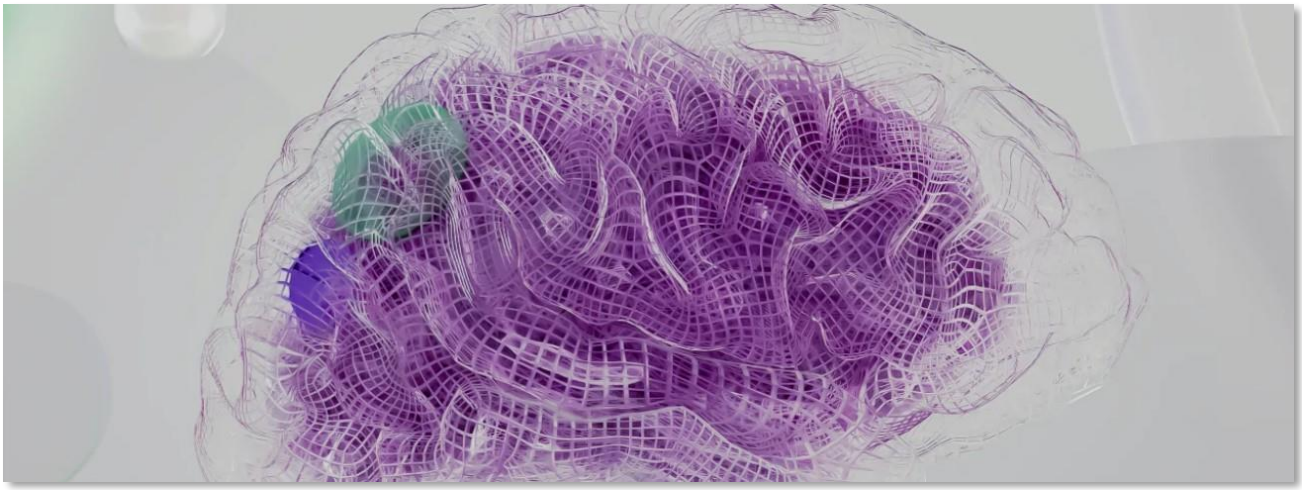
AI & Partners

EU AI Act Compliance Management Capability Maturity Model

A tool for assessing and improving the performance of EU AI Act Compliance Risk Management for firms operating in the EU



EU AI Act Compliance Risk Management Capability Maturity Model

AI & Partners

Disclaimer

The contents of this document are for information purposes only. AI & Partners assumes no liability or responsibility for any inaccurate or incomplete information, nor for any actions taken in reliance thereon. The published material is distributed without warranty of any kind, either express or implied, and the responsibility for the interpretation and use of the material lies with the reader. In no event shall, AI & Partners be liable for damages arising from its use.

AI & Partners takes no responsibility for the content of any external website referenced in this publication or for any defamatory, offensive or misleading information which might be contained on these third-party websites. Any links to external websites do not constitute an endorsement by AI & Partners, and are only provided as a convenience. It is the responsibility of the reader to evaluate the content and usefulness of information obtained from other sites.

The views, thoughts and opinions expressed in the content of this publication belong solely to the authors and do not necessarily reflect the views or policies of AI & Partners, their partners, their consultants, nor does it imply any endorsement. Therefore, AI & Partners carries no responsibility for the opinions expressed in this publication.

AI & Partners does not endorse or recommend any product, process, or service. Therefore, mention of any products, processes, or services in this document cannot be construed as an endorsement or recommendation by AI & Partners.

The contents of this document may be quoted or reproduced, provided that the source of information is acknowledged. AI & Partners would like to receive a copy of the document in which this publication is used or quoted.

EU AI Act – Advisory | Consultancy | Compliance Software
+31 6 57285579 and +44(0)75 35994 132
s.musch@ai-and-partners.com and m.borrelli@ai-and-partners.com
https://www.ai-and-partners.com/
https://twitter.com/AI_and_Partners @AI_and_Partners
https://www.linkedin.com/company/ai-&-partners/

EU AI Act Compliance Risk Management Capability Maturity Model

AI & Partners

Preface

This document is a guide for businesses operating in the European Union ("EU") to assess and improve their EU Artificial Intelligence Act (the "EU AI Act") Compliance Risk Management ("CRM") using a Capability Maturity Model ("CMM"). The guide outlines the purpose of the framework and explains how to apply the model.

High commercial performance in EU is strongly dependent on how well businesses succeed in making rational decisions to promote EU AI Act compliance and prevent non-compliance among businesses. The central aim of EU AI Act CRM Management is to help businesses to make these decisions. The CMM supports improvements of organisational capabilities important for reaching high performance doing EU AI Act CRM.

The model supports analyses related to the maturity of the EU AI Act CRM by prompting the questions: 'Where are we now?' 'Where do we want to be?' and 'How do we get there?'

The main objective of the model is to support businesses in their efforts to improve their EU AI Act CRM by leading them to a desired maturity level. Correct use of the model will increase the probability for businesses to make the right choices to increase compliance among themselves.

The document is the result of AI & Partners with origins from the European AI Scanner.

EU AI Act – Advisory | Consultancy | Compliance Software
+31 6 57285579 and +44(0)75 35994 132
s.musch@ai-and-partners.com and m.borrelli@ai-and-partners.com
https://www.ai-and-partners.com/
https://twitter.com/AI_and_Partners @AI_and_Partners
https://www.linkedin.com/company/ai-&-partners/

EU AI Act Compliance Risk Management Capability Maturity Model

AI & Partners

Glossary

Acceptance of Compliance Strategies: Employees share the beliefs and values expressed by the compliance strategies.

Actions to Stimulate Compliance: Instruments for supporting the compliance strategies to reach expected outcomes as for example audits, information activities, letter campaigns and guidance with proactive (e.g. filing aids) or reactive (penalties) aims.

Ad Hoc: Something is done for a special and immediate purpose or for a weak purpose without previous planning.

Alternative: One of the two or more ways of achieving the same desired end, an objective or a new alternative.

Analysis: Systematic approach to addressing and evaluating alternatives. The objective of a decision analysis is to discover the most advantageous alternative.

As Is: Current state of EU AI Act CRM maturity.

Attitude: A predisposition towards a certain idea, object, person, or situation. Attitudes often determine what we do.

Awareness: Employees perceive the fact that the capability is important.

Business Intelligence Tool: Types of application software that collect and process large amounts of unstructured data from internal and external systems.

Capability: The ability of a business to collectively deliver organisation objectives.

Capability Maturity Model: A tool to assess how capable an business is regarding a defined subject (e.g. CRM) and to improve the capabilities needed to perform the subject.

Capacity: A specific ability measured in term of quantity and/or quality over a delimited period.

Choice: An opportunity to select.

Communication: Exchanging and transmitting information successfully by using effective channels.

EU AI Act Compliance Risk Management Capability Maturity Model

Communication Strategy: Typically consists of pre-structured and on regular basis planned programs, campaigns, and actions, as well as more ad hoc and reactive responses to urgent issues and stakeholder concerns.

Competency: Capability, ability, skill, aptitude, knowhow, experience, expertise.

Complementary Relationship: Two or more different things (as teams, functions, responsibilities and relations) improve or emphasize each other´s qualities.

Compliance: Willingness of businesses to fulfil their regulatory obligations related to the EU AI Act

Compliance Map: The level of assurance of the EU AI Act compliance for different businesses.

Compliance Objectives: A formal statement detailing a desired outcome related to compliance.

Compliance Risk: The threat or probability that an action or event will adversely affect the ability to achieve the compliance objectives.

Compliance Risk Management: A systematic process for making substantiated choices about how to effectively stimulate compliance and prevent non-compliance.

Compliance Risk Management Model: Shows the steps in the CRM process, set in context, compliance objectives and strategies.

Compliance Risk Management Process: Shows the different steps in the in the decision making cycle.

Compliance Strategy: A general guide to help reduce and eliminate risks and to make use of opportunities in order to reach compliance objectives.

Consciousness: Employees have a complete understanding of the capability and its relation to other capabilities and how capabilities relate to perform an effective CRM.

Consequence: A result of a chosen alternative. Can be both a negative and a positive result (outcome) and can include both effects on business behaviour perspective and resource costs from a business perspective.

Creativity: A process of thinking about new ideas and concepts.

EU AI Act – Advisory | Consultancy | Compliance Software
+31 6 57285579 and +44(0)75 35994 132
s.musch@ai-and-partners.com and m.borrelli@ai-and-partners.com
https://www.ai-and-partners.com/
https://twitter.com/AI_and_Partners @AI_and_Partners
https://www.linkedin.com/company/ai-&-partners/

EU AI Act Compliance Risk Management Capability Maturity Model

Criteria The decisive characteristics determining the maturity level.

Decision A choice made between alternative courses of action and a commitment to act.

Decision Tree: A flow chart that visualize different alternatives of actions, events that the business does not control, and consequences (outcome, resource costs etc.).

Define: Setting a boundary that controls what is relevant and important.

Description: Tells what something is or what someone is like.

Differentiation: A collective term for segmentation and profiling.

Documentation: To archive and register something so that the information not will be lost. Usually a document is written but a document can also be made with pictures, videos and sound.

Education: Aims to broaden individual knowledge of employees and to develop their intellect, which is a lifelong process.

Effective: Do the right things achieving an expected result.

Efficient: Do the right job achieving an intended result with the least possible effort.

Elements: Characteristics representing a capability reflecting how to transform an input to an output as efficiently as possible. For example by the use of certain actions processes, technologies and methods. All supported by attitudes and behaviour in line with desired risk culture.

EU AI Act: Horizontal, risk-based approach on the regulation of artificial intelligence in the European Union.

EU AI Act Compliance as a Field of Research Field of multidisciplinary research essentially explaining what compliance obligations under the EU AI Act apply to businesses.

Evaluation: Assessment of on-going or completed actions in relation to its own previously stated objectives.

Evaluation Method: A way to establish if the action of the business has indeed led to achieving the intended outcome.

EU AI Act – Advisory | Consultancy | Compliance Software
+31 6 57285579 and +44(0)75 35994 132
s.musch@ai-and-partners.com and m.borrelli@ai-and-partners.com
https://www.ai-and-partners.com/
https://twitter.com/AI_and_Partners @AI_and_Partners
https://www.linkedin.com/company/ai-&-partners/

EU AI Act Compliance Risk Management Capability Maturity Model

Evidence: Presentation of documents, records, testimony, and other such items to prove the level of maturity.

Explanation: Clarifies the causes and consequences why something is or someone is.

External: Context Includes all interested parties including business as well as legal societies, technological, social behaviour of business, economic conditions, etc.

Extract data: Retrieve data from various sources.

Forecasting: Predicting what will happen in the future by taking into consideration events in the past and present.

