



D.7.5 A Maturity Model for Information Governance

DOI: 10.5281/zenodo.1173086

Grant Agreement Number:	620998
Project Title:	European Archival Records and Knowledge Preservation
Release Date:	14 th February 2018
Contributors	
Name	Affiliation
Diogo Proença	Instituto Superior Técnico
Ricardo Vieira	Instituto Superior Técnico
José Borbinha	Instituto Superior Técnico
Pável Calado	Instituto Superior Técnico
Bruno Martins	Instituto Superior Técnico
Jaime Kaminski	University of Brighton
Clive Billenness	University of Brighton
David Anderson	University of Brighton
Janet Anderson	University of Brighton

STATEMENT OF ORIGINALITY

Statement of originality:

This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both.

Executive Summary

The E-ARK project focuses on harmonizing currently fragmented solutions that support Archive services, especially in regard to Ingest, Archival Preservation and Dissemination of information. E-ARK solutions have been tested in an open pilot in various national contexts, using existing, near-to-market tools, and services developed by partners. In this deliverable, we create the E-ARK Maturity Model for Information Governance to enable the assessment of the information governance practice in organizations. The Maturity Model focuses on the most relevant references for Archival services especially those that are being improved in the context of the project.

Information Governance as defined by Gartner is the “specification of decision rights and an accountability framework to encourage desirable behaviour in the valuation, creation, storage, use, archival and deletion of information. Includes the processes, roles, standards and metrics that ensure the effective and efficient use of information in enabling an organization to achieve its goals”.¹ According to the concepts used in Appendix A, we understand the scope of the E-ARK concerns as “Information Governance (digital preservation perspective)”. Moreover, in the context of the E-ARK project the perspective of Digital Preservation relates to an archive that follows the recommendation and architecture detailed in the OAIS specification.

This deliverable details the second iteration of the E-ARK Maturity Model for Information Governance which is being used to assess the E-ARK Project use cases.

The first iteration resulted in D7.1, which was applied to assess the E-ARK project pilots before the application of the tools being developed in the project, the results and analysis of the first assessment and evaluation is detailed in D7.2. D7.6 will use the information contained in this deliverable to assess the E-ARK pilots at the end of the project, after the application of the outputs of the project. The main changes on this second iteration of the E-ARK Maturity Model for Information Governance are detailed in section 6.2.

The deliverable begins by providing an introduction to the concept of maturity models followed by a description of the core terms and definitions used in this domain. This is followed by a description of the maturity model development method and an analysis of its application in the first iteration of the model, the lessons learned and future steps. Then, the final version of the E-ARK Maturity Model for Information Governance is detailed. There is now an acronym for the model which is A2MIGO. The development strategy, maturity dimensions and levels are described. This is followed by tracing the ISO 16363 and ISO20652 criteria to the maturity levels of A2MIGO. This section is then concluded with the description of the maturity table which includes the criteria used for the assessment of each maturity level and dimension. The main body of the deliverable concludes with the self-assessment questionnaire that will be used to assess the E-ARK pilots in D7.6. This section details all the questions for each the assessment criteria of A2MIGO.

In this final version of the maturity model there is one appendix, which details the analysis of maturity models in literature that could be relevant to the development of A2MIGO

¹ <http://www.gartner.com/it-glossary/information-governance/>

Table of Contents

1.	Introduction	6
2.	Core Terms and Definitions	9
3.	Maturity Model Development Method	10
4.	The E-ARK Maturity Model for Information Governance (A2MIGO)	16
4.1.	A2MIGO Development strategy	16
4.2.	A2MIGO Dimensions	17
4.3.	A2MIGO Levels	17
4.4.	Tracing A2MIGO to ISO16363 and ISO20652	18
4.4.1.	ISO16363.....	19
4.4.2.	ISO20652.....	23
4.5.	A2MIGO Maturity Table	24
4.5.1.	Management	26
4.5.2.	Processes	29
4.5.3.	Infrastructure.....	33
4.5.4.	General	35
5.	A2MIGO Self-assessment questionnaire	36
5.1.	Introduction	36
5.2.	Management	36
5.3.	Processes	42
5.3.1.	Pre-Ingest.....	42
5.3.2.	Ingest	43
5.3.3.	Archival Storage and Preservation	48
5.3.4.	Data Management.....	50
5.3.5.	Access	51
5.4.	Infrastructure.....	53
5.5.	General	57
6.	Conclusions.....	61
6.1.	Scope and Method.....	61
6.2.	Changes from the first version of the Maturity Model	62
	References	63
	Appendices	65
A.	Information Governance Maturity Models	65
A.1.	Information Governance – General.....	67
A.1.1	DAM Maturity Model.....	67
A.1.2	ECM Maturity Model	68
A.1.3	Asset Management Maturity Model	69
A.1.4	Gartner Enterprise Information Management Maturity Model.....	70
A.2.	Information Governance – Digital Preservation.....	71
A.2.1	Digital Preservation Capability Maturity Model (DPCMM)	71
A.2.2	Brown Digital Preservation Maturity Model	72
A.2.3	Preservica Digital Preservation Maturity Model	73
A.3.	Information Governance – Data Management	74
A.3.1	CMM for RDM.....	74
A.3.2	Stanford Data Governance Maturity Model.....	75
A.3.3	Data Management Maturity (DMM) Model.....	76
A.4.	Information Governance – Records Management.....	77
A.4.1	ARMA Information Governance Maturity Model.....	77
A.4.2	JISC Records Management Maturity Model.....	78
A.5.	Process Management	78
A.5.1	ISO/ IEC 15504	78

A.5.2	Software Engineering Institute Capability Model Integration (CMMI)	79
A.5.3	OMG Business Process Maturity Model	80
A.5.4	Gartner BPM Maturity Model.....	81
A.5.5	Business Process Maturity Model (BPMM)	82
A.6.	IT Governance.....	83
A.6.1	Business-IT Alignment Maturity Model	83
A.6.2	The IT Service CMM	84
A.6.3	COBIT 4.1 Maturity Model	84
A.6.4	IT Capability Model Framework (IT-CMF).....	85
A.6.5	Group IT Controlling (GITC) Maturity Model	86
A.7.	Risk Management	87
A.7.1	Hillson Risk Maturity Model	88
A.7.2	RIMS Risk Maturity Model	88
A.7.3	Deloitte Risk Maturity Model	90
A.8.	Software Engineering Governance	90
A.8.1	Documentation Process Maturity Model	91
A.8.2	Metrics Based Verification and Validation Maturity Model (MB-V2M2)	91
A.8.3	Model-driven Development (MDD) Maturity Model	92

1. Introduction

Maturity models were first introduced due to different viewpoints amongst executive vice presidents and Information Technology (IT) Managers in regard to IT Management in several organizations. In 1974 Nolan proposed four stages of growth for the IT department [1]. The model proposed by Nolan was composed of three types of growth (1) computer applications, (2) personnel specialization and (3) formal management techniques and organization. For each of these types he proposed four stages of growth that were represented by an s-curve as depicted in Figure 1. The four stages of growth are (1) Initiation, (2) Expansion, (3) Formalization and (4) maturity.

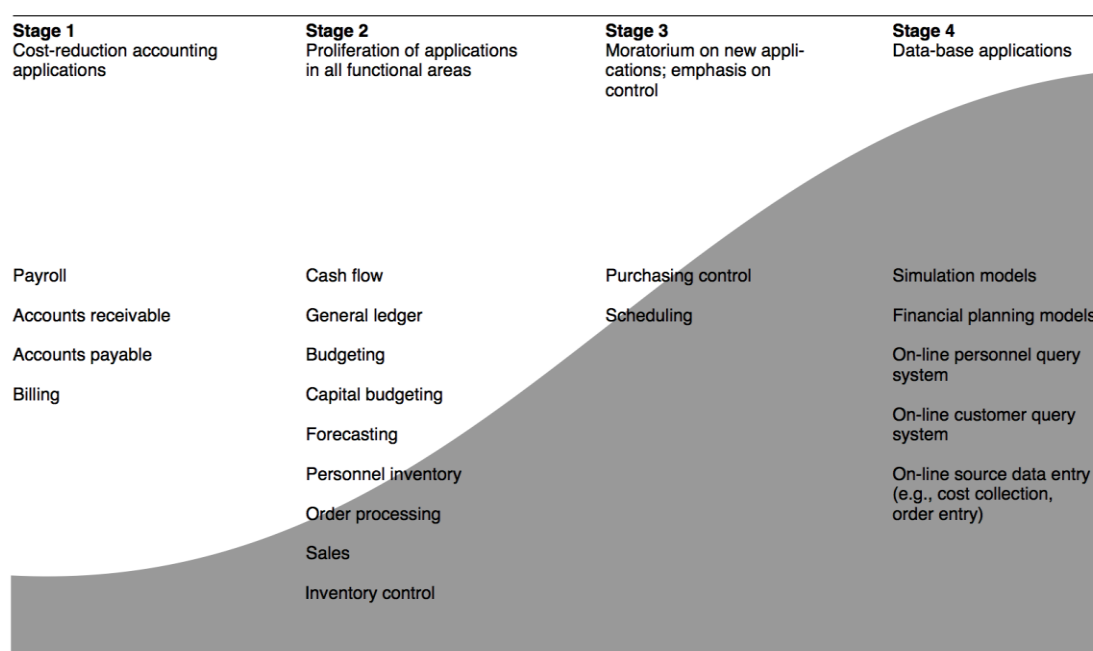


Figure 1. Nolan's Four Stages of Growth [2]

Nolan was a scholar at Harvard University when he first published the four stages of growth. He then left Harvard and founded a company Nolan, Norton & Co. where he further refined his work. Nolan's work was the first significant model of what IT planning is and how we can do it. It started as theories about computer systems in organizations which were then linked to organizational management and innovation theories. Then McFarlan [3], who worked with Nolan in Harvard, released the phases of assimilation in 1983. McFarlan proposed four phases of which were: (1) Identification and Initial investment, (2) Experimentation and Learning, (3) Control and (4) Widespread technology transfer [4]. These phases were based on the assumptions that at different points in the Information Systems (IS) technology evolution the balance between planning pressures would shift, and planning would have different purposes in each of these shifts, so he identified four phases of technology assimilation, each with its own challenges.

Sullivan, Earl and Galliers further continued the evolution of Stages theories. These authors come from the organizational and management side of IS and, as with Nolan, these theories have gone through various iterations over time. These authors initially combined the Nolan and McFarlan approaches but then developed their own specialized approach by focusing on the "organizational alignment" approach.

Sullivan's model [5] reviewed the existing IS planning models in several major US companies and concluded that there are two key determinants of IS planning success (1) Infusion, which focus on the impact and importance of IS and (2)

Diffusion, which focus on the decentralization and spread of IS. The effectiveness of the planning procedures is a correlation between these two factors and the type of planning approach.

Earl's Model was developed from the models of Sullivan, and focused on planning and organizational maturity in regard to planning while trying to give a more specific direction on what actions and organization should be taking at each of the five phases. [6] The five phases are (1) The organizations lacks IS resources and experience, (2) The IS department lacks understanding of the business and where IS can contribute, (3) Growing demand for IS creates a need for prioritization and control, (4) Business units starts to seek to use IS for competitive advantage and (5) IS becomes a key aspect of organizational business planning and directions. [7]

Galliers developed another version of Earl's approach which has as its key organizational elements including the strategy, structure, systems, staff, style, skills and goals [8]. It has six stages of IS growth and maturity (1) Adhocracy, (2) Starting the foundations, (3) Centralized dictatorship, (4) Democratic dialectic and co-operation, (5) Entrepreneurial opportunity and (6) Integrated harmonious relationships.

These models vary in focus as to what the stages relate to. For example, Nolan's models depicted stages in the level of experience in using IS and IT, while McFarlan's and Sullivan's stages relate to the organizational impact of IT. Finally, Earl and Galliers depict stages in organizational maturity for IS planning and management. These stages-based models were the fathers of the current well known maturity models.

A Maturity Model consists of a number of entities, including "maturity levels" (often six) which are, from the lowest to the highest, (0) Non Existent, (1) Initial, (2) Basic, (3) Intermediate, (4) Advanced and (5) Optimizing. Each process can have its own Maturity Model, which will express quantitatively the maturity level of an organization regarding a certain process. A Maturity Model also provides a way for organizations to see clearly what they must accomplish in order to progress to the next maturity level.

The use of maturity models is widespread and accepted, both in industry and academia. There are numerous maturity models, at least one for each of the most trending topics in such areas as Information Technology or Information Systems. Maturity Models are widely used and accepted because of their simplicity and effectiveness. They can help to understand the current level of maturity of a certain aspect in a meaningful way, so that stakeholders can clearly identify strengths and weaknesses requiring improvement, and thus prioritise what must be done in order to reach a higher level. This can be used to show the outcomes that will result from that effort, enabling stakeholders to decide if the outcomes justify the effort and/or investment.

Despite the numerous advantages of maturity models, one common criticism is that existing models lack empirical foundation and reality [46]. The fact is evidenced by the absence of theoretical frameworks and methodologies for the design and development of maturity models [46]. Consequently, maturity models tend to reflect the views of the stakeholders responsible for its creation on a specific problem. Although that does not nullify the value of maturity models it hinders its applicability since stakeholders are unable to (1) understand the requirements and views reflected on the maturity model and consequently (2) determine if the maturity model is suitable for purpose of their assessment. The problem is intensified by the lack of or unsatisfactory documentation of existing maturity models [46].

The E-ARK Project focuses on harmonizing currently fragmented solutions that support Archives services, especially with regard to Ingest, Archival Preservation and Dissemination of information. In order to understand the value and applicability of E-ARK solutions, they will be tested in an open pilot in various national contexts, using existing, near-to-market tools, and services developed by partners. The goal of the work package this deliverable is part of is to assess the value and alignment of E-ARK solutions to existing best practices. This deliverable aims to develop the E-ARK Maturity Model for Information Governance that will allow the assessment of the use cases of the project, before and after the

pilot. Taking into consideration the criticism described above, the maturity model will be designed using an existing development method that will enhance the traceability between the requirements and the model itself.

The Information Systems Audit and Control Association (ISACA) in their COBIT (Control Objectives for Information and Related Technologies) version 5 [59] framework states that

“Information Governance ensures that:

- Stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives which are to be achieved through the acquisition and management of information resources
- Direction is set for information management capabilities through prioritisation and decision-making
- Performance and compliance of the information resource are monitored against agreed-on direction and objectives”²

Information Governance as defined by Gartner is the “specification of decision rights and an accountability framework to encourage desirable behaviour in the valuation, creation, storage, use, archival and deletion of information. Includes the processes, roles, standards and metrics that ensure the effective and efficient use of information in enabling an organization to achieve its goals”.³ According to the concepts used in Appendix A, we understand the scope of the E-ARK to relate to “Information Governance (digital preservation perspective)”. Moreover, in the context of the E-ARK project the perspective of Digital Preservation consists of an archive that follows the recommendation and architecture detailed in the OAIS specification.

² <https://cobitonline.isaca.org/l3-main?book=information&hl=information%20governance#information-chapter01-section05>

³ <http://www.gartner.com/it-glossary/information-governance/>

2. Core Terms and Definitions

This section contains the definitions used throughout this deliverable. Most of the definitions come from SEI CMMI [32] because this is one of the most detailed and formal documents containing all the definitions for maturity models and maturity models assessment.

Archival Information Package (AIP): “An Information Package, consisting of the Content Information and the associated Preservation Description Information (PDI), which is preserved within an OAIS.” [44]

Assessment: “An examination of one or more processes by a trained team of professionals using an appraisal reference model as the basis for determining, at a minimum, strengths and weaknesses.” [32]

Capability Level: “Achievement of process improvement within an individual process area. A capability level is defined by appropriate specific and generic goals for a process area.” [32] Another definition from ISO/IEC 15504, “a point on the six-point ordinal scale (of process capability) that represents the capability of the process; each level builds on the capability of the level below.” [40]

Capability Maturity Model: “A model that contains the essential elements of effective processes for one or more areas of interest and describes an evolutionary improvement path from ad hoc, immature processes to disciplined, mature processes with improved quality and effectiveness.” [32]

Dissemination Information Package (DIP): “An Information Package, derived from one or more AIPs, and sent by Archives to the Consumer in response to a request to the OAIS.” [44]

Maturity: “The extent to which an organization has explicitly and consistently deployed processes that are documented, managed, measured, controlled, and continually improved. Organizational maturity can be measured via appraisals.” [32]

Maturity Level: “Degree of process improvement across a predefined set of process areas in which all goals in the set are attained.” [32]

Process: “A set of interrelated activities, which transform inputs into outputs, to achieve a given purpose. The terms process, sub-process and process element form a hierarchy with process as the highest, most general term, sub-processes below it, and process element as the most specific. A particular process can be called a sub-process if it is part of another larger process. It can also be called a process element if it is not decomposed into sub-processes. This definition of process is consistent with the definition of process in ISO 9000, ISO 12207, ISO 15504, and EIA 731.” [32]

Process Area: “A cluster of related practices in an area that, when implemented collectively, satisfies a set of goals considered important for making improvement in that area.” [32]

Process Assessment: “A disciplined evaluation of an organizational unit’s processes against a Process Assessment Model.” [40]

Submission Information Package (SIP): “An Information Package that is delivered by the Producer to the OAIS for use in the construction or update of one or more AIPs and/or the associated Descriptive Information.” [44]

3. Maturity Model Development Method

As described above, one recurrent criticism of maturity models is that they lack empirical foundation and traceability [46]. The main reason for the criticism is that existing maturity models typically do not follow a theoretical framework or methodology for their development [46]. In fact, there is an absence on literature regarding methods and practices for the design and development of maturity models [46].

One of the most well-known development model for maturity models is from Becker in [41], a procedure based on a scientific research method called Design Science Research (DSR). The well-argued claim of the design procedure [41] is that these fundamental requirements should drive the development of every maturity model. Apart from evaluating well-known models according to these dimensions, the article also delineates a set of steps to correctly develop a maturity model. It depicts which documentation should result from each step, and includes an iterative maturity model development method that proposes that each iteration of the maturity model should be implemented and validated before going to a new iteration. The procedure is depicted in Figure 2 (below). It delineates eight requirements (R1 – R8) [41]:

1. R1 – **A Comparison with existing maturity models** is presented and clearly argues for the need of a new model or the adaptation of an existing one;
2. R2 – **Iterative Procedures** are followed to ensure a feedback loop and refinement;
3. R3 – The principles, quality and effectiveness behind the design and development effort of a maturity model should pass through an iterative **Evaluation** step;
4. R4 – The design and development of maturity models should follow a **Multi-methodological Procedure** whose use must be well founded;
5. R5 – During the development of a maturity model there should be a clear **Identification of Problem Relevance** so that the problem solution can be relevant to practitioners and researchers;
6. R6 – **Problem Definition** should include the application domain for the maturity model and also detail the intended benefits and constraints of application;
7. R7 – There should be a **Targeted Presentation of Results** regarding the users' needs and application constraints;
8. R8 – The design of a maturity model must include **Scientific Documentation**, which details the whole process design for each step of the process, as well as, the methods applied, people involved and the obtained results.

This deliverable is structured according to the different stages of the development method proposed by Becker [41], and represents the second iteration of the E-ARK Maturity Model for Information Governance. The first iteration is detailed in deliverable 7.1 and the initial assessment in deliverable 7.2. Appendix A compares existing maturity models, and Section 4 describes the problem in focus and describes the development strategy, as well as the resulting maturity model. It is important to note that this deliverable focuses only on the first four stages of the method regarding the development of the maturity model. Deliverable 7.6 will focus on the application of the maturity model on the use cases after the project pilot, i.e. the next three stages of the method.

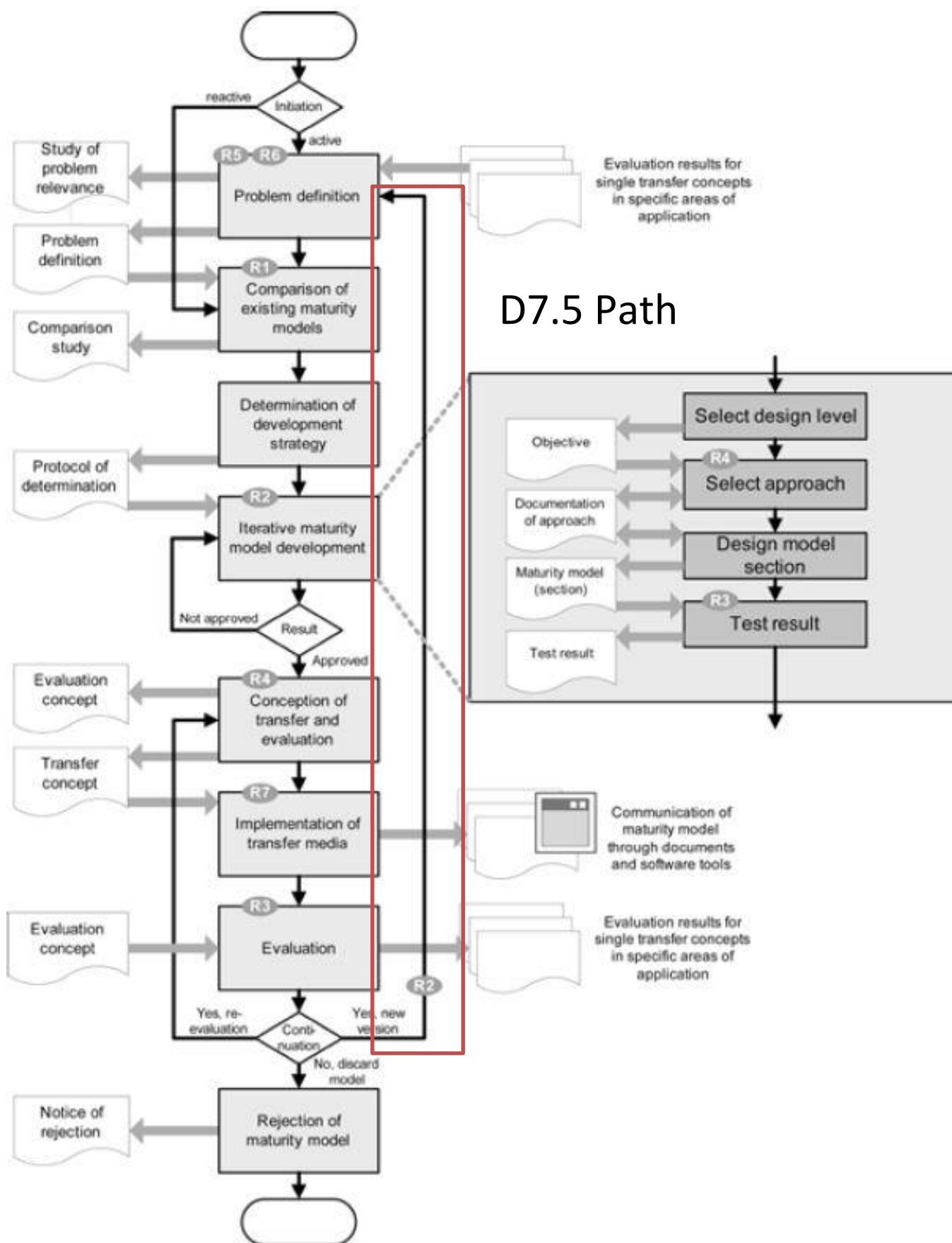


Figure 2. Maturity Model Design Procedure [41]

From the analysis of existing maturity models (Appendix A), we can conclude that the selected maturity models do not detail the development method used, apart from the GITC Maturity Model [35]. The method is the same as the one described in [41] and previously described in this section. Additionally, we can reach the conclusion that there are several attributes being used. If we look at the models that are based on the SEI CMMI they all use process areas as attributes. Process areas are aggregations of processes according to their objective.

However other maturity models use other attributes, such as, dimensions. Dimensions are different viewpoints of the maturity model subject. For example, the COBIT 4.1 Maturity Model has six dimensions that evaluate IT Processes from different viewpoints, such as, tools and automation or plans and procedures. In COBIT 5 this has been transformed into the Process Capability Assessment Model which continues to apply dimensions [59]. The conclusion is that maturity models do not use a single attribute, many even use more than one attribute, such as, dimension and sub-dimensions when the maturity model subject is too complex and needs to be further decomposed. Despite this, the attributes have three objectives: (1) Decompose the Maturity Model into easily understandable sections; (2) Aggregate several business processes into process areas that aggregate processes meeting the same business goal and (3) Provide different viewpoints of the maturity level. We can also conclude that maturity models use different maturity levels. There is no standard number of maturity levels. Despite this, when maturity models are based or follow the SEI CMMI they often use the same five levels used by it and even try to maintain the same maturity level guidelines used by CMMI.