Function: Action or activity performed with a specific purpose.

Help: Question Aims to facilitate discussions and communications and to align thoughts when assessing the 'as is' and deciding the 'to be'.

Implementation Plan: List of actions, costs, expected difficulties, and schedules that are required to achieve the objectives in prioritized order related to a decision made by the business.

Implementation Process: A sequence of recurrent interdependent steps to implement a decision.

Innovation: Process of transforming creative thoughts into concrete features.

Intuitive: Something is done on the basis of personal experiences, feelings or beliefs, not on the basis of proven best practices, scientific findings, or other objective arguments.

Involvement in Compliance Strategies: Employees contribute to complete compliances strategies via acts, discussions, setting objectives, ways of thinking, etc.

Knowledge: Information combined with experiences, theories and data that gives an understanding in how to take effective action to achieve the compliance objectives.

Knowledge Management: Making the right knowledge available to the right people.

Leadership: All persons in the organisation, responsible for one or more teams on all levels of hierarchy having skills to motivate employees and provide them with the right conditions so that effective CRM work can be performed.

Manage Data: Integrate, store, prepare etc. data for analytics.

EU AI Act Compliance Risk Management Capability Maturity Model

Management: A function at the highest organisational level related to organising, timing, delegation, communication and to inspire and motivate their teams.

Maturity Level: Consist of predefined criteria as indicators, positions or stages on a scale of quantity, extent, or quality related to a capability.

Maturity Path: Describes the path to improvement based on predefined criteria that must be fulfilled to achieve a certain maturity level.

Method: Technique for collecting data and creating knowledge.

Monitoring: Supervising actions, processes etc. in progress to ensure they are on course and on schedule in meeting the objectives and performance objectives.

Opportunity: An exploitable set of circumstances in the environment as a chance for improvement and progress.

Option: One of the two or more ways of achieving the same desired end, an objective or a new alternative.

Organisational Structure: Division of work among employees in a business and the coordination of the activities related to CRM.

Outcome: Something that follows as a result or consequence from an output.

Outcome Evaluation: Focuses on measuring if the intended outcome is achieved.

Output: What is produced.

Prescriptive Decision Theory: Prescribes methods for making optimal decisions. Principles Predefined rules as for example how much uncertainty and which risks should be accepted.

Prioritization: Arrange something in order of importance to deal with the most important first.

Proactive Attitude: A predisposition to act in advance rather than to wait for something to happen.

Proactive Methods: Acting in anticipation by causing change.

Process: A collection of related, structured actions to convert inputs into outputs.

EU AI Act – Advisory | Consultancy | Compliance Software
+31 6 57285579 and +44(0)75 35994 132
s.musch@ai-and-partners.com and m.borrelli@ai-and-partners.com
https://www.ai-and-partners.com/
https://twitter.com/AI_and_Partners @AI_and_Partners
https://www.linkedin.com/company/ai-&-partners/

Process Evaluation: Focuses on the implementation of the CRM process or parts of it and attempts to determine how successfully the decisions are made by the CRM process.

Profile: A representation of an individual or a group of businesses in the form of, for example, a detailed description or a set of correlated data.

Rationality: To consider the most important values, available alternatives based on the information available.

Reactive Methods: Reacting to change when it happens.

Relation: Various connections in which persons are brought together.

Relevance/Relevant: Significant, important, and sufficient to support the cause in question.

Responsibility: A duty or obligation to perform or complete a task.

Reviewing: An account of the strengths, weaknesses, and the relevant developments related to expected objectives.

Risk: The threat or probability that an action or event will adversely affect an organisation's ability to achieve its objectives.

Risk Analysis: Most important aspects are investigated as frequency (the number of risks/risky businesses), likelihood and consequence. Risk analysis also involves the 'why' question: what is the reason for non-compliant behaviour.

Risk Appetite: A general level of risk that an organisation is willing to pursue or retain given objectives and resources.

Risk Assessment: Determines possible compliance risks, their likelihood and consequences, and the tolerance for such events.

Risk Culture: The system of values and behaviour, present in a business. Can also be expressed as a system of ideas and ways of behaving and communicating.

Risk Tolerance: The degree of variance from its risk appetite that an organisation is willing to pursue or retain for each risk.

Scenario: A description of possible future developments.

Segmentation: To divide businesses into groups and sub groups with similar characteristics.

Team: Two or more people who work together to achieve a common objective. A team can have one or more functions.

Theory: Systematic explanations of underlying reasons for a phenomenon or behaviour.

To Be: The desired state of CRM maturity.

Training: To gain or improve a specific skill to better perform a particular job.

Trend: A prevailing inclination in the way that people are behaving.

Uncertainty: A situation where the current state of knowledge is unknown, the consequences, extent, or magnitude of circumstances, conditions, or events is unpredictable.

Understanding Employees: comprehend why a capability is important.

Understanding of Compliance Strategies: Employees know how the compliance strategies works to achieve the compliance objectives.

Value: What one consider as important, desirable, or worthwhile. Values are the ends deciding how to formulate objectives, strategies and decide how to act.

EU AI Act Compliance Risk Management Capability Maturity Model

AI & Partners

Table of Contents

EU AI Act – Advisory | Consultancy | Compliance Software
+31 6 57285579 and +44(0)75 35994 132
s.musch@ai-and-partners.com and m.borrelli@ai-and-partners.com
https://www.ai-and-partners.com/
https://twitter.com/AI_and_Partners @AI_and_Partners
https://www.linkedin.com/company/ai-&-partners/

AI & Partners

EU AI Act – Advisory | Consultancy | Compliance Software
+31 6 57285579 and +44(0)75 35994 132
s.musch@ai-and-partners.com and m.borrelli@ai-and-partners.com
https://www.ai-and-partners.com/
https://twitter.com/AI_and_Partners @AI_and_Partners
https://www.linkedin.com/company/ai-&-partners/

EU AI Act Compliance Risk Management Capability Maturity Model

1. Executive Summary

Everything businesses do to improve compliance is the result of a decision. Managing a business effectively is about making decisions related to risks and opportunities while the resources are scarce. Ultimately, decisions are the only way to have a purposeful influence on anything. Various decision-making processes will probably lead to different choices, and different choices will lead to different outcomes. If a business is able to identify and frame important decision situations related to compliance risks and opportunities and make the best combination of choices, compliance will probably increase. 'The purpose of applying Risk Management is to enable a business to accomplish its objectives(s) by facilitating management to make better decisions.' (European AI Scanner, 2023). This document advocates the importance of having key capabilities in place regarding the performance of EU AI Act CRM and the continuous improvement of such capabilities.

The EU AI Act CRM CMM (hereinafter referred to as 'EU AI Act CRM CMM' or 'the model') enables business to assess and understand their current CRM capability maturity levels, define what level they want to achieve, identify the gaps, set objectives, and identify and prioritize actions for key improvements, all with the aim of increasing business compliance and prevent non-compliance.

The EU AI Act CRM CMM presented in the Appendix consists of five themes (that correspond to the most important areas involved when performing an effective CRM) including 20 capabilities, each with five possible maturity levels that provide criteria against which businesses can assess their current maturity level and decide the desired maturity level. To avoid any subjective assessment and in order to effectively assess performance and progress, evidence for the business's current maturity level must be provided.

The EU AI Act CRM CMM mainly serves as a learning tool, a communication tool and a means to align thoughts to improve the CRM process. Discussions about risk management can be difficult because some concepts may be ambiguous. Therefore, a common language is important. The most important concepts are explained in the right margin and in the glossary of this document. The concepts have been formulated as they should be understood in the context of this document.

EU AI Act Compliance Risk Management Capability Maturity Model

The EU AI Act CRM CMM is built on both practical and theoretical ideas. The practical ideas are based on research analysed from compliance risk experts across the world. The theoretical ideas are based on academic literature describing important concepts and practices related to capabilities considered to be most important for performing CRM. The document contains a reference list of literature that has been used as source of inspiration for constructing the CRM CMM.

The guide explains why a strong commitment to CRM is important, what a CMM is, how the CRM CMM is constructed, how to use the EU AI Act CRM CMM, and, finally, describes the content of the CRM CMM. In the Appendix, all capabilities are described with maturity paths, including a set of questions to help use the EU AI Act CRM CMM.

EU AI Act – Advisory | Consultancy | Compliance Software
+31 6 57285579 and +44(0)75 35994 132
s.musch@ai-and-partners.com and m.borrelli@ai-and-partners.com
https://www.ai-and-partners.com/
https://twitter.com/AI_and_Partners @AI_and_Partners
https://www.linkedin.com/company/ai-&-partners/

EU AI Act Compliance Risk Management Capability Maturity Model

AI & Partners

2. Introduction

2.1 Why develop a Capability Maturity Model for Compliance Risk Management?

The Capability Maturity Model ("CMM") describes key capabilities that are needed to perform an effective Compliance Risk Management ("CRM") under the EU AI Act.

In the forthcoming months and years, many businesses are likely to start using the principles of risk management to improve the effectiveness of their limited resources to achieve the best possible level of regulatory compliance under the EU AI Act. The general objective of the EU AI Act CRM Platform is to assist all businesses in bringing compliance risk management under the EU AI Act to a higher level.

We intend for the EU AI Act CRM platform to provide businesses with a tool to assess the maturity of their EU AI Act CRM work or a systematic approach to set and pursue the desired maturity. The EU AI Act CRM CMM described in this document is created by AI & Partners for businesses to support them in their efforts to improve their EU AI Act CRM maturity.

The objective of the **EU AI Act CRM CMM** is to lead businesses to higher CRM maturity taking into account their objectives and available resources.

The EU AI Act CRM CMM can be used by businesses to:

- Assess their current maturity regarding CRM;
- Define the desired CRM maturity regarding their objectives and resources;
- Identify areas where they might want to focus their improvement efforts with the aim to achieve the desired CRM maturity; and
- Identify ways to improve.

Correctly used, the EU AI Act CRM CMM is expected to improve CRM capabilities in a systematic and consistent way. However, it cannot guarantee that each and every initiative will be successful. The EU AI Act CRM CMM mainly functions as a learning tool, a communication tool, and a means to align thoughts. The EU AI Act CRM CMM cannot be used properly without having a common understanding about key words and key concepts in CRM and CMM.

They must be accurately communicated and understood in the same way throughout the business. A common understanding of key words and key concepts is a precondition for developing the capabilities in a positive way. This guide explains, amongst other things, the key words and key concepts used in CRM and CMM.

The EU AI Act CRM CMM is not intended to be used as a source of comparison between businesses of various sectors. Indeed, businesses work under different conditions and circumstances .

Instead, the EU AI Act CRM CMM can serve to identify important areas of cooperation between businesses when identifying solutions on how to improve capabilities related to CRM. It is important to keep in mind that all businesses benefit if CRM maturity is raised in business dealings.