Other models use a number of maturity levels deemed relevant for the maturity model subject which vary from four to six, based on the maturity models analysed. The ones that use four levels, in line with Nolan's four stages, do not reference it, so our conclusion is that despite having the same number of levels/stages they are not basing their work in Nolan's four stages. There are also models that use level 0. This level usually depicts that there is complete lack of maturity and maybe even a lack of awareness of the need for a maturity model subject. In conclusion, maturity models can use various quantities of maturity levels, according to the maturity model subject. The ones based on SEI CMMI usually use the five levels. There are also maturity models that use level 0.

We have also noted existing work in the area of a Digital Preservation Maturity Models undertaken by Adrian Brown where the author examines the notion of "trusted" digital repositories and proposes a maturity model for digital preservation, whose goal is to enable organizations to assess their capabilities and create a roadmap for developing them to the required maturity level [51]. We have also noted the work of Charles Dollar that proposes a Capability Maturity Model to assess digital preservation requirements [52] according to the Open Archival Information System (OAIS) Reference Model (ISO14721) [44] and Trustworthy Repository Assessment Criteria (TRAC) Standard (ISO16363) [43].

In [55] the main principles of design that a generic maturity model should comply in case it is comparative, descriptive or prescriptive are listed, as shown in Table 1. The complexity of the requirements associated with the maturity levels increase from a comparative model to a prescriptive model. However, the classification of minimum requirements for a comparative model can be misleading because, although minimal, these are the principles that act as foundations and non-compliance can condemn the model to fail.

By analysing Table 1 we can see that the minimum requirements described do not include principles associated with improvement measures and review. The design principles that consider improvement measures and their evaluation are only considered in prescriptive models, the most complex maturity models, which contain the principles of defining verifiable criteria and evaluation methods. This table also provides the tracing between various maturity model design principles and the sections where they are described in this document and the other documents that are related to the E-ARK Maturity Model for Information Governance, namely deliverables 7.1 (D7.1), 7.2 (D7.2), 7.5 (D7.5) and 7.6 (D7.6).

Table 1. Maturity Models Design Principles [55]

Group	Design Principles		Details Location
(1) Minimum Requirements	1.1	Basic info	-
		Scope and prerequisites for applicability.	Section 4.1
		Purpose of use.	Section 4.1
		Target audience.	Section 4.2
		Classes of entities in research.	Section 4.2
		Differentiation of related maturity models.	Section 3 and Appendix A
		Process design and empirical validation process.	Section 3 and D7.2
	1.2	Definition of the central aspects of maturity.	-
		Maturity and maturity dimensions.	Section 4.2
		Maturity Levels and paths.	Section 4.3
		Levels of granularity of maturation 4.2 and 4.3	Sections 4.2, 4.3
		Theoretical foundations supporting the model.	Section 4.1
	1.3	Definition of key aspects related to the application domain.	Sections 2, 4.1, 4.4
	1.4	Documentation related to the target audience.	D7.1, D7.2, D7.5, D7.6
(2) Descriptive	2.1	Verifiable criteria for each maturity level.	Section 4.5
	2.2	Method of assessment focused on to the target audience.	-
		Procedure model.	Section 5
		Guidance on the assessment of criteria.	Section 5
		Guidance on the adaptability and configuration of the criteria.	Section 5
		Knowledge of experts from other previous application.	Section 1 and D7.2
(3) Prescriptive	3.1	Improvement measures for each maturity level.	Section 4.5
	3.2	Calculations used for selection of the improvement measures.	-
		Description of the relevant objectives of the model.	Section 4.5
		Description of the relevant influencing factors.	Section 4.5
		Distinction between the external reporting and internal improvement perspective.	Sections 4.1, 4.5
	3.3	Method of maturity determination focused on to the target audience.	-
		Procedure model.	Section 5 and D7.2, D7.6
		Guidance on the assessment variables.	Section 5
		Guidance in terms of implementation and adaptability of improvement measures.	Section 4.5 and Section 5
		Guidance in terms of adaptability and configuration of decision calculations.	Section 4.5 and Section 5
		Knowledge of experts from other previous application.	Section 1 and D7.2

Figure 3 depicts a comparison between the pilots from the initial assessment and evaluation of the E-ARK pilots (D7.2). The deliverable 7.2 builds on the knowledge from the maturity models that were documented in detail in deliverable 7.1, process assessment and assessment in general and focus on assessing the maturity levels of the seven pilots of the E-ARK project:

- Pilot 1: SIP creation of relational databases (Danish National Archives);
- Pilot 2: SIP creation and ingest of records (National Archives of Norway);
- Pilot 3: Ingest from government agencies (National Archives of Estonia);
- Pilot 4: Business archives (National Archives of Estonia, Estonian Business Archives);
- Pilot 5: Preservation and access to records with geodata (National Archives of Slovenia);
- Pilot 6: Seamless integration between a live document management system and a long-term digital archiving and preservation service (KEEP SOLUTIONS);

- Pilot 7: Access to databases (National Archives of Hungary).

Pilot 1 is the one which achieved the best overall results, especially in pre-ingest and access where it achieved the best results. Pilot 2 achieved the second best results. However, there are still some enhancements to perform in the access capability where it achieved maturity level 2. Despite this fact, the access capability is not the focus in pilot 2. Pilot 7 also shows a high level maturity across the capabilities measured in the assessment. However, as in pilot 2, there are still some important enhancements to perform to the access capability. In pilot 7, the importance of the access capability is considerable due to it being one of the focuses of the pilot.

The other four pilots showed similar results among the capabilities. With some exceptions for pilot 3, where it shows higher maturity levels for pre-ingest and the access capabilities. Another exception is pilot 6 which shows higher maturity levels for ingest and data management capabilities. Pilot 5 did not provide an answer to the questions for the archival storage and preservation and as the result no maturity level was calculated. As this is not the focus capability of the pilot there is no major problem with this fact.

There are still several capabilities at maturity level 1 or 2 for all pilots except pilot 1. These should be addressed as soon as possible to reach at least maturity level 3 for the focus capabilities. This is due to the fact that maturity level 3 is considered an intermediate level between “lack of definition of consistency of mechanism and procedures typical of maturity level 1 and 2” and “the documentation and assessment of mechanism and procedures typical of maturity level 4 and 5”. Maturity level 3 depicts aspects that are consistent and defined throughout the organizational or pilot context and shows a state of change in this context from No Definition to Improvement. The expectation is that the outputs of the E-ARK project will help the pilots to reach this maturity level and will also assist other organizations to reach higher levels of maturity and as a result improve archival practice.

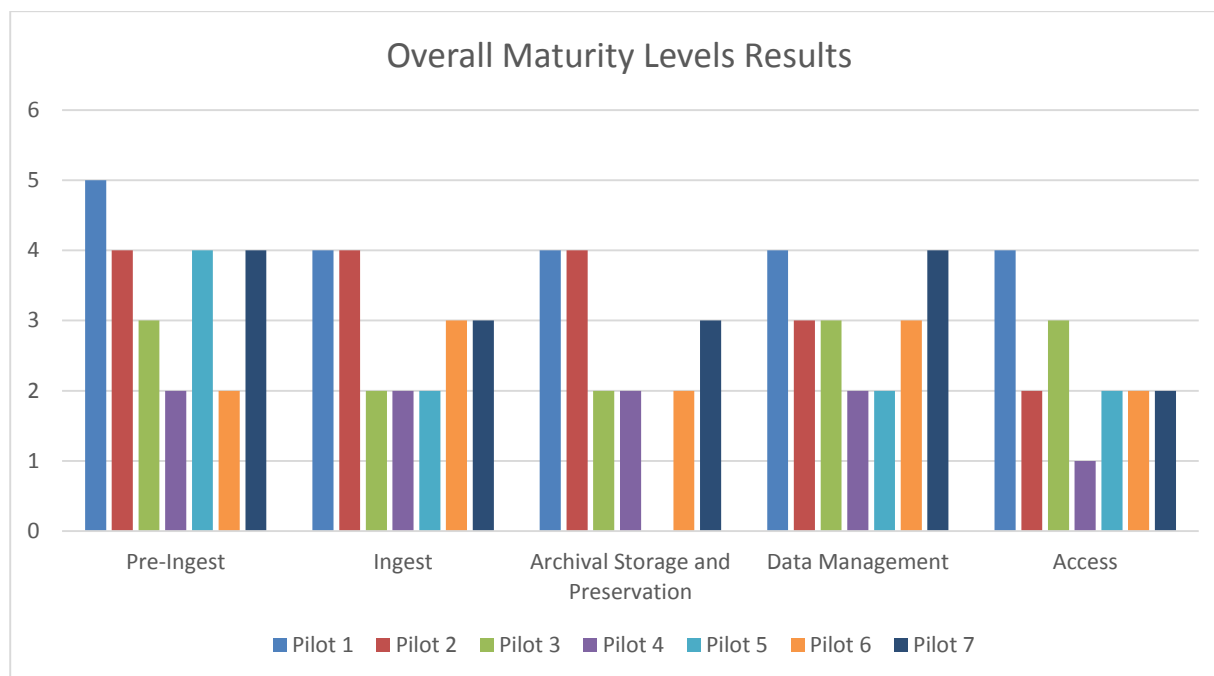


Figure 3. Final Results of the Maturity Levels for All Pilots

D7.2 presented the method to perform the assessment of the E-ARK pilots, as well as the questionnaire itself and the analysis of the results for the pilots. The questionnaire was developed based on a self-assessment questionnaire. The self-assessment consists of following a series of predetermined steps in which the pilot owners answer questions that will result in the determination of a maturity level. As can be seen by reading D7.2, the self-assessment questionnaire D7.5

enabled a detailed analysis and comparison of the pilots and proved useful in identifying both weak points and strengths of the pilot participants. Using these results, it is then possible for pilots to identify points of improvement which can then lead to the creation of an improvement path for the pilots. Despite this there was still room for improvement of the questionnaire. There were some comments left by the pilot owners regarding the difficulty of answering some questions. They reported that there was a difficulty in understanding the differences in each possible answer for the assessment questions. As an example, pilots could understand what a “documented procedure” is but it was difficult for them to understand what is a “defined procedure” or even an “ad hoc assessed procedure”. This led to a revision of the assessment questionnaire and an overhaul of the maturity model to accommodate the changes to the assessment questionnaire. This is detailed in section 4.5. These comments are considered in this revision of the maturity model (in D7.5) and in the final assessment (in D7.6). One other aspect to take into consideration is that only one of the maturity model dimensions was assessed in D7.2 as the E-ARK pilots do not have an organizational context supporting them. However, in D7.5 the questions to assess the other two dimensions are included so that all organizations can use the E-ARK Maturity Model for Information Governance and enhance their current practice. The main changes on this second iteration of the E-ARK Maturity Model for Information Governance are detailed in section 6.2.

This deliverable focuses on the four first stages of the maturity model development method (see section 3 and Table 10) that concentrate on the transfer and evaluation of the maturity model. This deliverable iterates the development of the maturity model based on the application results to improve and extend the maturity model. Finally, deliverable 7.6 will conduct a new self-assessment using the final version of the maturity model after the project pilot.

After analysing the results of the post-assessment questionnaire and meeting with the pilots to address all the issues found during the analysis, it was concluded that the current maturity model development method being used proved very useful to develop and enhance the maturity model. It was also concluded that the current means of communication between the maturity model development team and pilots is appropriate and useful. As a result, the maturity model development team agreed to continue the application of the maturity model development method for deliverables 7.5 and 7.6. In the development method for the maturity model there are two paths that can be taken after the development of the first iteration of the maturity model, based on the results obtained it was realized that during the evaluation of the maturity model there are new aspects of the problem definition that should be taken into consideration and as a result the path depicted in Figure 2 was chosen.

4. The E-ARK Maturity Model for Information Governance (A2MIGO)

This section describes the E-ARK Maturity Model for Information Governance, whose acronym is A2MIGO (which can be spelled as “amigo”, and stands for “E-Ark Maturity Model for Information Governance”).

4.1. A2MIGO Development strategy

As noted in the Introduction, ‘Information Governance’ is defined by Gartner is the “specification of decision rights and an accountability framework to encourage desirable behaviour in the valuation, creation, storage, use, archival and deletion of information. Includes the processes, roles, standards and metrics that ensure the effective and efficient use of information in enabling an organization to achieve its goals”⁴. According to the concepts used in Appendix A, we understand the scope of the E-ARK concerns as “Information Governance (digital preservation perspective)”. Moreover, in the context of the E-ARK project the perspective of Digital Preservation consists of an archive that follows the recommendation and architecture detailed in the OAIS specification.

One limitation of most of the reviewed maturity models is that it is typically not clear which requirements were used for the design and development of the model. In other words, there is weak or non-existent traceability between the maturity model and the requirements that are used as reference. Consequently, stakeholders that wish to use the maturity model are unable to understand if the model is aligned with current best practices.

Since the E-ARK project focuses on Archival services and processes, in this deliverable we will focus on Archival references namely the **Open Archival Information System – Reference Model (OAIS/ISO14721)**, the **Trustworthy Repositories Audit and Certification (TRAC/ISO16363)** and the **Producer-Archive Interface Methodology Abstract Standard (PAIMAS/ISO20652)**. The former provides a checklist to assess the trustworthiness of digital repositories based on the OAIS model [44]. The final version of TRAC was published in 2011, it contains 108 criteria that are divided into three main sections: Organizational Infrastructure, Digital Object Management and Infrastructure and Security Risk Management. A successor version of TRAC, a standard for Trusted Digital Repositories (TDR), was published in February 2012 as the ISO 16363:2012 standard [43]. The latter, PAIMAS is an OAIS-based standard that describes the interface between Producers, i.e. the stakeholders responsible for the creation of the information, and the Archive. It is important to note that the selected references are essential and enough to assess the use cases of the project since their focus is precisely the processes that are being improved in E-ARK (Ingest, Archival Preservation and Dissemination).

This section describes the maturity dimensions and levels that are used for the E-ARK Maturity Model for Information Governance. As described in section 3, existing maturity models differ regarding dimensions and levels. For our maturity model we decided to use the dimensions described in ISO9001 and the levels defined in SEI CMMI. The SEI CMMI levels were selected due to their broader scope making them suitable for wider fields such as that of IG. The latter were selected because they are well-known tested and used levels. In fact, most of the analysed maturity models used the same levels as the ones from SEI CMMI.

⁴ <http://www.gartner.com/it-glossary/information-governance/>

4.2. A2MIGO Dimensions

The E-ARK Maturity Model for IG, consists of three dimensions:

- **Management:** “The term management refers to all the activities that are used to coordinate, direct, and control an organization.” [42]
- **Processes:** “A process is a set of activities that are interrelated or that interact with one another. Processes use resources to transform inputs into outputs. Processes are interconnected because the output from one process becomes the input for another process. In effect, processes are “glued” together by means of such input output relationships.” [42]
- **Infrastructure:** “The term infrastructure refers to the entire system of facilities, equipment, and services that an organization needs in order to function. According to ISO 9001, Part 6.3, the term infrastructure includes buildings and workspaces (including related utilities), process equipment (both hardware and software), support services (such as transportation and communications), and information systems.” [42]

These dimensions provide different viewpoints of information governance which help to decompose the maturity model and enable easy understanding.

4.3. A2MIGO Levels

For each dimension a set of levels is defined, from one to five, where level one shows the initial phase of maturity of a dimension and level five shows that the dimension is fully mature, self-aware and optimizing. These levels and their meaning were based on the levels defined for SEI CMMI. [31]

- **Level 1 (Initial)** - At maturity level 1, information governance practice is viewed as something which is a ‘good thing’ but is ad hoc and chaotic. The organization usually does not provide a stable environment to support information governance. Success in these organizations depends on the competence of the people in the organization and not on the use of proven procedures. Practices are not documented and are not shared even within departments. This leads to variable levels of success in managing information assets. In spite of this chaos, maturity level 1 organizations often provide services that work, but they frequently exceed the budget and schedule documented in their plans. Maturity level 1 organizations are characterized by a tendency to over-commit, abandon proven practices in a time of crisis, and be unable to repeat their successes.
- **Level 2 (Managed)** - At maturity level 2, the information governance procedures are planned and executed in accordance with locally-defined policies; the procedures employ skilled people who have adequate resources to produce controlled outputs; involve relevant stakeholders; are monitored, controlled, and reviewed; and are evaluated for adherence to their procedures descriptions. The discipline reflected by maturity level 2 helps to ensure that existing procedures are retained during times of stress. When these procedures are in place, these are performed and managed according to their documented plans. Also at maturity level 2, the status of the services is visible to management at defined points (e.g., at major milestones, at the completion of major tasks). Commitments are established among relevant stakeholders and are revised as needed. Services are appropriately controlled and satisfy their specified descriptions, standards, and procedures.
- **Level 3 (Defined)** - At maturity level 3, information governance procedures are well characterized and understood, and are described in standards, processes, tools, and methods. The organization’s set of standard procedures, which is the basis for maturity level 3, is established and improved over time. These standard procedures are used to establish consistency across the organization. A critical distinction between maturity levels 2 and 3 is the scope of standards, process descriptions, and procedures. At maturity level 2, the standards, process descriptions, and procedures can be quite different in each specific iteration. At maturity level 3, the

standards, process descriptions, and procedures for a project are tailored from the organization's set of standard procedures to suit a particular project or organizational unit and therefore are more consistent except for the differences allowed by the tailoring guidelines. Another critical distinction is that at maturity level 3, procedures are typically described more rigorously than at maturity level 2. A defined process clearly states the purpose, inputs, entry criteria, activities, roles, measures, verification steps, outputs, and exit criteria. At maturity level 3, processes are managed more proactively using an understanding of the interrelationships of process activities and detailed measures of the process, its work products, and its services. At maturity level 3, the organization further improves its procedures.

- **Level 4 (Quantitatively Managed)** - At maturity level 4, the organization and projects establish quantitative objectives for quality and process performance and use them as criteria in managing projects. Quantitative objectives are based on the needs of customers, end users, and organization. Quality and process performance is understood in statistical terms and is managed throughout the life of projects. Specific measures of performance are collected and statistically analysed. When selecting which aspects to measure and analyse, it is critical to understand the impact of these aspects on achieving the objectives for quality and process performance. Such an approach helps to ensure that monitoring using statistical and other quantitative techniques is applied to where it has the most overall value to the business. Performance baselines and models can be used to help set quality objectives that help achieve business objectives. A critical distinction between maturity levels 3 and 4 is the predictability of performance. At maturity level 4, the performance of projects and selected aspects is controlled using statistical and other quantitative techniques, and predictions are based, in part, on a statistical analysis of fine-grained data.
- **Level 5 (Optimizing)** - At maturity level 5, an organization continually improves its procedures based on a quantitative understanding of its business objectives and performance needs. The organization uses a quantitative approach to understand the variation inherent in procedures and the causes of outcomes. Maturity level 5 focuses on continually improving performance through incremental and innovative procedures and technological improvements. The organization's quality and performance objectives are established, continually revised to reflect changing business objectives and organizational performance, and used as criteria in managing improvement. The effects of deployed improvements are measured using statistical and other quantitative techniques and compared to quality and performance objectives. The project's defined procedures and supporting technology are targets of measurable improvement activities. A critical distinction between maturity levels 4 and 5 is the focus on managing and improving organizational performance. At maturity level 4, the organization and projects focus on understanding and controlling performance at the procedures level and using the results to manage projects. At maturity level 5, the organization is concerned with overall organizational performance using data collected from multiple projects. Analysis of the data identifies shortfalls or gaps in performance. These gaps are used to drive organizational procedures improvement that generates measureable improvement in performance.

4.4. Tracing A2MIGO to ISO16363 and ISO20652

This section details the relationships between the ISO16363 and ISO20652 and the dimensions and levels of A2MIGO. Using these mappings organizations can position themselves in the maturity levels by checking if they meet the required criteria for a certain level and dimension. One important is the lack of mappings to levels 1, 2 and 5 of the E-ARK Maturity Model for Information Governance. Level 1 depicts a complete lack of documented and repeatable procedures in information governance, as such, that means that there are no criteria to be evaluated at this level. Level 2 depicts an organization where there is understanding of the need for information governance however procedures are informal, non-repeatable and performed by individuals. As such, there might be some procedures in place that are in line with the criteria depicted in this section however as these are not properly formalized and defined these do not meet the

level 3 specifications. For level 5, none of the standards depicted here have criteria for this level because it is characterized by top-of-the-line procedures that often are not included in any standard and can only be found in research papers. Organizations at this level fulfil all the levels below 5 which means that their procedures are formally defined and measured.

4.4.1. ISO16363

The ISO 16363 details the recommendation to audit and certificate trustworthy digital repositories. It contains a set of criteria classified into four major areas: (1) Organizational Infrastructure, (2) Digital Object Management, (3) Digital Object Management, and (4) Infrastructure and Security Risk Management. This standard uses the same terminology as found in the ISO14721, the Open Archival Information System (OAIS) standard. The criteria detailed in the ISO16363 are useful to provide assessment criteria for the E-ARK Maturity Model for Information Governance. As such, the criteria in the ISO16363 were mapped to the dimensions and levels of the maturity model and are detailed in the subsections below. One aspect to take into consideration is that the fulfilment of the criteria of ISO16363 is not to be considered as all that is needed to reach a certain level. In this first version of the maturity model also the ISO20652 criteria must be taken into consideration. One aspect to take into consideration is that maturity levels 1 and 2 were not traced to the ISO16363 as this standard's criteria correlates to the maturity level 3 where procedures and documents are formally defined and maturity level 4 where these procedures and documents are also ad hoc assessed.

The traceability of the A2MIGO levels to ISO16363 is detailed in the following tables (work based on [43]):

- Table 2. Tracing of A2MIGO to the ISO16363 management dimension
- Table 3. Tracing of A2MIGO to the ISO16363 infrastructure dimension
- Table 4. Tracing of A2MIGO to the ISO16363 processes dimension

Table 2. Tracing of A2MIGO to the ISO16363 management dimension

A2MIGO Level	ISO16363 Section	ISO16363 Criterion
2	3.1.1	The organization has a mission statement that reflects a commitment to the preservation of, long term retention of, management of, and access to digital information.
2	3.1.2	The organization has a Preservation Strategic Plan that defines the approach the organization will take in the long-term support of its mission.
2	3.1.2.1	The organization has an appropriate succession plan, contingency plans, and/or escrow arrangements in place in case the organization ceases to operate or the governing or funding institution substantially changes its scope.
2	3.1.2.2	The organization monitors its organizational environment to determine when to execute its succession plan, contingency plans, and/or escrow arrangements.
3	3.1.3	The organization has a Collection Policy or other document that specifies the type of information it will preserve, retain, manage, and provide access to.
3	3.2.1	The organization has defined the adequate skills and experience that staff must possess to fulfil the duties that it needs to perform.
3	3.2.1	The organization has appointed staff with adequate skills and experience to fulfil the duties that it needs to perform.
2	3.2.1.1	The organization has identified the duties that it needs to perform.
3	3.2.1.1	The organization has established the duties that it needs to perform.
3	3.2.1.2	The organization has the appropriate number of staff to support all functions and services.
2	3.3.1	The organization has defined its Designated Community and associated knowledge base(s) and shall have these definitions appropriately accessible.
3	3.3.3	The organization has a documented history of the changes to its operations, procedures, software, and hardware.

3	3.3.4	The organization commits to transparency and accountability in all actions supporting the operation and management of the repository that affect the preservation of digital content over time.
3	3.3.5	The organization has defined its information integrity measurements.
3	3.3.5	The organization has collected, tracked, and appropriately provided its information integrity measurements.
4	3.3.6	The organization has committed to a regular schedule of self-assessment and external certification.
4	3.4.1	The organization has short- and long-term business planning processes in place to sustain the repository over time.
3	3.4.2	The organization has financial practices and procedures which are transparent, compliant with relevant accounting standards and practices, and audited by third parties in accordance with territorial legal requirements.
3	3.4.3	The organization analyses and reports on financial risk, benefit, investment, and expenditure (including assets, licenses, and liabilities).
3	3.5.1	The organization has and maintains appropriate contracts or deposit agreements for digital materials that it manages, preserves, and/or to which it provides access.
3	3.5.1.1	The organization has contracts or deposit agreements which specify and transfer all necessary preservation rights, and those rights transferred are documented.
3	3.5.1.2	The organization has defined all appropriate aspects of acquisition, maintenance, access, and withdrawal in written agreements with depositors and other relevant parties.
3	3.5.1.3	The organization has written policies that indicate when it accepts preservation responsibility for contents of each set of submitted data objects.
3	3.5.1.4	The organization has policies in place to address liability and challenges to ownership/rights.
4	5.1.1.6	The organization has identified and documented critical processes that affect its ability to comply with its mandatory responsibilities.
3	5.1.1.6.1	The organization has a documented change management process that identifies changes to critical processes that potentially affect the repository's ability to comply with its mandatory responsibilities.