2.2 What is a capability?

We define capabilities related to CRM as the specific abilities, faculties or powers of a business that enable it to collectively deliver EU AI Act compliance objectives in the face of risks and opportunities.

Capabilities include, but are not limited to: processes, technologies, assets, people, decision-related behaviours, practices, attitudes, competencies, disciplines, and approaches used to achieve compliance objectives. Organisational capabilities can be related to both individual's competencies and organisational capacities.

For instance, the organisational capability to define, describe and explain risks and opportunities is related to the staff's competency in transforming statistical data into knowledge, the capacity of the database, the culture of sharing and receiving information from other governmental organisations, etc.

We can draw three important conclusions at this stage:

1. Capabilities that don´t contribute to achieve something important are not useful. Important capabilities for a business are those that support the values it really cares about. This applies regardless of whether it is about carrying out a process, a project, etc. Therefore, a business must prioritize and focus on the most important capabilities related to achieving an effective CRM.

2. Good capability performance assumes there are some basic elements in place characterizing and representing the capability. Therefore, the business must focus on the most important capabilities with its most prominent elements and to strengthen their consistency related to what is valued as important.

3. Capabilities must not be confused with capacity, which represents the maximum amount that can be produced or held by the organisation. For businesses: number of audits, size of operational staff, and number of employees trained and able to perform specific activities. Quality must also be taken into account. However, a high capacity is not worth much if it's not focused on the right capabilities.

2.3 What is a Capability Maturity Model?

The CMM is a tool to assess the maturity of organisations, processes, or systems. It describes the key capabilities and their development in a specified sequence (maturity level), which will be used as a base to assess the 'as is' and decide the desired 'to be' (but without skipping any levels).

The CRM CMM is not based on comparisons with 'best practices'. Businesses work under various conditions and circumstances and have different objectives. A business should focus on improving key capabilities required to achieve what it values as important.

The CRM CMM has a repeatable construct with content representing inputs (resources invested in accomplishing a task) and outputs (the accomplishment itself) leading to outcomes. Capabilities may include unused and undeveloped or still-developing abilities. The CRM CMM assesses how developed they are at any current point in time ('as is') or should be at a targeted moment of time ('to be').

In a CMM criteria have a specific meaning, namely they correspond to the decisive characteristics related to a capability with which one can determine the maturity level of that capability.

The predefined criteria consist of characteristics provided with indicators, positions or stages on a scale of quantity, extent, or quality related to that capability. These criteria should be supported by visible and verifiable evidence to prove that a certain maturity level has been reached.

Recording and keeping evidence accessible is important because:

1. It increases the validity of the assessment;

2. It increases confidence in the results; and

3. It remains accessible and reusable when re-assessing against the framework to identify improvements in maturity levels.

2.4 The Capability Maturity Model main features

1. The CRM CMM itself covers the most important capabilities needed to perform an effective CRM.

2. It is important that the CRM CMM does not recommend any compliance strategies or actions to stimulate compliance in particular.

3. The CRM CMM is not to be used to compare businesses or rankings between businesses. The CRM CMM can serve as an inspiration for cooperation and discussion with other businesses; for example, how to achieve higher maturity levels (improvement actions).

4. The structure of the maturity levels for each capability consists of a 1-5 scale, where 1 represents weak performance and 5 represents excellent performance.

5. Performance at the higher levels of maturity cannot be attained unless the key elements of the lower levels are in place and functioning well (for example, Level 4 includes the elements at Level 3, Level 2 and Level 1 plus additional ones for Level 4). In order to be at a certain level, the requirements of this level and all lower levels must be met.

6. Level 5 is not necessarily the right objective for all businesses or all capabilities. Level 3 or 4 might be quite adequate for most businesses. The effort required to reach and maintain the highest maturity levels for all capabilities may indeed be disproportionate to potential benefits. A business should aim for the maturity levels at which it can most effectively reach its EU AI Act compliance objectives.

7. Achieving a particular level is never acquired, as there is continuous change in a business's external environment and internal capacity. Therefore, constant effort and awareness is required to maintain performance at a particular level. At Level 5, continuous improvement has become a standard part of the business's culture.

8. It is advisable to use the results of the CRM CMM assessment as an input for other documents (strategy, annual plans, etc.).

9. It is recommended to periodically evaluate the business's maturity level, using the CRM CMM to ensure improvement in its chosen capabilities.

10. Remember that the concept of a capability is complex but nevertheless important to understand in order to improve. By reading the guide and Appendix that describes the capabilities, maturation paths, and help questions, the concept of a capability can be better understood.

3. Compliance Risk Management

3.1 Purpose of CRM

There are two major ways to effectively stimulate EU AI Act compliance or to prevent EU AI Act non-compliance. The first is to decide which external opportunities could be used, and the second is to decide which compliance risks to treat and how. Because businesses have scarce resources, they must prioritize and focus efforts on these only, letting other risks and opportunities pass by.

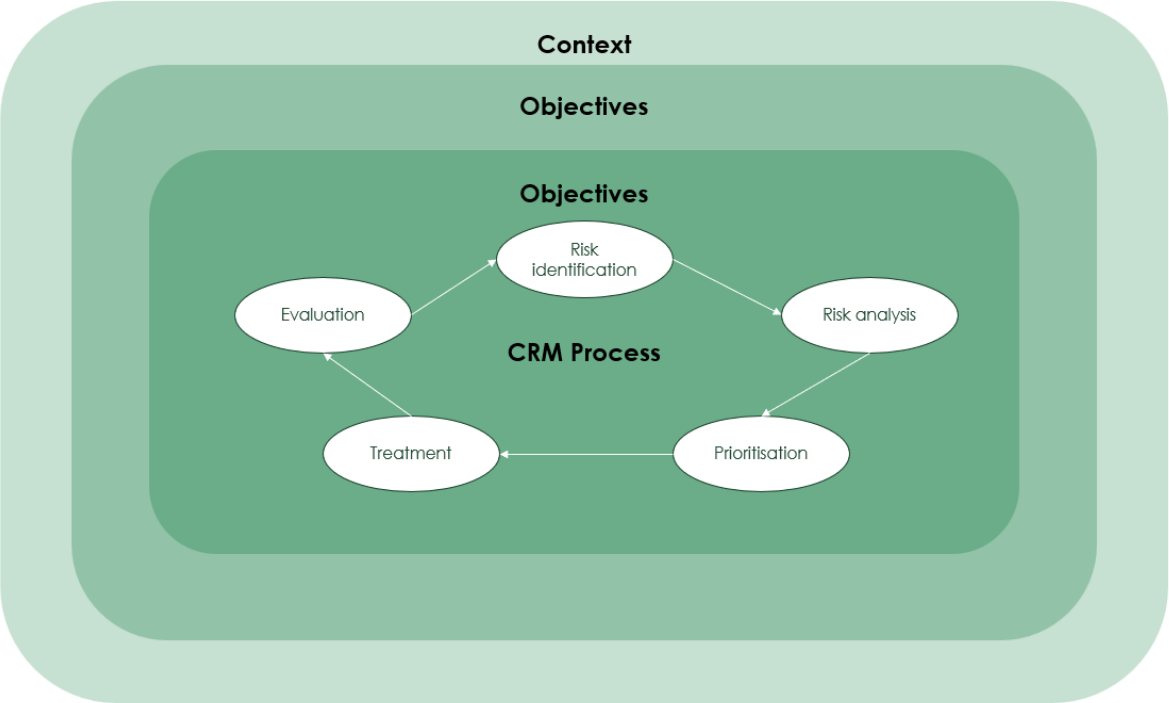
Compliance Risk Management ("CRM") is 'a systematic process in which a business makes substantiated choices about which treatment instruments could be used to effectively stimulate compliance and prevent non-compliance, based on the knowledge of the behaviour of all businesses and related to the available resources and capacity' (European AI Scanner, 2023). So, in the end, CRM is about making the right decisions concerning compliance risks and opportunities with a focus on what will probably have the most influence on or be the most beneficial to the achievement of the compliance objectives. The Compliance Risk Management Model shows the steps in the Compliance Risk Management Process:

- Identification
- risk analysis
- prioritization
- action
- evaluation

Set in context, compliance objectives and strategies. The CRM process helps to identify the different steps in the decision making cycle, and allows businesses to make explicit and more well-informed decisions in each stage of the process before moving on to the next one. Central to the CRM process is the context which can be defined as the environments in which the business operates.

Compliance objectives describe what to achieve and the compliance strategies serve as a general guide on how to reach compliance objectives taking into account the external context (see **Figure 1**).

Figure 1: The Compliance Risk Management Model



3.2 Compliance objectives and compliance strategies

Compliance is the willingness of business to fulfil their regulatory obligations under the EU AI Act.

Compliance objectives describe the desired outcome and what must be achieved at any business unit within a business in order to promote compliance amongst businesses. These objectives also have an impact on risk assessment included how risks are formulated and addressed. Overall, every decision that is made in the CRM process must take the compliance objectives into account.

When using the EU AI Act CRM CMM, it is expected that robust compliance objectives are already in place. In other words, there are no capabilities in the EU AI Act CRM CMM regarding the formulation of compliance objectives.

However, to use the EU AI Act CRM CMM, it is important to know the concept of compliance and understand the compliance objectives since the compliance objectives are the starting point for performing CRM. Compliance risks are the threat or probability that an action or event will adversely affect the business's ability to achieve its compliance objectives. Similarly, the business must know and understand its compliance objectives in order to recognize opportunities and benefit from them. If there are difficulties in understanding compliance objectives, that may lead to decisions that are not in the business's best interests.

The above reflects and explains the relationship between compliance objectives and the CRM process, which is a tool to achieve these objectives. As mentioned above, the steps in the CRM process should revolve around compliance objectives.

The identification of risks must start with high-level compliance objectives (improve compliance) and be divided into more specific compliance objectives on lower levels (for example a specific risk related to new AI system not being subject to post-market monitoring).

Examples of high-level compliance objectives are:

- Increase the level of compliance amongst businesses;
- Increase compliance regarding registering of high-risk artificial intelligence systems;
- Increase confidence and improve reputation in a business; and
- Minimize reporting errors.

The level and formulation of compliance objectives determine how a business will formulate its compliance strategies. The CRM approach can be seen as a main tool in a business's compliance strategies to achieve compliance objectives. The capability to formulate and implement compliance strategies, as a way to achieve compliance objectives, will, therefore, be part of the CRM CMM (see **Section 6.2.1**)

4. Overview of the Capability Maturity Model

4.1 Construction of the model

The EU AI Act CRM CMM presented in Appendix of this document consists of five components.

1. **Themes**: each theme groups a number of related capabilities;
2. **Capabilities**: each capability is clarified by a name and a short description;
3. The 5 levels of **maturity**;
4. Criteria of each level of **maturity** for each capability;
5. Questions that help the user of the model to assess the current **state**, the 'as is' and to decide the desired level 'to be'.

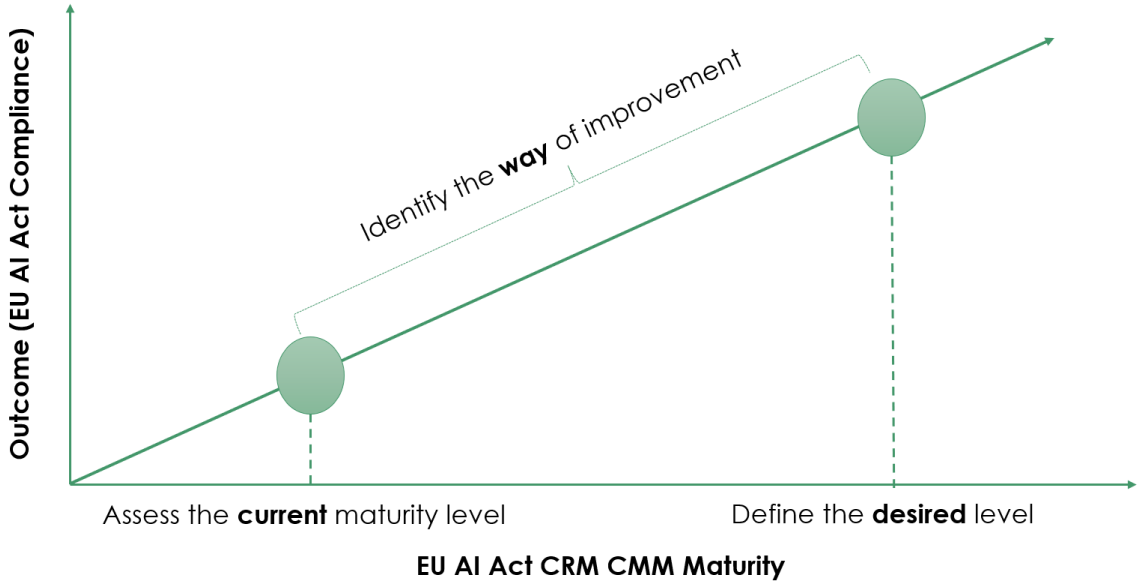
Figure 2: The components of the EU AI Act CRM CMM

Themes	Capabilities	Level 1	Level 2	Level 3	Level 4	Level 5
Strategy	Formulating compliance strategies					
	Implementing compliance strategies					
Knowledge of external context	Differentiating firms					
	Forecasting the future					
	Knowing reasons for firm's compliance/non-compliance					
	Knowing methods of influence					
Decision making	Defining, describing and explaining risks and opportunities					
	Generating alternatives					
	Making decisions					
	Implementing decisions					
Organisation	Leadership					
	Risk culture					
	Organisational culture					
	Acquiring and developing competencies					
	Managing knowledge					
	Fostering creativity and innovation					
	Communication					
	Extracting, managing and ensuring data					
Evaluation	Evaluating the outcome of actions to stimulate compliance					
	Evaluating the CRM process					

4.2 Outcome of using the model

The objective of the model is to support the improvement of CRM. Given that the model is correctly constructed and used, the probability that the CRM process will have a better outcome (higher EU AI Act compliance), will increase.

Figure 3: Major steps in using the model



The assessment of current maturity levels, followed by defining desired maturity levels will result in 'gaps' that reflect the difference between the current state, the 'as is', and the desired state, the 'to be'. An analysis of the gaps should result in an improvement plan with the aim to overcome the gaps and achieve higher levels of maturity.

Improving capabilities relevant to CRM means increased CRM maturity which in turn is assumed to contribute to an increased probability of higher compliance amongst businesses. Higher compliance amongst businesses is also supposed to be achieved efficiently, that is: through fewer resources and less effort.

4.3 Capability descriptions

The description of a capability consists of three parts.

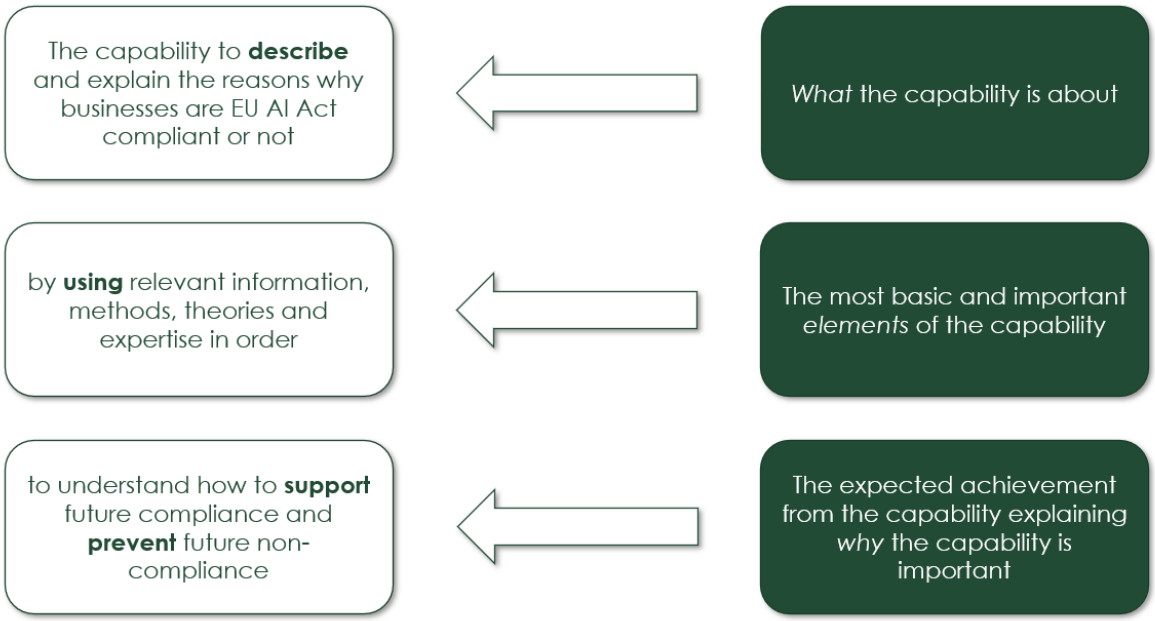
First, the description frames and describes what the capability is.

Secondly the description lists the most basic and important elements for performing the capability like processes, actions, methods, tools, techniques, competencies, etc. (see **Section 2.2**). In the description of maturation paths these elements correspond to 'evidence of quality or completion' expressed as criteria to be used to decide the level of maturity (as is).

Finally, the description expresses the expected achievement from the capability or the why the capability is regarded as important.

The description of the 'why' indicates how the capability connects to compliance objectives or how the capability supports other capabilities with the common purpose of achieving compliance objectives.

Figure 4: Three parts describing a capability using its description



The three parts reflect and support the EU AI Act's CRM CMM's internal and external validity. This means, for example, that the what must be consistent with performing an effective CRM. The more the capabilities are consistent with performing an effective CRM, the higher the external validity. Furthermore, the more unambiguous and functional the elements are to achieve the why, the higher the internal validity is.

The words 'relevance' and 'relevant' are often used in the descriptions of capabilities and maturation paths to stress the importance of consistency between different parts of the EU AI Act CRM CMM (internal validity) and the consistency between the CRM CMM and to perform an effective CRM (external validity). 'Relevant' stands for: significant, important and sufficient to support the cause in question. 'Relevance' is one of several indicators significant for maturity.

Fundamental for the EU AI Act CRM CMM is that high maturity can occur only when capabilities with their most important elements, are consistent with an effective CRM and in the end consistent with the compliance objectives.

4.4 Defined levels of maturity

The assessment scale for measuring the maturity of each capability consists of five levels as follows:

Level 1 – Emerging

This level reflects an immature, undeveloped state. Things happen ad hoc or do not happen at all. There is little or no awareness about the capabilities, their importance, and their relation to CRM.

Level 2 – Evolving

The businesses and its employees begin to be aware about the capabilities and their relation to CRM, although with limited understanding. Action mostly begins on an intuitive basis.

Level 3 – Enhancing

At this level, things evolve to higher levels of formalization, although remaining partial (irregular). The awareness and understanding of the capabilities' importance, how to perform them, and their relation with CRM are clear but still incomplete.

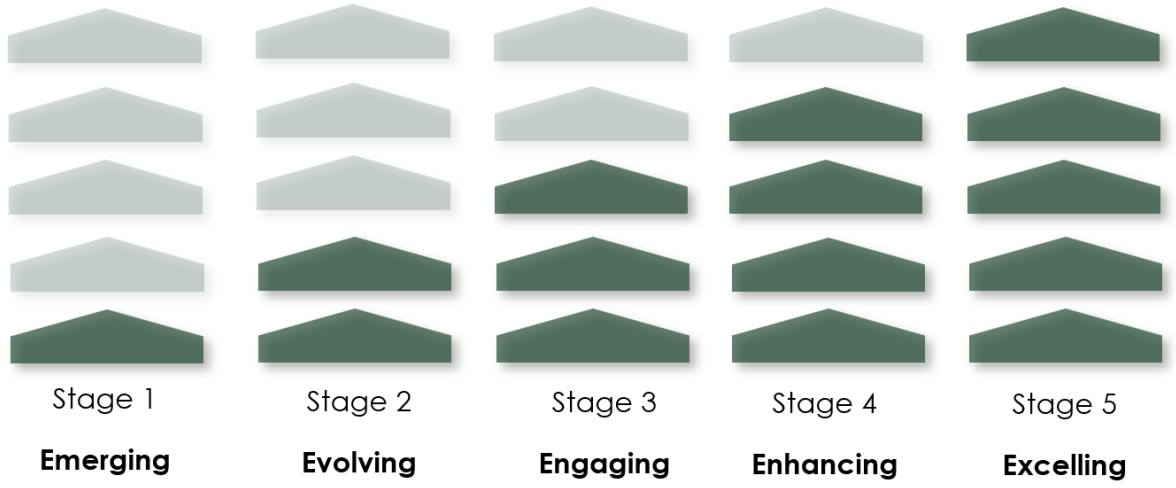
Level 4 – Enhancing

Awareness is widespread throughout the business; internal processes, etc. are documented and employees are reaching high levels of consciousness, understanding, and practice of the capabilities. Organisation, formalization and systematization are total or almost total with a focus on monitoring and reviewing processes, practices, and competencies.

Level 5 – Excelling

The highest level of maturity according to state-of-the-art CRM. The focus is on continuous improvement of the capabilities and is achieved through a proactive attitude and actions by the organisation and its employees.