Table 3. Tracing of A2MIGO to the ISO16363 infrastructure dimension

A2MIGO Level	ISO16363 Section	ISO16363 Criterion
3	3.3.2	The organization has Preservation Policies in place to ensure its Preservation Strategic Plan will be met.
4	3.3.2.1	The organization has mechanisms for review, update, and ongoing development of its Preservation Policies as the repository grows and as technology and community practice evolve.
3	3.3.3	The organization has a documented history of the changes to its operations, procedures, software, and hardware.
2	3.3.5	The organization has defined its information integrity measurements.
3	3.5.2	The organization tracks and manages intellectual property rights and restrictions on use of repository content as required by deposit agreement, contract, or license.
3	5.1.1	The organization has identified and manages the risks to its preservation operations and goals associated with system infrastructure.
3	5.1.1.1	The organization has employed technology watches or other technology monitoring notification systems.
3	5.1.1.1.1	The organization has hardware technologies appropriate to the services it provides to its designated communities.

3	5.1.1.1.2	The organization has documented procedures in place to monitor and receive notifications when hardware technology changes are needed.
3	5.1.1.1.3	The organization has documented procedures in place to evaluate when changes are needed to current hardware.
3	5.1.1.1.4	The organization has procedures, commitment and funding to replace hardware when evaluation indicates the need to do so.
3	5.1.1.1.5	The organization has software technologies appropriate to the services it provides to its designated communities.
3	5.1.1.1.6	The organization has documented procedures in place to monitor and receive notifications when software changes are needed.
3	5.1.1.1.7	The organization has documented procedures in place to evaluate when changes are needed to current software.
3	5.1.1.1.8	The organization has procedures, commitment, and funding to replace software when evaluation indicates the need to do so.
3	5.1.1.2	The organization has adequate hardware and software support for backup functionality sufficient for preserving the repository content and tracking repository functions.
2	5.1.1.3	The organization has mechanisms to detect bit corruption or loss.
3	5.1.1.3.1	The organization has procedures to record and report to its administration all incidents of data corruption or loss.
3	5.1.1.3.1	The organization has procedures defined to repair/replace corrupt or lost data.
3	5.1.1.4	The organization has defined procedures to record and react to the availability of new security updates based on a risk-benefit assessment.
3	5.1.1.5	The organization has defined procedures for storage media and/or hardware change (e.g., refreshing, migration).
3	5.1.1.6.2	The organization has a documented process for testing and evaluating the effect of changes to the repository's critical processes.
2	5.1.2	The organization has documented procedures on how to manage the number and location of copies of all digital objects.
2	5.1.2.1	The organization has documented mechanisms in place to ensure any/multiple copies of digital objects are synchronized.
3	5.2.1	The organization maintains a systematic analysis of security risk factors associated with data, systems, personnel, and physical plant.
3	5.2.2	The organization has implemented controls to adequately address each of the defined security risks.
3	5.2.3	The organization has defined roles, responsibilities, and authorizations related to implementing changes within the system.
3	5.2.4	The organization has suitable documented disaster preparedness and recovery plan(s), including at least one off-site backup of all preserved information together with an offsite copy of the recovery plan(s).

Table 4. Tracing of A2MIGO to the ISO16363 processes dimension

A2MIGO Level	ISO16363 Section	ISO16363 Criterion
3	4.1.1	The organization has identified the Content Information and the Information Properties that the repository will preserve.
3	4.1.1.1	The organization has a procedure(s) for identifying those Information Properties that it will preserve.
3	4.1.1.2	The organization has a record of the Content Information and the Information Properties that it will preserve.
3	4.1.2	The organization has specified the information that needs to be associated with specific Content Information at the time of its deposit.

3	4.1.3	The organization has specifications enabling recognition and parsing of the SIPs.
3	4.1.4	The organization has mechanisms to verify the identity of the Producer of all materials.
3	4.1.5	The organization has an ingest process which verifies each SIP for completeness and correctness.
3	4.1.6	The organization obtains sufficient control over the Digital Objects to preserve them.
2	4.1.7	The organization provides the producer/depositor with appropriate responses at agreed points during the ingest processes.
3	4.1.8	The organization has contemporaneous records of actions and administration processes that are relevant to content acquisition.
3	4.2.1	The organization has for each AIP or class of AIPs preserved by the organization an associated definition that is adequate for parsing the AIP and fit for long-term preservation needs.
3	4.2.1.1	The organization is able to identify which definition applies to which AIP.
3	4.2.1.2	The organization has a definition of each AIP that is adequate for long term preservation, enabling the identification and parsing of all the required components within that AIP.
2	4.2.2	The organization has a description of how AIPs are constructed from SIPs.
3	4.2.3	The organization has documented the final disposition of all SIPs.
3	4.2.3.1	The organization follows documented procedures if a SIP is not incorporated into an AIP or discarded and shall indicate why the SIP was not incorporated or discarded.
2	4.2.4	The organization has and uses a convention that generates persistent, unique identifiers for all AIPs.
3	4.2.4.1	The organization has uniquely identified each AIP within the repository.
3	4.2.4.1.1	The organization has unique identifiers.
3	4.2.4.1.2	The organization has assigned and maintained persistent identifiers of the AIP and its components so as to be unique within the context of the organization.
3	4.2.4.1.3	Documentation describes any processes used for changes to unique identifiers.
3	4.2.4.1.4	The organization is able to provide a complete list of all unique identifiers and do spot checks for duplications.
3	4.2.4.1.5	The system of identifiers is adequate to fit the organization's current and foreseeable future requirements such as numbers of objects.
3	4.2.4.2	The organization has a system of reliable linking/resolution services in order to find the uniquely identified object, regardless of its physical location.
3	4.2.5	The organization has access to necessary tools and resources to provide authoritative Representation Information for all of the digital objects it contains.
3	4.2.5.1	The organization has tools or methods to identify the file type of all submitted Data Objects.
3	4.2.5.2	The organization has defined tools or methods to determine what Representation Information is necessary to make each Data Object understandable to the Designated Community.
3	4.2.5.3	The organization has access to the requisite Representation Information.
3	4.2.5.4	The organization has tools or methods to ensure that the requisite Representation Information is persistently associated with the relevant Data Objects.
3	4.2.6	The organization has documented processes for acquiring Preservation Description Information (PDI) for its associated Content Information and acquire PDI in accordance with the documented processes.
3	4.2.6.1	The organization has documented processes for acquiring PDI.
4	4.2.6.2	The organization executes its documented processes for acquiring PDI.
3	4.2.6.3	The organization has defined procedures to ensure that the PDI is persistently associated with the relevant Content Information.
3	4.2.7	The organization has defined procedures to ensure that the Content Information of the AIPs is understandable for their Designated Community at the time of creation of the AIP.

3	4.2.7.1	The organization has a documented process for testing understandability for their Designated Communities of the Content Information of the AIPs at their creation.
3	4.2.7.2	The organization executes the testing process for each class of Content Information of the AIPs.
3	4.2.7.3	The organization has defined procedures to bring the Content Information of the AIP up to the required level of understandability in case it fails the understandability testing.
2	4.2.8	The organization verifies each AIP for completeness and correctness at the point it is created.
3	4.2.9	The organization has provides an independent mechanism for verifying the integrity of the organizations' collection/content.
3	4.2.10	The organization has contemporaneous records of actions and administration processes that are relevant to AIP creation.
3	4.3.1	The organization has documented preservation strategies relevant to its holdings.
2	4.3.2	The organization has mechanisms in place for monitoring its preservation environment.
3	4.3.2.1	The organization has mechanisms in place for monitoring and notification when Representation Information is inadequate for the Designated Community to understand the data holdings.
3	4.3.3	The organization has mechanisms to change its preservation plans as a result of its monitoring activities.
3	4.3.3.1	The organization has mechanisms for creating, identifying or gathering any extra Representation Information required.
3	4.3.4	The organization provides evidence of the effectiveness of its preservation activities.
3	4.4.1	The organization has specifications for how the AIPs are stored down to the bit level.
3	4.4.1.1	The organization has defined procedures to preserve the Content Information of AIPs.
4	4.4.1.2	The organization actively monitors the integrity of AIPs.
3	4.4.2	The organization has contemporaneous records of actions and administration processes that are relevant to storage and preservation of the AIPs.
3	4.4.2.1	The organization has procedures for all actions taken on AIPs.
3	4.4.2.2	The organization has documented procedures that enable to demonstrate that any actions taken on AIPs were compliant with the specification of those actions.
2	4.5.1	The organization has specified the minimum information requirements to enable the Designated Community to discover and identify material of interest.
3	4.5.2	The organization captures or creates the minimum descriptive information and ensures that it is associated with the AIP.
3	4.5.3	The organization maintains bi-directional linkage between each AIP and its descriptive information.
3	4.5.3.1	The organization maintains the associations between its AIPs and their descriptive information over time.
3	4.6.1	The organization complies with Access Policies.
3	4.6.1.1	The organization has defined procedures to log and review all access management failures and anomalies.
3	4.6.2	The organization has policies and procedures that enable the dissemination of digital objects that are traceable to the originals, with evidence supporting their authenticity.
3	4.6.2.1	The organization records and acts upon problem reports about errors in data or responses from users.

4.4.2. ISO20652

The ISO 20652 details the Producer-Archive Interface Methodology Abstract Standard, which describes the structure of interactions between an Archive and an Information Producer. It defines the method to perform the initial contact between the producers and archive until the first objects are received and validated by the archive. This section details

the mapping of the phases and specific aspects of the phases and the maturity dimensions and levels. One aspect to consider is that there must be a policy and procedures to comply with these criteria for all new producers that begin a project with the archive and also for existing projects with producers. For this standard there were no criteria mapped to the management and infrastructure dimensions because the method this standard defines is related to the pre-ingest phase of an archive. The pre-ingest phase can be viewed as a process which begins with a new project from a producer and is finalized with the ingestion and validation of the first object in the archive. As such, ISO20652 was mapped to the processes dimension, as detailed in Table 5.

Table 5. Tracing of A2MIGO to the ISO20652 dimensions (based on [45])

A2MIGO Dimension	A2MIGO Level	ISO20652 Phase	ISO20652 Criterion
Processes	3	Preliminary Phase	There are Feasibility studies performed.
	3		There is a Preliminary definition of the scope of the project.
	3		There is a draft of the SIP definition.
	3		There is a Draft Submission Agreement.
	3		There is Summary document on the feasibility of the Producer-Archive Project.
	3		There is a Final Decision on proceeding to the formal definition phase which might be approved or might stop the project.
	3		There is an estimate of required Resources.
	3	Formal Definition Phase	There is a complete SIP design.
	3		There are precise definitions of the digital objects to be delivered.
	3		The Submission Agreement is completed.
	3		There are contractual transfer conditions.
	3		Restrictions on access are defined.
	3		A delivery Schedule is defined.
	3		There is a data Dictionary. Note: "A formal repository of terms used to describe data." [45]
	3		A formal Model is defined. Note: A formal model "contains a definition of the objects to be delivered that is as precise and non-ambiguous as possible." [45]
	3		The Information Objects to ingest are defined.
	3	Transfer Phase	There is evidence of transfer of the SIP from the Producer to the Archive.
	3		There is evidence of preliminary processing of the SIP by the Archive.
	3	Validation Phase	There is evidence of validation processing of the SIP by the Archive.
	3		There is evidence that producers receive a validation object.

4.5. A2MIGO Maturity Table

This section details the maturity table for A2MIGO. A maturity table consists of a table that crosses maturity levels with the maturity dimensions and characterizes each dimension in each level. Figure 4 presents the maturity table. The mapping to the assessment criteria for each dimension and maturity level is later detailed in Sections 4.5.1 to 4.5.3. For each criterion there is an identifier that is defined as "Dimension (First Letter)" "Maturity Level". "Criterion ID", as an example the second criterion for maturity level 3 of the processes dimension would be "P3.2" At Maturity Levels 4 and 5 there is general criteria applied to all dimensions which are depicted as "GX.X" and detailed in section 4.5.4. The main goal of A2MIGO is to improve the value of information in an organization. Information value will increase when going from a lower to a higher maturity level, as depicted in Figure 4. Moreover, the lack of procedures and policies in lower levels results in the organization's information being at risk and this risk reduces as policies and procedures become implemented, defined, documented and assessed. Then, in Sections 4.5.1 to 4.5.3, each dimension and maturity level

are described in detail. For each dimension, the aspects being evaluated are detailed and then for each maturity level the key aspects of that specific level are presented. The aspects being evaluated in each dimension are presented in bold. These can be linked to each of the questions title of the self-assessment questionnaire in Section 5.