Figure 5: Three parts describing a capability using the description of the capability



Awareness means that the employees involved in the capability, perceive the fact that the capability is important and that they have some ideas of why these specific characteristics are representing the capability. Understanding involves awareness about why the capability is important and what it intends to achieve included an understanding of how the characteristics reflecting the most important elements of the capability will transform an input to an output.

Consciousness is a higher quality of understanding, as understanding is a higher quality of awareness. Awareness and understanding are necessary conditions for consciousness. To be conscious, one must have a complete understanding of the capability, including the understanding of how the capability relates to other capabilities and how they support each other when performing CRM. In short, an understanding of a capability's importance and the way to perform it creates better conditions than only awareness, and consciousness creates better conditions than understanding.

Level 4 is characterized by formalization, amongst others. That means, for example, that the internal processes are documented to secure that work is always performed in the same way regardless the employees. Processes must be organisational, not personal.

At Level 5, a business not only has consciousness but also a proactive attitude, which means that the employees involved are prepared to adjust pro-actively rather than just try to make improvements because of events that have already occurred. One way to constantly improve is to interact with external experts and sources like universities, businesses in other countries or to be inspired by various certification tools. A proactive attitude requires awareness, understanding, and consciousness. For Level 5 in particular, a critical dimension is time – external factors (political, economic, technological and others) and internal factors (strategy, employee's qualifications, competencies and experience and others) change with time. What is considered to be important at a particular level at a particular period in time can be considered as more or less important at another period.

The completion of the capabilities most important elements will be assessed in a sliding scale with the help of terms such as 'not at all', 'ad hoc', 'intuitive', and 'exist' (activities, processes etc. are in place). 'Ad hoc' means that something is done for a special and immediate purpose or for a weak purpose without previous planning. 'Intuitive' means that something is done on the basis of personal experiences, feelings or beliefs, not on the basis of proven best practices, scientific findings, or other objective arguments.

Level 3 and higher requires that analyses are executed in an increasingly methodical and thoroughgoing way. An important aspect is that in ad hoc and intuitive decision-making, in comparison with decisions based on analytic procedures, it is difficult to know what one has actually learned from making a decision. A transparent procedure when analysing and making decisions is by far preferable.

The more in-depth analysis proving that the capabilities' elements connect with what is to be achieved, the higher the maturity is. A higher degree of relevance is assumed by having documented arguments (from Level 4) connecting the capabilities' elements with what is to be achieved.

Monitoring is a form of observation that takes place to ensure actions, processes etc. controlling that everything goes as planned. Reviewing should be seen as an account of the strengths and weaknesses or what is positive or negative regarding the relationship between the performance and what is to be achieved.

Nothing is perfect and there is always room for improvement. Continuous improvement is about an ongoing, proactive series of improvements, related to the prominent elements of a capability through constant monitoring and reviewing. To improve, the business has to change. These can be small changes or large scale changes. The latter aim at breaking established paradigms of how to think and act into new ones.

4.5 Maturity path description

The maturity path description for a capability explains what criteria must be fulfilled to achieve a certain maturity level. Levels for all capabilities are based on the same principles (see **Section 4.4**), but the content is adjusted to each specific capability.

The maturity paths follow a progression starting with uncertainty at the lowest level. Through awareness, understanding, and consciousness, a business can achieve its objectives more effectively. Monitoring, reviewing, learning, innovating, and maintaining an overall proactive attitude will lead to continuous improvement. To strengthen each capability, the consistency between the capabilities' important elements and why to perform it (what to achieve) is an important key to progress.

5. How to use the model

5.1 Some general points

As the maturity assessment covers a wide range of knowledge of CRM and other organisational themes, it is recommended, but not a requirement, for evaluators:

- To have at least 2-3 years of experience in CRM;
- To consult with experts if there is a lack of knowledge about a specific capability;
- To involve senior level management during the assessment as well as in discussion about results; and
- To internally agree on concepts. A common language is an absolute prerequisite for being able to use the CRM CMM effectively.

When a business defines a desired maturity level – the 'to be', it must keep in mind that the objective is not to achieve the highest maturity level in all capabilities. That objective entails a huge expense, as it might require changing significant elements in the current situation. It also might be inappropriate, especially when the objectives can be met with a lower level of maturity. However, the business must always keep in mind that deciding to improve one capability may cause the business to improve one or more capabilities that are interdependent with the initial one. In summary, by deciding on changes, the business must consider both the costs of these changes and the probability that they will lead to a significant improvement.

After the EU AI Act CRM CMM assessment, the results needs to be shared with the employees who have been a part of the assessment. Also, the application of a CMM is not a one-off exercise. It is important to measure progress repeatedly while moving towards the 'to be' state. The gaps may be used as a feedback mechanism for analysis and thoughts on improvement. Reapplying the EU AI Act CRM CMM provides an indication that capabilities are heading in the right direction.

5.2 The 'as is' (where are you) assessment

A business carries out the 'as is' assessment using the themes and capabilities in the EU AI Act CRM CMM to evaluate itself.

We recommend the assessment process to be as follows:

1. Choose a theme;

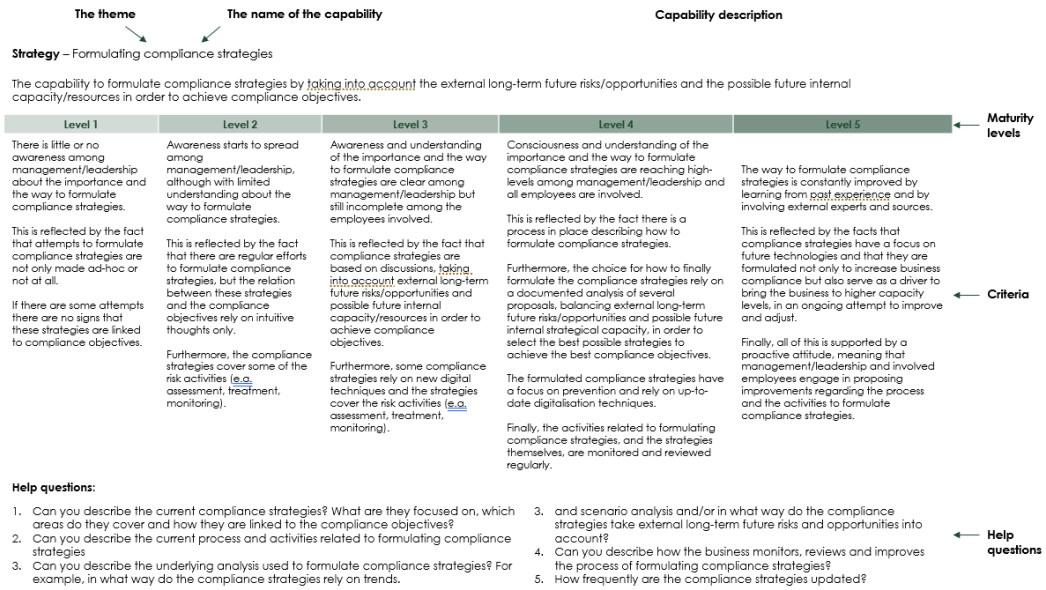
2. Start with the first capability;

3. Be sure to understand the essence of the capability description (see **Section 4.3**) and how the capability relates to other themes/capabilities (see **Section 6.1**);

4. To agree on the most basic things, discuss the help-questions concerning the capability. After that, read the criteria for each maturity level.

5. Follow the process for all capabilities in all themes.

Figure 6: Different parts constituting the EU AI Act CRM CMM



EU AI Act Compliance Risk Management Capability Maturity Model

AI & Partners

It is crucial to have an idea of awareness, understanding and consciousness regarding the capability. The degree of awareness, understanding, and consciousness of the importance of the capability and the way to perform it should, therefore, be assessed first. The maturity cannot be at a higher level than the level of organisational awareness, understanding, and consciousness. The more awareness, understanding, and consciousness there is, the better the conditions to perform the capability with high maturity. The next step is to assess the presence and quality of activities, processes, competencies etc. expressed by the criteria.

From Level 2, the performance must be judged against the examined level plus the previous level(s). The next level can be reached only if all previous levels have been achieved. It is important that the assessment of each capability is carried out using the most objective arguments and facts, avoiding subjective interpretations as much as possible.

The following steps should be considered when businesses determine the current state for each capability in the EU AI Act CRM CMM:

- Collect evidence as support to identify the current level. Evidence should be collected from the business's operations and documents and across various levels of employees and management in order to get a comprehensive picture. Engagement with senior level management is advisable as is incorporating their knowledge in the assessment stage and obtaining their agreement; and

- Select the level of maturity that best reflects the current state in relation to each capability based on the evidence gathered.

This means that when the business achieves a level where it becomes increasingly difficult to provide the evidence, it indicates that the maturity level for the business must be situated at the previous level.

In summary, the business must weigh, on one side, all known and relevant facts serving as evidence and, on the other side, the criteria for each maturity level. Although gathered evidence should avoid subjective interpretations as much as possible, this is not an exact science – it cannot be done with complete accuracy. The most important thing is to find a maturity level that all those involved can agree upon.

EU AI Act – Advisory | Consultancy | Compliance Software
+31 6 57285579 and +44(0)75 35994 132
s.musch@ai-and-partners.com and m.borrelli@ai-and-partners.com
https://www.ai-and-partners.com/
https://twitter.com/AI_and_Partners @AI_and_Partners
https://www.linkedin.com/company/ai-&-partners/

5.3 The 'to be' (where you want to be) decision

The determination of the current CRM maturity (the 'as is') is not the only purpose of the EU AI Act CRM CMM. It is equally essential to define the desired CRM maturity, the 'to be'. Unlike to decide the 'as is', which is an aggregate assessment of facts from different dimensions, the 'to be' is to decide what the business ought to be. This is a normative judgment. That is, it cannot be deduced from facts.

It should be noted that if the current situation of one or more capabilities is adequate for a business, the desired maturity level may coincide with the current maturity level. It is also important to note that it is not necessary, nor even recommended, to set as an objective to reach the highest, fifth maturity level. Often this will require an excessive amount of resources (financial, human resources, etc.) compared to the possible outcome and, therefore, be an inefficient objective. Furthermore, the key feature of maturity Level 5 is continuous improvement. Because the use of the EU AI Act CRM CMM is dynamic and ongoing, what is considered to be at Level 5 (or any other level for that matter) at a certain moment in time probably may not be at that level in the future, given that reality changes continuously.

The following should be considered when a business determines the 'to be':

- Engagement with senior level management is advisable as is incorporating their knowledge in the assessment when defining the 'to be' decision; and

- The decision must be made having in mind whether the desired situation can be achieved at a justifiable effort and cost (see next Section).