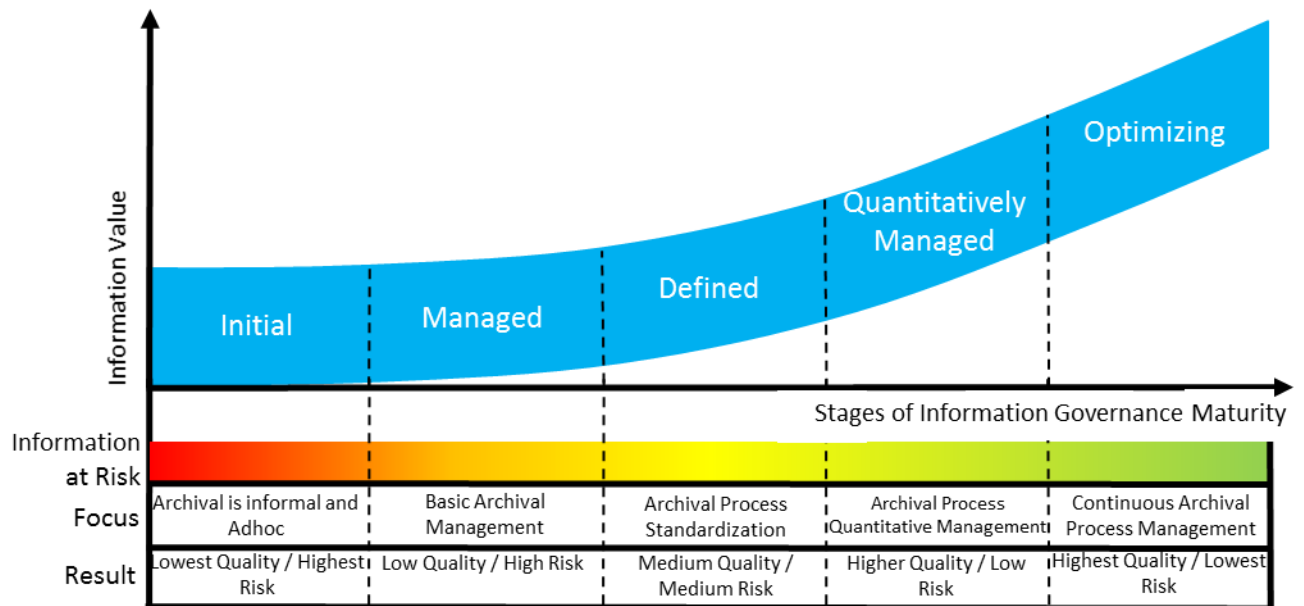


Figure 4. A2MIGO Maturity Table

4.5.1. Management

This section details the meaning of each of the maturity levels for the management dimension of the A2MIGO. Figure 5 depicts the aspects that are considered for each maturity level. For the management dimension the criteria and purpose detailed in Table 6 are considered when calculating the maturity levels.

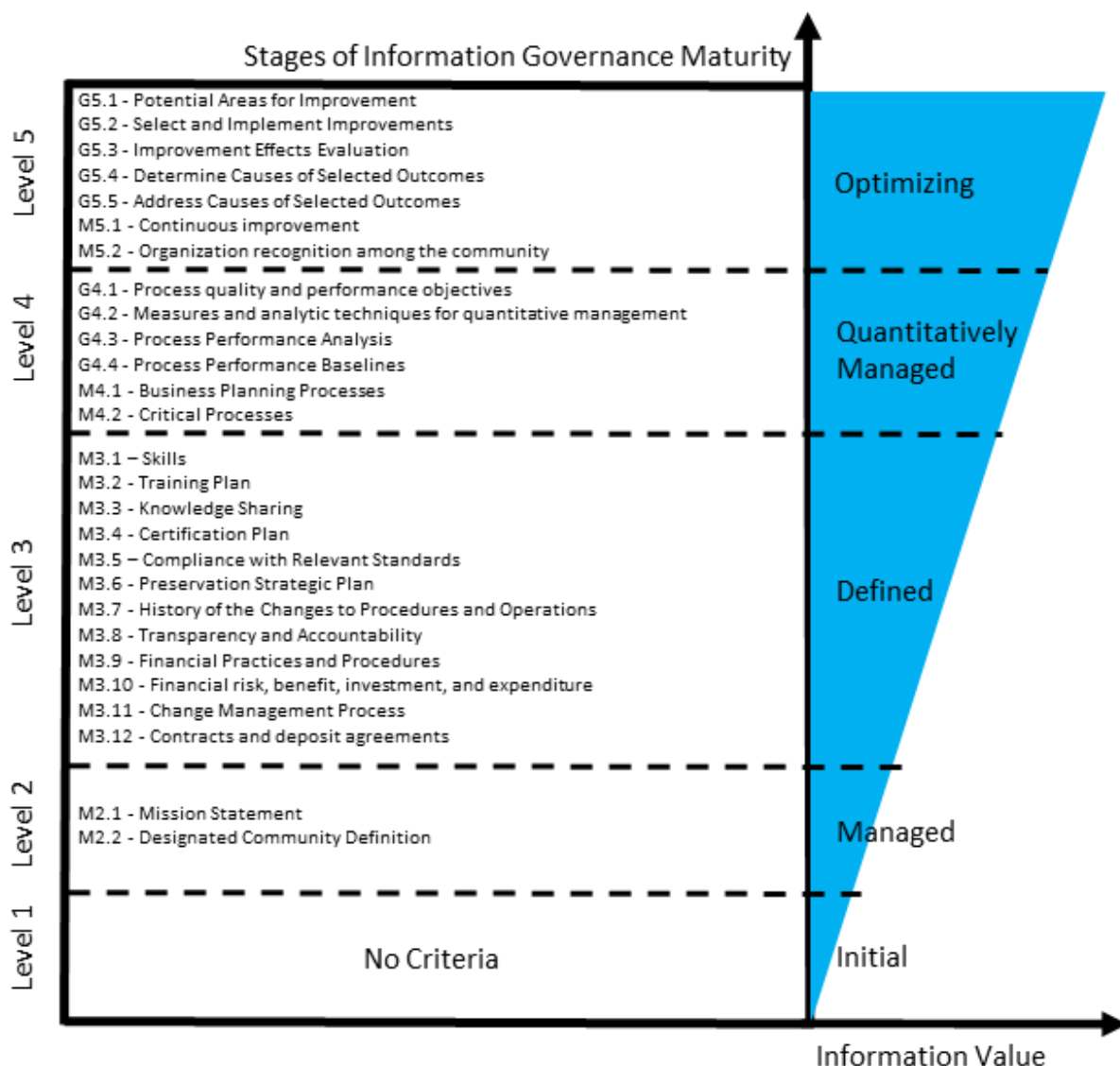


Figure 5. A2MIGO Management Dimension Maturity Levels

Table 6. Management Dimension Assessment Criteria

Maturity Level	Criteria and Purpose
Level 1	No Criteria
Level 2	<ul style="list-style-type: none"> M2.1 - Mission Statement: The purpose is to identify if there is a commitment to preservation, retention, management and access at the organization's highest administrative level;

Maturity Level	Criteria and Purpose
	<ul style="list-style-type: none"> • M2.2 - Designated Community Definition: The purpose is to identify if the organization has a designated community definition which can be used to ascertain if the organization meets the needs of its Designated Community;
Level 3	<ul style="list-style-type: none"> • M3.1 - Skills: The purpose is to identify if the organization guarantees that the relevant skills are identified and present in the organization; • M3.2 - Training Plan: The purpose is to identify if a training plan is developed and implemented in the organization. A training plan outlines the competencies to be obtained, the time frame for achieving these competencies, the training to be undertaken; the delivery modes for the training; among other things; • M3.3 - Knowledge Sharing: The purpose is to identify if the organization share the knowledge existent in the organization man power and if it has a focus on information governance; • M3.4 - Certification Plan: The purpose is to identify if the organization has undergone certification, or if it has plans to do it; • M3.5 - Compliance with Relevant Standards: The purpose is to identify if the organization seeks compliance with relevant standards, such as, the ISO27001 standard for information security management, the ISO14721 standard for the open archival information system, the ISO16363 standard for trustworthy repository assessment checklist, the ISO20652 standard for the Producer-Archive Interface Methodology Abstract Standard, among others; • M3.6 - Preservation Strategic Plan: The purpose is to identify if there is a Preservation Strategic Plan that helps the organization make administrative decisions, shape policies, and allocate resources in order to successfully preserve its holdings. The strategic plan should be based on the organization's established mission, and on its defined values, vision and goals. Strategic plans typically cover a particular finite time period, normally in the 3-5 year range; • M3.7 - History of the Changes to Procedures and Operations: The purpose is to identify if the organization can provide an 'audit trail' through which stakeholders can identify and trace decisions; • M3.8 - Transparency and Accountability: The purpose is to identify if there is transparency in the organization, in the sense of being available to anyone who wishes to know, is the best assurance that the organization operates in accordance with accepted standards and practices; • M3.9 - Financial Practices and Procedures: The purpose is to identify if the organization can protect itself against malfeasance or other activity that might threaten its economic viability. Achieved by financial practices and procedures which are transparent, compliant with relevant accounting standards and practices, and audited by third parties in accordance with territorial legal requirements; • M3.10 - Financial risk, benefit, investment, and expenditure: The purpose is to identify if the organization can demonstrate that the organization has identified and documented these categories, and actively manages them, including identifying and responding to risks, describing and leveraging benefits, specifying and balancing investments, and anticipating and preparing for expenditures. (including assets, licenses, and liabilities); • M3.11 - Change Management Process: The purpose is to identify if the organization can document not only the current processes, but the prior processes that were applied to its holdings. • M3.12 - Contracts and deposit agreements: The purpose is to identify if the organization can ensure that it has the rights and authorizations needed to enable it to collect and preserve information objects over time, make that information available to its Designated Community, and defend those rights when challenged.

Maturity Level	Criteria and Purpose
Level 4	<ul style="list-style-type: none"> • M4.1 - Business Planning Processes: The purpose is to identify if the organization performs a business planning process which can be used to ensure the viability of the organization over the period it has promised to provide access to its contents for its Designated Community • M4.2 - Critical Processes: The purpose is to identify if the critical processes can be monitored to ensure that they continue to meet the mandatory responsibilities and to ensure that any changes to those processes are examined and tested;
Level 5	<ul style="list-style-type: none"> • M5.1 - Continuous improvement: The purpose is to identify if the organization is always striving for continuous improvement of their management policies and procedures, as well as, skills and other relevant aspects of management; • M5.2 - Organization recognition among the community: The purpose is to identify if peers recognize the organization as a good example of information governance through the dissemination of implemented procedures and innovative approaches to information governance;

4.5.2. Processes

This section details the meaning of each of the maturity levels for the processes dimension of the A2MIGO. Figure 6 depicts the aspects that are considered for each maturity level. For the processes dimension the criteria and purpose detailed in Table 7 are considered when calculating the maturity levels.