5.4 Deciding how to get to the level you want

Once the business has completed a broad assessment on the 'as is' and 'to be', it should aim to identify the capabilities most in need of improvement and then lay out a roadmap for working towards these improvements. In order to achieve the desired maturity level for a capability, the business must meet the requirements and conditions described at the appropriate maturity level in the EU AI Act CRM CMM. The decision on how to get to the level you want should be made using the EU AI Act CRM CMM and its help questions and by reading the detailed descriptions of capabilities in Section 6.2.

By discussing and answering the help-questions and by considering criteria that are in the gap between the 'to be' and 'as is', this will generate suggestions on how to reach the desired maturity level and overcome a current maturity gap.

It is advisable to make a plan of what needs to be done to reach the desired maturity level, by whom, how and when. To be able to reach the desired maturity level, it is advisable to approve only such levels for which a realistic time frame and responsibilities have been defined.

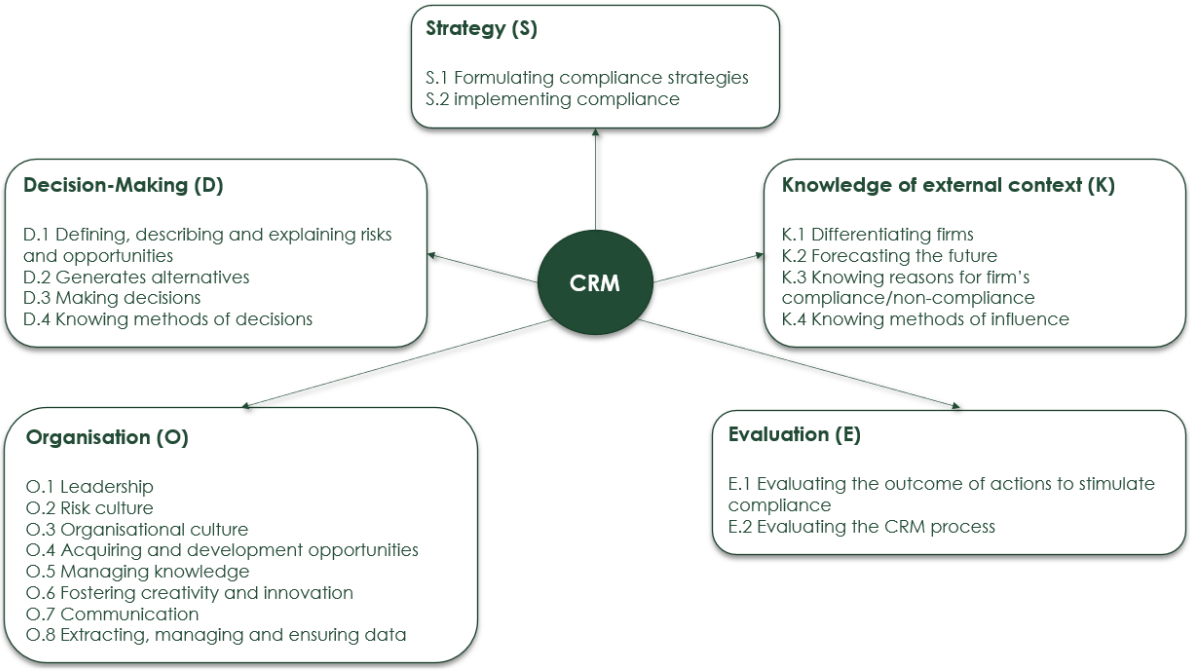
By using the EU AI Act CRM CMM, a business will, over time, gain more and more experience with the capabilities and their interconnections. The more experience a business gains by using the EU AI Act CRM CMM, the more advanced it will be in understanding how to orchestrate improvements of capabilities. It will know how to best coordinate improvements, conscious of the idea that the whole is more than the sum of its parts.

6. Themes and capabilities

The EU AI Act CRM CMM is built upon five themes and each theme consists of several capabilities related to CRM. The themes that correspond to the most important areas to perform an effective CRM are:

- Strategy
- Knowledge of external context
- Decision making
- Organisation
- Evaluation

Figure 7: The five themes and capabilities



The themes group the most important capabilities needed to perform CRM effectively. Deciding to improve one capability can result in the need to improve another capability as well. Therefore, it is important to know how the themes and the capabilities are interconnected and how an improvement in one capability can trigger a consequence or a need to define an action in another capability. Section 6.1 will give a brief explanation of the themes and how the capabilities relate to each other.

Section 6.2 will give a more detailed description of the respective themes and their capabilities. Amongst others the descriptions will give a deeper understanding of important concepts, the most prominent elements of the capabilities and the expected achievement from the capability.

AI & Partners

6.1 How the themes and the capabilities connect

Since the capabilities are interconnected, they do not follow a strict sequence, that is, the EU AI Act CRM CMM has no start or end points. But, for the sake of explaining, we will start with the theme 'Strategy'.

Formulating compliance strategies (C1) relates to how to achieve compliance objectives in general. When formulating strategies, it is important to consider the most important long-term future external risks and opportunities and simultaneously consider internal capacity and resources. If the resources available when formulating the compliance strategies are deemed insufficient to meet the desired objectives and if the business wants to maintain these objectives nevertheless, the compliance strategies should comprise of a plan to address shortages. To formulate compliance strategies is, amongst others, dependent on the capability to forecast the future developments (C4).

Furthermore, compliance strategies are of no use if they are not implemented properly (C2). Therefore, employees must be involved in compliance strategies that, in turn, require their acceptance and understanding of the compliance strategies. Inter alia, the risk culture must be aligned (C12) with the values expressed by the compliance objectives and strategies. Here, communication (C17) will play an essential role.

Whether it is formulating compliance strategies (C1) or considering actions to stimulate compliance or to make benefit of opportunities supporting the compliance strategies, a business will need information and knowledge. The ability: to differentiate businesses in risk areas (C3), to forecast the future (C4), to know the reasons why businesses are compliant or not (C5), to know how to influence business behaviour (C6), and to have access to data (C18) are important capabilities that provide relevant information and knowledge. In order to benefit from all the knowledge created through the CRM process, a business must have a systematic process for managing knowledge, supported by technical tools (C15).

When deciding on compliance strategies or on actions supporting the strategies, the decisions should be based on reasoning (C9). Rationality imposes the utmost use of available knowledge and information (C3-C6, C18) while considering risks and uncertainties.

To be a rational decision maker means to start from defined risks and opportunities (C7) and to have relevant alternatives to choose from on how to treat risks and how to make use of opportunities (C8). A decision not well implemented (C10), the intended effects will not be achieved.

Furthermore, all the above must be supported by organisational capabilities: besides already mentioned risk culture (C12), managing knowledge (C15), communication (C17) and data (C18) there must be a capability to train, promote and support a leadership style in order to provide the right conditions for employees involved to perform an effective CRM (C11); to have an organisational structure promoting an effective CRM process that defines teams, functions, responsibilities, and relationships in a complementary way (C13); the capability to recruit, retain, educate, and train a sufficient number of employees so that they possess the necessary competencies performing the CRM process (C14); and, the capability to foster the creativity and innovation that is needed in several parts of the CRM process (C16).

Finally, performing relevant evaluations of the outcomes of actions to stimulate compliance and of the CRM process itself (C19, C20) will contribute to learning and understanding of how to better formulate compliance strategies (C1) and to make decisions on compliance strategies and the actions needed to support them (C9).

6.2 Descriptions of the themes

6.2.1 Strategy (S)

Regarding CRM, a compliance strategy can be described as a general guide to reach compliance objectives. The compliance objectives describe what to achieve and the compliance strategies describe how to achieve them. Furthermore, actions are the way strategies make objectives happen. Compliance strategies provide lead-time for planning responses on risks and opportunities. Choices on compliances strategies are therefore concerned with the perfect match between the business and its external context. A business can have the best possible compliance strategies; however, if not implemented well, they are not worth much. These major elements form the basis for the capabilities: Formulating compliance strategies and Implementing compliance strategies.

Formulating compliance strategies (S1)

Formulating compliance strategies can be seen as a process that seeks to discover and invent new courses of action. Compliance strategies are methods that guide actions for the long run to avoid risks and take benefit of opportunities. However, compliance strategies also incorporate principles for ways of thinking to guide all employees in various situations. Compliance strategies should reflect a good balance between selected external long-term future risks/opportunities and available internal capacity and resources in order to achieve the set of compliance objectives. If no compliance strategy exists, the business will probably 'tend to stumble from one problem to another'. What really matters is the formulation of a strategy that evidently contributes to compliance objectives.

When formulating compliance strategies, there must be knowledge and understanding about future development built on strategical analyses such as trend analysis and/or scenario analysis. To consider the future is to deal with uncertainty which amongst other means that compliance strategies must be developed before that full scientific information is available. By searching for and considering several options of compliance strategies to choose from the probability for success will increase. Discussion on how and why compliance strategies will contribute to the achievement of the compliance objectives are to be considered as proof of a higher maturity in performing the capability.

Implementing compliance strategies (S2)

Implementation of compliance strategies is about how to put a chosen strategy into action. To do that three elements are required: the employees' involvement by gaining their understanding and acceptance of the compliance strategies. Involvement means that employees contribute to the fulfillment of compliance strategies through actions, discussions, setting objectives, and ways of thinking. Understanding concerns employee knowledge about how compliance strategies are linked to achieving compliance objectives. Acceptance occurs when employees share the beliefs and values that the compliance strategies are built on. Having discussions about how and why the implementation of the compliance strategies will lead to the achievement of compliance objectives is an important criterion when evaluating the capability.

6.2.2 Knowledge of external context (K)

Having knowledge about external context is probably the most crucial issue when performing CRM. Knowledge can be defined as the necessary understanding an organisation possesses to make decisions about strategies and actions supporting those strategies. Knowledge about the most important external short- and long-term compliance risks and opportunities, knowledge about how to understand business behaviour, and knowledge about how to influence business behaviour is the foundation for making good decisions about how to effectively stimulate compliance and prevent non-compliance. Lack of knowledge can lead to wrong actions on wrong compliances risks and/or on wrong opportunities. Sometimes we are inclined to believe that all kinds of knowledge are useful and the more, the better. However, knowing more does not guarantee that we understand better. Knowledge must always be relevant to performing an effective CRM. The acquisition of knowledge is therefore a matter of being able to prioritize. Deciding to provide new knowledge must relate to the benefits it is supposed to bring. Knowledge associated to human behaviour can be divided into four types: describing reality (what is happening, by whom and how), explaining why things happen, predicting the future (what will probably happen), and knowing how to define actions with the aim to change behaviour. This subdivision forms the basis of four capabilities: Differentiating businesses, Forecasting the future, Knowing the reasons why businesses are compliant or not and Knowing how to influence business.