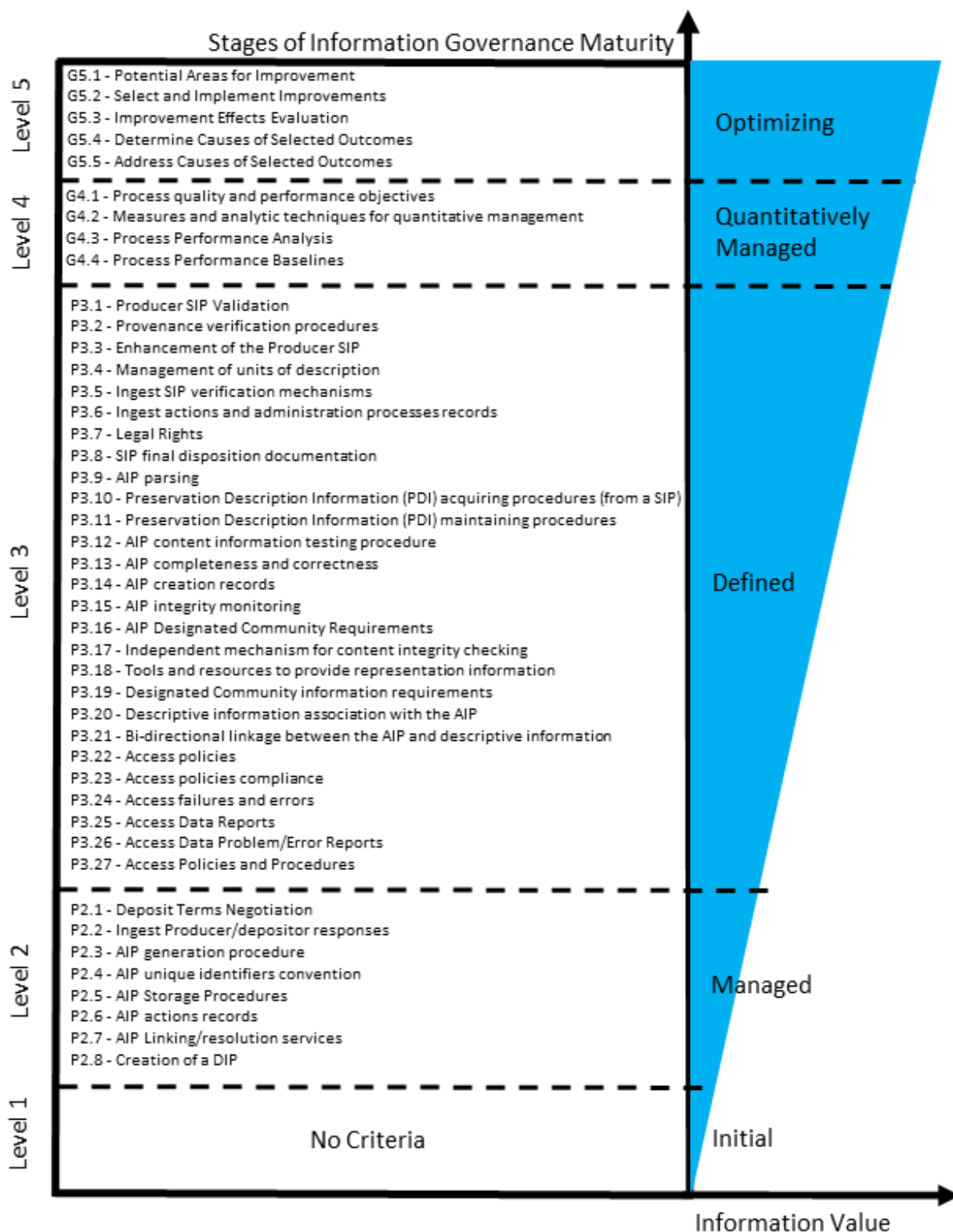


Figure 6. A2MIGO Process Dimension Maturity Levels

Table 7. Processes Dimension Assessment Criteria

Maturity Level	Criteria and Purpose
Level 1	No Criteria
Level 2	<ul style="list-style-type: none"> • P2.1 - Deposit Terms Negotiation: The purpose is to identify if the Archive can negotiate the terms of deposit with Producers. Terms of deposit might include the specification of the metadata that must be included at the time of deposit, the schedule and method of deposit, the responsibilities of the Producer and the Archive regarding the information being ingested, among other examples; • P2.2 - Ingest Producer/depositor responses: The purpose is to identify if the organization provides responses to the Producer at the agreed points to ensure that there are no faults in communication that might lead to loss of a SIP; • P2.3 - AIP generation procedure: The purpose is to identify if the organization can generate an AIP from a SIP. The organization must ensure that the AIP correctly represents the SIP; • P2.4 - AIP unique identifiers convention: The purpose is to identify if the organization generates persistent, unique identifier for each AIP so that an AIP can be found in the future. This also ensures that an AIP can be distinguished from all other AIP in the repository. Understand if the organization has records that detail how changes to unique identifiers are to be performed so that AIP don't lose context, are not lost and can be distinguished from all other AIP in the repository; • P2.5 - AIP Storage Procedures: The purpose is to identify if there are procedures that define how the AIP is stored down to the bit level, that ensure that information can be extracted from an AIP; • P2.6 - AIP actions records: The purpose is to identify if there are records, according to their legal and regulatory environment, to serve as evidence of the actions performed during storage and preservation of the AIP, to ensure that documentation is up to date, valid and authentic; • P2.7 - AIP Linking/resolution services: The purpose is to identify if the organization has a system of reliable linking/resolution services to find a uniquely identified object, regardless of its physical location so that all actions related to an AIP can be traced over time, system and storage changes; • P2.8 - Creation of a DIP: The purpose is to identify if there is a procedure to create a DIP from an AIP;
Level 3	<ul style="list-style-type: none"> • P3.1 - Producer SIP Validation: The purpose is to identify if the Archive validates the Producer SIP regarding format and structure. If the SIP has deviations the Archive might reject the SIP and request the Producer to deliver a corrected SIP; • P3.2 - Provenance verification procedures: The purpose is to identify if the organization has mechanisms to guarantee the provenance of the information to be Ingested; • P3.3 - Enhancement of the Producer SIP: The purpose is to identify if a Producer SIP is checked and completed. This can be done by adding further metadata, or restructure the SIP, among other procedures. • P3.4 - Management of units of description: The purpose is to identify if the Archive can manage units of description based on the Producer SIP information, or if reuses existing ones for scoping the new SIP; • P3.5 - Ingest SIP verification mechanisms: The purpose is to identify if the organization has mechanisms to detect and correct errors during the creation of a SIP or of transmission errors during an Ingest session; • P3.6 - Ingest actions and administration processes records: The purpose is to identify if the organization has the updated records of all documentation relevant for the Ingest process which may be solicited during an audit; • P3.7 - Legal Rights: The purpose is to identify if the Archive can manage the legal rights (copyright, data protection, and ownership) of objects during Ingest into the Archive. In

Maturity Level	Criteria and Purpose
	<p>this sense managing legal rights involves checking if the content being ingested has legal rights associated; check if the content is not duplicated from previous ingests or even plagiarized from other Producers. It also includes creating access restrictions to certain objects when the producer requests it;</p> <ul style="list-style-type: none"> • P3.8 - SIP final disposition documentation: The purpose is to identify if the organization has defined procedures to demonstrate that a specific SIP has either accepted, incorporated as part of an AIP, or been rejected and disposed; • P3.9 - AIP parsing: The purpose is to identify if the organization can store a wide variety of information types and create AIP classes to describe AIPs that store the same type of information. The AIP classes are important to understand the variety of information that is stored and to enable correct parsing of all information stored in the Archive; • P3.10 - Preservation Description Information (PDI) acquiring procedures (from a SIP): The purpose is to identify if the organization has defined procedures to ensure that the PDI is associated with the relevant content information. This will support authenticity of the preserved objects and enable the detection of unauthorized changes; • P3.11 - Preservation Description Information (PDI) maintaining procedures: The purpose is to identify if the organization has defined procedures to ensure that the PDI is maintained through its life cycle. This includes performing changes in the PDI as result from external requirements changes; • P3.12 - AIP content information testing procedure: The purpose is to identify if the organization has a procedure for testing if the content information of the AIP at its creation is understandable by the designated communities so that all Ingested objects are deemed relevant and usable by the designated community; • P3.13 - AIP completeness and correctness: The purpose is to identify if the organization verifies the completeness and correctness of each AIP when it is created to ensure that all AIP can be traced back to the SIP provided by Producers; • P3.14 - AIP creation records: The purpose is to identify if the organization has records, according to their legal and regulatory environment, to serve as evidence of the actions performed to create an AIP, as to ensure that nothing is omitted from AIP records which might be needed to verify that all AIP have been properly created and in accordance with the documented procedures. • P3.15 - AIP integrity monitoring: The purpose is to identify if AIP integrity is monitored, which is necessary to protect the integrity of an AIP over time; • P3.16 - AIP Designated Community Requirements: The purpose is to identify if there is a procedure to gather and review the AIP requirements from the designated community; • P3.17 - Independent mechanism for content integrity checking: The purpose is to identify if the organization has mechanism for content integrity checking that enables independent audits; • P3.18 - Tools and resources to provide representation information: The purpose is to identify if the organization has tools or methods to identify the file type of all submitted objects, to determine what other more representation information is necessary to make each object understandable, and the ability to ensure that all that Representation information is associated with the relevant objects. • P3.19 - Designated Community information requirements: The purpose is to identify if the Archive enables discovery of its holdings; • P3.20 - Descriptive information association with the AIP: The purpose is to identify if the Archive ensures that descriptive information is associated with the AIP. The archive must evidence that it associates with each AIP, the minimum descriptive information that was received from the producer or created by the archive. Associating the descriptive information with the AIP is important, although it does not require one-to-one

Maturity Level	Criteria and Purpose
	<p>correspondence, and may not necessarily be stored with the AIP. Hierarchical schemes can allow some descriptive information to be associated with many AIP;</p> <ul style="list-style-type: none"> • P3.21 - Bi-directional linkage between the AIP and descriptive information: The purpose is to identify if the Archive ensures that all AIP can be located and retrieved. An archive must have procedures on how to establish and maintain relationships between the descriptive information and the AIP, and should ensure that every AIP has descriptive information associated with it and that all descriptive information must point to at least one AIP. • P3.22 - Access policies: The purpose is to identify if the organization has accesses policies defined with the designated communities; • P3.23 - Access policies compliance: The purpose is to identify if the organization complies with accesses policies defined with the designated communities. Failure to comply might affect the trust that designated community has on the organization about the support of the user community; • P3.24 - Access failures and errors: The purpose is to identify if the organization maintains a log and reviews all access failures and errors, which can help identify security threats and access system failures; • P3.25 - Access Data Reports: The purpose is to identify if the organization records access to the contents, as a measure to detect abuses or misuses; • P3.26 - Access Data Problem/Error Reports: The purpose is to identify if the organization investigates and resolves both incident and problem reports about errors in data or responses from Consumers essential to become a trustworthy source of information; • P3.27 - Access Policies and Procedures: The purpose is to identify if the organization maintains an auditable chain of authenticity from the AIP to a DIP.

4.5.3. Infrastructure

This section details the meaning of each of the maturity levels for the infrastructure dimension of A2MIGO. Figure 7 depicts the aspects that are considered for each maturity level. For the infrastructure dimension the criteria and purpose detailed in Table 8 are considered when calculating the maturity levels.