Differentiating businesses (K1)

Differentiating businesses, addresses a business's important needs (for example: guidance and need of information) and compliance risks. It is not possible to describe each individual business. To be useful and understandable, the business must reduce the knowledge of businesses to relevant categories. Differentiation is a collective term for segmentation and profiling. Segmentation is the process of dividing businesses into groups and sub-groups with similar characteristics. A profile is a representation of an individual or a group of business; a profile can be, for example, a detailed description or a set of correlated data. The differentiation is a prerequisite to define the most important risks and opportunities and/or in the end to generate ideas about new compliance strategies and actions supporting the strategies. To differentiate businesses, the business will require different methods.

Having arguments for how and why activities differentiating businesses will help to address a business´s needs and compliance risks, is an important criterion when evaluating the capability.

Forecasting the future (K2)

By forecasting the future, the business should address the most important short- and long-term compliance risks and opportunities to formulate compliance strategies. Forecasting refers to the practice of predicting what will happen in the future by taking into consideration events in the past and present. Forecasting the future probably requires a business intelligence tool that is able to scan the external environment and conduct analysis built on both external and internal datasets related to econometrics, big data, statistics, etc. The analyses can be used to identify societal trends that in turn can be used to identify risks and opportunities. Scenarios are descriptions of possible future developments where important but uncertain trends often are used as a starting point. Having arguments on how and why the forecasting activities will serve to formulate compliance strategies is proof of higher maturity in performing the capability.

Knowing the reasons for firm's compliance/non-compliance (K3)

Knowing the reasons why businesses are compliant or not is a prerequisite to understand how to support future compliance and prevent future non-compliance. If the root of the problem is not identified, then one is inclined to address the symptoms and the problem will continue to exist.

Knowing methods of influence (K4)

By knowing how to influence business behaviour, the business is able to create alternatives for how to treat risks and make use of opportunities in various situations. Social psychology examines how people affect one another's thoughts, feelings, and behaviours. For example, situational forces, social roles, and social norms have a strong influence on human behaviour. Influencing business behaviour is also part of the field of regulatory compliance, which has generated several theories. These theories can help when trying to influence businesses in general and serve as a starting point in learning how to influence businesses by proactive and/or reactive methods in special situations. Discussing how and why knowledge about influencing business behaviour will serve to provide effective ways for stimulating compliance is considered as a sign of quality performance of the capability.

6.2.3 Evaluation (E)

Related to CRM, performance evaluation is the way to learn and understand how to make better decisions in the future to effectively stimulate compliance and prevent non-compliance. Besides, that it is not possible to know what would have happened if the business had decided differently two important questions arise: Have the best possible actions been chosen to stimulate compliance?; Is the CRM process organised in the best possible way to guarantee the best possible decision making?

There are two ways to answer these questions: one is to make an outcome measurement for one or more actions to verify if the intended outcome has been achieved, and the second is to evaluate the CRM process to verify if decisions have been made in an optimal way. When deciding whether to perform an outcome evaluation of actions or to perform an evaluation of the CRM process, a business must consider the fact that its resources are limited, both quantitatively and qualitatively. The business must therefore select which evaluations to perform, considering: 1) the costs performing the evaluation, 2) how robustly the causal link between the outcome and the method used must be, and 3) how certain the probability will be that the evaluation will yield useful information that will contribute to learning and understanding in how to make better decisions in the future. In other words, the evaluations must be relevant so that the results of the evaluation will influence future decisions. Having a process in place, including criteria for how to choose can be an effective way to prioritize the most important evaluations.

Both an outcome evaluation of actions and an evaluation of the CRM process require standardized processes describing how to perform such evaluations and providing practical guidance. The process always starts with an evaluation plan and ends with the understanding of and acting upon the results. Another important step in this process of performing evaluations is to choose the most adequate evaluation method as a way to establish if the action or the CRM process has led to the desired outcome.

Various methods exist based on how robustly the causal link between the outcome and the action must be. Many are internationally recognized methods and/or are based on published scientific articles. A business can also develop its own methods or adapt existing methods to suit its own purpose. But regardless of the origin of the method, the method chosen must always be validated: the business must establish beforehand that the method will indeed measure what it is intended to measure.

The two ways of evaluation, form the basis for two capabilities: Evaluating the outcome of actions to stimulate compliance and Evaluating the CRM process.

Evaluating the outcome of actions to stimulate compliance (E1)

An outcome evaluation focuses on whether the intended outcome (be it a single action or several actions) has been achieved or not. The result of the outcome evaluation of an action will be an indicator for whether the right choice regarding the treatment of a risk has been made or not. Having arguments for how and why the chosen evaluation, with its method, will serve as a way to learn and understand how to make better decisions in the future to effectively stimulate compliance and prevent non-compliance will be considered as proof of a high maturity in performing evaluations.

Evaluating the CRM process (E2)

A process evaluation focuses on the implementation and the effectiveness of the CRM process, or parts of it, and attempts to determine how successful the CRM process is in delivering good decisions. Process evaluations also allow making the important distinction between implementation failure and theory failure. Implementation failure is the lack of expected results due to poor implementation of the action. To be effective is to do the right things typically associated with the extent to which improved outcomes are being achieved.

Theory failure occurs when the action, although correctly implemented, fails to deliver the expected outcome, meaning that the theory upon which the activity was based was incorrect. To be efficient is to reduce the use of resources to produce a given level of outputs regardless if the job is the right one to be done or not. Having arguments for how and why the chosen evaluation, with its method, will serve as a way to learn and understand how to make better decisions in the future to effectively stimulate compliance and prevent non-compliance will be considered as proof of a high maturity in performing evaluations.

6.2.4 Organisation (O)

When performing an effective CRM, allocation of human and other resources must be made accordingly to the selected risks and opportunities and not the other way around. Compliance strategies and treatment actions should not be based on the current availability of staff included their competences. Compliance strategies should be based on prioritized risks and knowledge, and the allocation of staff and its competencies will need to adapt to this over the course of time. As prerequisites, the business's leadership, promoted by the management, must serve as a driver of the central aspects of CRM and the risk culture must be aligned with the values expressed by the compliance objectives, compliances strategies, policies, etc. Employees must have the required competencies to perform CRM work. Furthermore, the organisational structure and the leadership must support CRM work, creativity and innovation must be promoted, and knowledge must be managed in a proper way. A business must also be able to communicate all CRM related issues internally. And finally, a business must have the capability to extract, manage, and ensure available and relevant data from various internal and external original sources. All these capabilities adhere to the theme of organisation. In summary there are eight capabilities related to 'Organisation'; they are all required to ensure an effective CRM process in a business.

Leadership (O1)

Leadership as a capability should, in this context, be understood as the ability to motivate employees to perform an effective CRM work by focusing on the most central aspects of CRM. Studies indicate that leadership and effective strategies are positively related and that leadership is the driver of organisational culture.

To have a leadership capable of stimulating an effective CRM process, the management needs to define how leadership serves as the driver of the central aspects of CRM, such as achieving the desired risk culture, formulating and implementing compliance strategies, developing and nurturing CRM competences, promoting creativity and innovation, managing digital activities related to CRM, and controlling CRM performances in general. Having descriptions of how to train, promote and support a leadership style in order to provide the right conditions for employees involved to perform an effective CRM work are considered as proof of higher maturity in performing the capability.

AI & Partners

Risk culture (O2)

Risk culture is the system of values and behaviour present in a business that will shape decision making. What the business values as important will influence what to consider a risk and which treatment to choose. However, the employees' ideas, ways of behaving and communicating must be aligned to the values. To achieve the desired risk culture, that is that employees behave and communicate in line with the values expressed by the compliance objectives and strategies, the business must have good communication and education programs. A common language used throughout the organisation should be part of this. This is especially true when it comes to value-laden concepts or words, and an important pre-condition is that the business has already clearly expressed its values. These values will evoke expectations from the desired risk culture.

Having descriptions about how and why communication and education activities will help align employee behaviour with the desired risk culture is an important criterion when evaluating the capability.

Organisational culture (O3)

Organisational structure has an impact on organisational performance. CRM organisational structure can be defined as the division of work among employees in a business and the coordination of activities related to CRM. To have an appropriate organisational structure, a business should define and structure teams, functions, responsibilities and relations in a complementary way that all support effective CRM work. Structuring will depend on individual business specifics. However, it always seems important to define clearly roles and responsibilities and to clarify the relations between the functions.

Furthermore, it is important that employees behave in ways consistent with professional role expectations. Having descriptions about how and why the chosen CRM organisational structure was made to promote the CRM process is considered as a sign of quality performance of the capability.

AI & Partners

Acquiring and development opportunities (O4)

To have employees with the required competencies to perform CRM work, the business must recruit, retain, educate, and train employees so that they can perform an effective CRM. To begin with, employees must understand the business's compliance objectives and strategies. Involved employees also must understand the essence of CRM, ensuring that the business 'does the right thing'. To have a strong risk culture, employees need training to understand CRM and in the end, how to make educated risk-related decisions. Important fields of knowledge relevant for education can be the theoretical fields of. Having descriptions about how and why recruitment, education, and training will contribute to an effective CRM process is considered an important asset performing the capability.

Managing knowledge (O5)

Managing knowledge is about making the right knowledge available to the right people. It is about making sure that an organisation can learn, retrieve, and use its knowledge assets in current applications as they are needed, driving decisions to create value. To manage knowledge, a business needs to have an appropriate process in place and tools supporting it. A systematic process to manage knowledge can consist of the following steps: create, store, share, use, and update knowledge. A technical tool, as any kind of IT system, should offer the following functionalities: storing, sharing, and the possibility of searching for knowledge. The most important element of managing knowledge is that it creates possibilities for employees in a business to use existing knowledge as for example to continually fostering innovation business and, by doing so, to create new knowledge. Managing knowledge is usually of high maturity when there are explanations on how and why the need for effective use of managing knowledge can enhance the performance of CRM.

Fostering creativity and innovation (O6)

Creativity is about the ability to create new ideas and concepts while innovation is the process of transforming new ideas into concrete things as a new or improved process. To create value is an implicit objective of innovation.

Creativity and innovation are needed in several parts of the CRM process; for example, when identifying risks and opportunities and methods for analysing risks or how to evaluate the effects of CRM. But creativity and innovation is particularly needed when providing ideas in how to best deal with risks and how to make the best of opportunities in order to influence compliance in a positive way. Creativity and innovation cannot arise without a certain degree of theoretical and practical knowledge based on many interactions in knowledge creation, use of technology, learning processes, and ongoing problem-solving activities. Adequate human relation conditions, adequate organisational structure and specific expertise are needed to foster creativity and innovation but also require theoretical and practical knowledge about important fields related to CRM. Having descriptions about how and why the use of creativity and innovation can enhance the performance of CRM is an important criterion when evaluating the capability.

Communication (O7)

Communication is about exchanging and transmitting information successfully through effective channels. CRM related communication can be used to give all concerned parts of the administration insight and to stimulate an employee's behaviour change in accordance to the understanding of compliance strategies and other important CRM aspects. Therefore, internal communication must be regarded as important. 'The ability to obtain, assimilate, analyse and communicate information is critical to organisational success.'. To have a successful internal communication, a business must have a communication strategy and have an understanding of the factors that influence employees' consciousness and behaviour. Anyone working in communication with the aim to influence behaviour should understand the main theories of change, as well as be able to explain behaviour and its implications for communication.

In practice, a communication strategy typically consists of pre-structured and on regular basis planned programs, campaigns, and actions, as well as more ad hoc and reactive responses to urgent issues and stakeholder concerns. By adjusting and balancing, perceptions of the external and internal context requires continuous flexibility in internal communication. Having descriptions about how and why internal communication activities can give insights and understanding in order to stimulate employees' consciousness in accordance to the compliance strategies and other important CRM aspects will be considered as proof of a higher maturity in performing the capability.

Extracting, managing and ensuring data (O8)

To support the different steps in the CRM process with relevant data, it is important to extract, manage, and ensure data from various internal and external sources and make it available for the employees involved in CRM. It is necessary to have a collection of structured and unstructured large volume data (big data such as business records) that may be analysed to reveal and understand patterns, trends, and associations within the data to provide value to the CRM process. This requires identification of the most relevant sources of the main relevant sectors for CRM, that data is updated continuously and easily accessible to employees. Having descriptions on how and why the data that is extracted, managed and made available support the steps in CRM process is considered an important asset performing the capability.

6.2.5 Decision-Making (D)

Whether it is about to decide on compliance strategies or on actions supporting the compliance strategies, decisions can be considered as the capability to rank alternatives according to what you want and then act consistently with this ranking. This presupposes not only the decision itself but also how to structure the decision-making process, as to define the problem and generate alternatives, which in turn is influenced by what the organisation values as important and the level of risk appetite and risk tolerance. In reality decisions also have to do with culturally influenced mechanisms. Whether this is good or bad depends on the extent to which the organisation has succeeded in integrating culture with the official objectives and strategies stated (see risk culture, **Section 6.2.4**).

With regard to CRM, there are two main ways to effectively stimulate compliance or to prevent non-compliance. The first is to decide which opportunities generated by external context to make use of, and the second is to decide which compliance risks to treat and how. Because businesses have scarce resources, they must prioritize and decide which choices really matter and focus efforts on these only, deferring other risks and opportunities. Knowing that different decisions will lead to different outcomes, decisions must have a purposeful influence. By controlling and deciding when, which, and how to deal with risks and opportunities, a business can influence the achievement of the compliance objectives. Everything a business does to stimulate compliance or to prevent non-compliance should be the result of a deliberate decision no matter at what organisational level the decisions are made.

That also means that different decisions relate and affect each other, and the business must make decisions resulting in a mix of various actions. The quality of the decisions determines how successful a business will be. To be as rational as possible, the only thing the business can do is to use the available knowledge and information and to consider various alternatives; however, always with the ambition to reduce uncertainties by providing new knowledge and information. Prescriptive decision theory states that there are some major steps in decision making: define the problem, create alternatives, describe the consequences of each alternative, analyse pros and cons for how well each alternative meets the objectives, including considering risks and uncertainties with each alternative, and, finally, determine which alternative is the best. These major steps form the basis for the capabilities: Defining, describing and explaining risks and opportunities, Generating alternatives, Making decisions and Implementing decisions.

Defining, describing and explaining risks and opportunities (D1)

To define, describe and explain risks and opportunities starts with considering facts from multiple sources simultaneously having relevant preferences in mind expressed by business´s compliance objectives, compliance strategies, etc. According to Keeney, 'The first element of figuring out a decision problem is to define it carefully, that is, to frame it'. Further on, the definition 'determines the options and consequences to be considered and the kinds of information and uncertainty to be taken into account'. Defining what the problem is 'goes a long way to determining what the answer will be.'. To have a clear and unambiguous definition of risks and opportunities will be the basis from which to generate alternatives of how to treat risks or of how to benefit from opportunities.

Poorly-defined risks and opportunities will make it difficult to describe and explain them and, ultimately, will lead to difficulties to make a rational decision and to understand and implement it. A common method to describe and explain something in order to cover its relevant aspects is to answer the questions who, what, where, when, why, how with respect to the values that a business really cares about.

Discussion on how and why definitions, descriptions, and explanations will serve as a way to agree on facts and as a starting point, generating alternatives is an important criterion when evaluating the capability.

Generates alternatives (D2)

Generating alternatives to treat risks and/or take benefit of opportunities is limited by compliance objectives: only alternatives relevant to the compliance objectives should be considered. Keeping in mind that different decisions will lead to different outcomes, having more than one alternative to choose from will increase the probability of a successful decision (and high outcome). Alternatives must be described by pros and cons relevant to the compliance objectives and by using several sources of information. Furthermore, the more mutually exclusive the alternatives are from each other the easier it is to make a decision. Generating alternatives must start with identifying the most important compliance objectives impacted by the risk and/or opportunity at hand. The search for alternatives is not just a search for ready-made solutions.

It also seeks to discover and invent new courses of action and in best case alternatives, pay attention to elimination of the root of the problem. '…the payoff from seeking good, new creative, alternatives can be extremely high.'. Idea generation techniques can be useful: brainstorming, constructing decision trees and mind mapping.

Discussion on how and why the activities of generating alternatives will serve as a way to increase the probability for a successful decision is considered an asset for this capability.

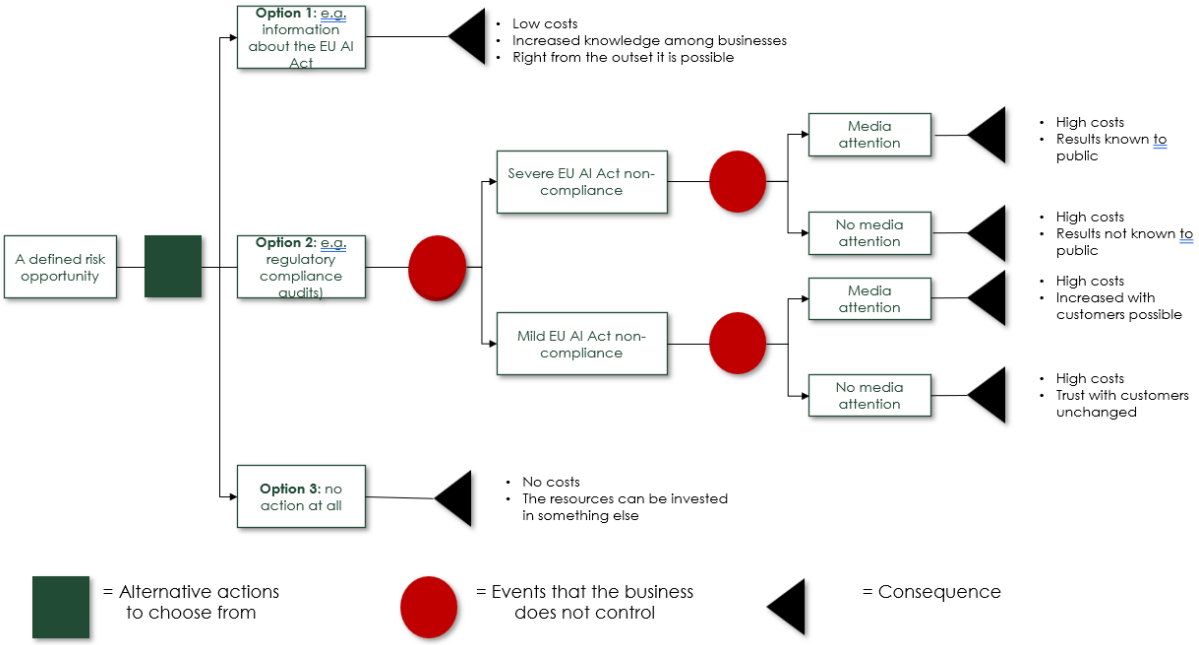
Making decisions (D3)

Making decisions is to choose one of several alternatives. If there is only one alternative there is no decision-situation. Furthermore, decisions should rely on rational reasons only. Rational reasoning means evaluating and comparing alternatives by considering the consequences (see **Figure 8**) with respect to some criteria derived from the compliance objectives and by taking into account established principles as for example how to deal with uncertainties. All based on the information available at the time when the decision is made. Just as in determining the choices of risks and opportunities to care about, decisions about how to treat these risks or take benefit from these opportunities contain an inevitable degree of uncertainty. Indeed, the future is always uncertain – not all available alternatives are known nor are the consequences of each alternative or their probabilities.

Therefore, a business should have some principles in place for how much uncertainty and which risks it is willing to accept or not (known as risk appetite and risk tolerance).

Having descriptions about how and why the decisions effectively stimulate compliance will be considered proof of a higher maturity in performing the capability.

Figure 8: A decision tree for regulatory compliance



Knowing methods of decisions (D4)

Implementing the decisions should generate the outcome expected by the decision. Keeping in mind that many decisions fail because of poor implementation, it is important to implement decisions in a structured way. By having an implementation process, an implementation plan, and cooperation between the decision-maker and the decision-implementers, the probability of successful implementation will increase. Discussions about how and why implementation activities will serve to achieve the intended outcome are considered an important criterion when assessing the capability.

EU AI Act Compliance Risk Management Capability Maturity Model

AI & Partners

Appendix – The EU AI Act CRM CMM

Themes	Capabilities	Level 1	Level 2	Level 3	Level 4	Level 5
Strategy	Formulating compliance strategies					
	Implementing compliance strategies					
Knowledge of external context	Differentiating firms					
	Forecasting the future					
	Knowing reasons for firm's compliance/non-compliance					
	Knowing methods of influence					
Decision making	Defining, describing and explaining risks and opportunities					
	Generating alternatives					
	Making decisions					
	Implementing decisions					
Organisation	Leadership					
	Risk culture					
	Organisational culture					
	Acquiring and developing competencies					
	Managing knowledge					
	Fostering creativity and innovation					
	Communication					
	Extracting, managing and ensuring data					
Evaluation	Evaluating the outcome of actions to stimulate compliance					
	Evaluating the CRM process					

EU AI Act – Advisory | Consultancy | Compliance Software
+31 6 57285579 and +44(0)75 35994 132
s.musch@ai-and-partners.com and m.borrelli@ai-and-partners.com
https://www.ai-and-partners.com/
https://twitter.com/AI_and_Partners @AI_and_Partners
https://www.linkedin.com/company/ai-&-partners/