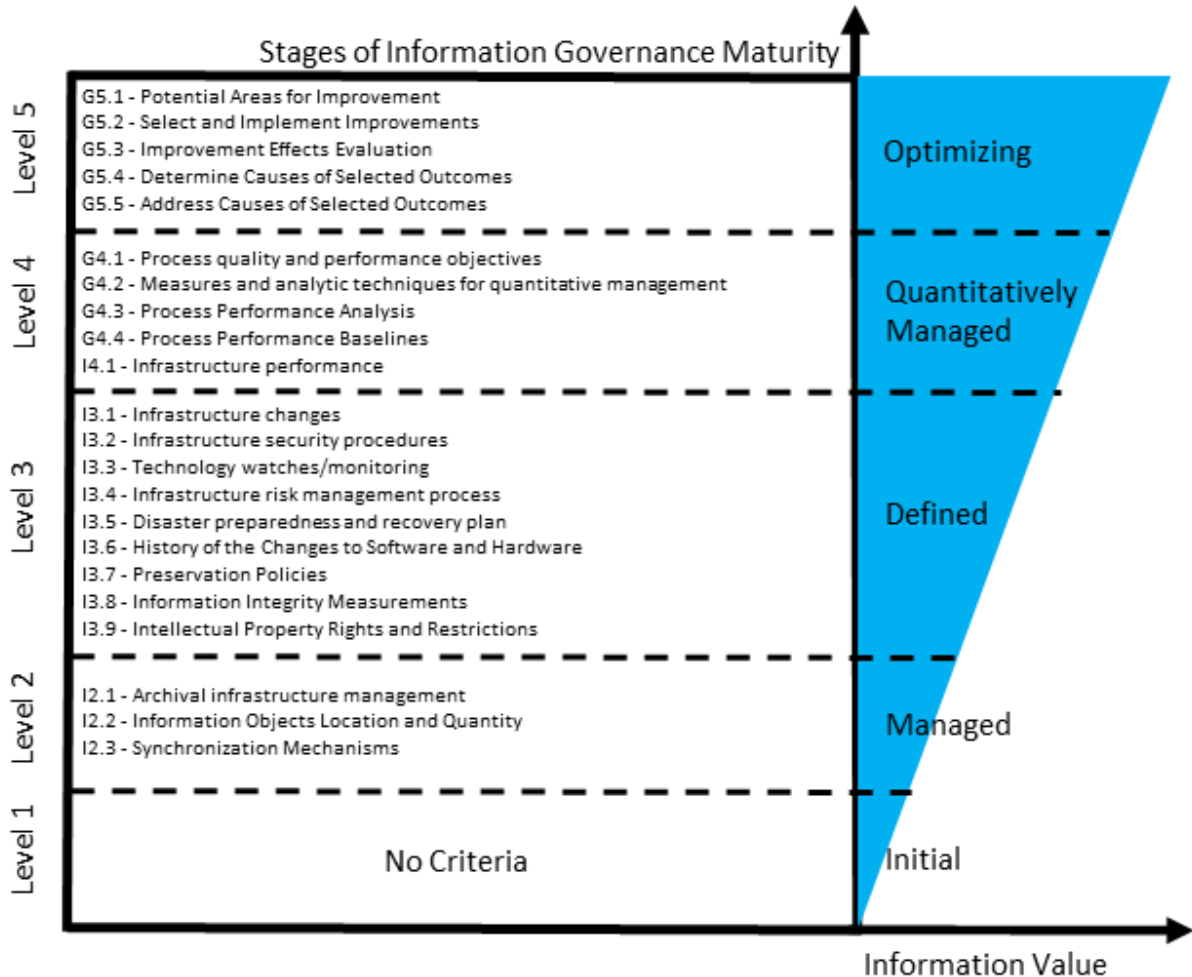


Figure 7. A2MIGO Infrastructure Dimension Maturity Levels

Table 8. Infrastructure Dimension Assessment Criteria

Maturity Level	Criteria and Purpose
Level 1	No Criteria
Level 2	<ul style="list-style-type: none"> I2.1 - Archival infrastructure management: The purpose is to identify if the organization manages the infrastructure that supports its business; I2.2 - Information Objects Location and Quantity: The purpose is to identify if the organization can assert that it is providing an authentic copy of a particular information object; I2.3 - Synchronization Mechanisms: The purpose is to identify if the organization can ensure that multiple copies of an information object remain identical, within a time established as acceptable by the organization, and that a copy can be used to replace a corrupted copy of the object;

Maturity Level	Criteria and Purpose
Level 3	<ul style="list-style-type: none"> • I3.1 - Infrastructure changes: The purpose is to identify how the infrastructure is upgraded and maintained so that it continues to remain operational and meet the customers' requirements; • I3.2 - Infrastructure security procedures: The purpose is to identify if the organization has security procedures for the infrastructure and how these procedures are implemented; • I3.3 - Technology watches/monitoring: The purpose is to identify if the organization has mechanisms for technology watch/monitoring and how they are implemented in the organization; • I3.4 - Infrastructure risk management process: The purpose is to identify how risk management is performed in the organization; • I3.5 - Disaster preparedness and recovery plan: The purpose is to identify if the organization maintains a suitable disaster preparedness and recovery plan(s); • I3.6 - History of the Changes to Software and Hardware: The purpose is to identify if the organization can provide an 'audit trail' through which stakeholders can identify and trace decisions; • I3.7 - Preservation Policies: The purpose is to identify if the organization can fulfil the part of its mission related to preservation; • I3.8 - Information Integrity Measurements: The purpose is to identify if the organization can provide documentation that it has developed or adapted appropriate measures for ensuring the integrity of its holdings; • I3.9 - Intellectual Property Rights and Restrictions: The purpose is to identify if the organization can track, act on, and verify rights and restrictions related to the use of the information within the organization, as required by deposit agreement, contract, or license;
Level 4	<ul style="list-style-type: none"> • I4.1 - Infrastructure performance: The purpose is to identify if the organization monitors the infrastructure performance;

4.5.4. General

This section details the aspects that are taken into consideration when assessing the maturity levels 4 and 5 of all the dimensions of the A2MIGO. These aspects, depicted in Table 9, are considered when calculating the maturity levels.

Table 9. General Assessment Criteria for Maturity Levels 4 and 5

Maturity Level	Criteria and Purpose
Level 4	<ul style="list-style-type: none"> • G4.1 - Process quality and performance objectives: The purpose is to identify if objectives for quality and process performance are established and negotiated at an appropriate level of detail to permit an overall evaluation of the objectives and risks at the process level. • G4.2 - Measures and analytic techniques for quantitative management: The purpose is to identify if the organization selects measures and analytic techniques to be used in quantitative management. • G4.3 - Process Performance Analysis: The purpose is to identify if the selected measures are analysed to characterize the performance of the organizations' processes. • G4.4 - Process Performance Baselines: The purpose is to identify if process performance baselines are established and compared to the organization's quality and process performance objectives to determine if the quality and process performance objectives are being achieved.
Level 5	<ul style="list-style-type: none"> • G5.1 - Potential Areas for Improvement: The purpose is to identify if the organization identifies potential areas for improvement that could contribute to meeting business objectives. • G5.2 - Select and Implement Improvements: The purpose is to identify if there is a selection and implementation of improvements for deployment throughout the organization based on an evaluation of costs, benefits, and other factors. • G5.3 - Improvement Effects Evaluation: The purpose is to identify if the organization evaluates the effects of deployed improvements on quality and process performance using statistical and other quantitative techniques. • G5.4 - Determine Causes of Selected Outcomes: The purpose is to identify if the organization systematically determines the root causes of selected and analysed outcomes. • G5.5 - Address Causes of Selected Outcomes: The purpose is to identify if the organization implements and evaluates selected action proposals developed in causal analysis.

5. A2MIGO Self-assessment questionnaire

This section details the self-assessment questionnaire to assess a scenario according to the A2MIGO. The questionnaire comprises of three main sections, one for each of the maturity model dimensions, with a set of questions in each section. Each question is structured in a table with the following fields:

1. **ID:** Which identifies the number of the question in the overall questionnaire;
2. **Title:** Which depicts the main topic the question refers to;
3. **Question:** Which details the question itself;
4. **Objective:** Which details the objective of that question, what knowledge the question intends to capture;
5. **Notes:** Which either clarifies some aspects and/or terms of the question or details examples of evidence to substantiate the answer for the question;
6. **Terms:** Which identifies the terms that are detailed in EVOC. EVOC is the vocabulary manager which makes part of the knowledge centre being developed in work package 7, as part of D7.3 and D7.4;
7. **Answers:** Which depicts the five possible answers to the question;
8. **Source:** Which details the source from which that specific question originates.

The questionnaire starts by providing an introduction. This introduction provides details on the purpose of the questionnaire, how it will be analysed, and clarifies concepts being constantly used throughout the questionnaire. Sections 5.2 to 5.5 detail the questionnaire that can be used to calculate the information governance maturity levels.

5.1. Introduction

This questionnaire consists of a set of questions that will be used to determine the information governance maturity level of the organization for each of the three dimensions of the maturity model. All questions are mandatory.

For each question there is a field that respondents can use to provide additional comments, clarifications or a justification to the answer. These comments will be considered by the assessment team when evaluating the answers.

5.2. Management

This section details the questions used in the self-assessment to calculate the maturity levels for the management dimension.

ID	M2.1
Title	Mission Statement
Question	Does the organization have a mission statement?
Purpose	The purpose is to identify if there is a commitment to preservation, retention, management and access at the organization's highest administrative level.
Notes	Examples of evidence to demonstrate this can be a mission statement of the organization or its parent organization that specifically addresses or implicitly calls for the preservation of information and/or other resources it holds; a legal, statutory, or government regulatory mandate applicable to the organization that specifically addresses or implicitly requires the preservation, retention, management and access to information and/or other resources.
Terms	-
Answers	No: There is no mission statement of the organization.
	Yes: There is a mission statement of the organization.
Source	TRAC – Criterion 3.1.1 [43]

ID	M2.2
Title	Designated Community Definition
Question	Is there an accessible definition of the organization's designated community?
Purpose	The purpose is to identify if the organization has a designated community definition which can be used to ascertain if the organization meets the needs of its Designated Community.
Notes	An example of evidence to demonstrate this is a written definition of the Designated Community. Examples of Designated Community definitions include: (1) General English-reading public educated to high school and above, with access to a Web Browser (HTML 4.0 capable); (2) Astronomer (undergraduate and above) with access to Flexible Image Transport System (FITS) software such as FITSIO, familiar with astronomical spectrographic instruments.
Terms	Designated Community (http://evoc.sysresearch.org/E-ARK/OAIS/Designated%20Community)
Answers	No: There is no accessible definition of the organization's designated community.
	Yes: There is an accessible definition of the organization's designated community.
Source	TRAC – Criterion 3.3.1 [43]

ID	M3.1
Title	Skills
Question	Are the required skills managed?
Purpose	The purpose is to identify if the organization guarantees that the relevant skills are identified and present in the organization.
Notes	Examples of evidence to demonstrate this can be a procedure that assesses the current skills within the organization on a periodic basis; an automatic mechanism, with a defined set of indicators used to assess skills, that runs continuously and alerts when an indicators or set of indicators reach a certain threshold; documentation on the required skills within the organization, among others.
Terms	-
Answers	No: There is no skill management in place.
	Yes: There is skill management in place.
Source	COBIT 4.1 – Page 21 [26]

ID	M3.2
Title	Training Plan
Question	Is there a training plan developed and implemented in the organization?
Purpose	The purpose is to identify if a training plan is developed and implemented in the organization. A training plan outlines the competencies to be obtained, the time frame for achieving these competencies, the training to be undertaken; the delivery modes for the training; among other things.
Notes	Examples of evidence to demonstrate this can be a procedure that assesses the current training plan within the organization on a periodic basis; an automatic mechanism, with a defined set of indicators used to measure the efficacy and applicability of the training plan, that runs continuously and alerts when an indicators or set of indicators reach a certain threshold, among others.
Terms	-
Answers	No: There is no training plan.
	Yes: The training plan is developed and implemented.
Source	COBIT 4.1 – Page 21 [26]

ID	M3.3
Title	Knowledge Sharing

Question	Is knowledge sharing part of the organizational culture?
Purpose	The purpose is to identify if the organization share the knowledge existent in the organization man power and if it has a focus on information governance.
Notes	Knowledge sharing refers to the organizational systematic effort to share the knowledge that exists in the organization. This means sharing experiences, hard and soft skills, as well as, lessons learned in external training that can enrich the organizational knowledge. Knowledge sharing can be achieved through several means, such as, internal training, wikis and shared documentation.
Terms	-
Answers	No: There is no knowledge sharing within the organization.
	Yes: Knowledge sharing within the organization is performed.
Source	COBIT 4.1 – Page 21 [26]

ID	M3.4
Title	Certification Plan
Question	Is there a certification plan developed and implemented in the organization?
Purpose	The purpose is to identify if the organization has undergone certification, or if it has plans to do it.
Notes	Standards certification can be used to certify that the processes and procedures implemented in the organization are aligned with best practice, relevant, efficient or effective. They are also a means for potential customers or funders to have a certain degree of confidence in the organization. Standards Certification must be issued by a recognized organization. Standards might include IEEE, ISO or other relevant standards.
Terms	-
Answers	No: There is no certification plan.
	Yes: The certification plan is developed and implemented.
Source	COBIT 4.1 – Page 21 [26]

ID	M3.5
Title	Compliance with Relevant Standards
Question	Does the organization assess the compliance with relevant standards?
Purpose	The purpose is to identify if the organization seeks compliance with relevant standards, such as, the ISO27001 standard for information security management, the ISO14721 standard for the open archival information system, the ISO16363 standard for trustworthy repository assessment checklist, the ISO20652 standard for the Producer-Archive Interface Methodology Abstract Standard, among others.
Notes	Examples of evidence to demonstrate this can be documentation of the analysis of relevant standards for the organization, documentation of the analysis of a specific standard for the organization, plans on adopting measures from relevant standards, documentation of adopted measures from relevant standards.
Terms	-
Answers	No: There is no compliance assessment with relevant standards.
	Yes: Compliance assessment with relevant standards is performed.
Source	COBIT 4.1 – DS5 – Pages 117-120 [26]

ID	M3.6
Title	Preservation Strategic Plan
Question	Is there a Preservation Strategic Plan?
Purpose	The purpose is to identify if there is a Preservation Strategic Plan that helps the organization make administrative decisions, shape policies, and allocate resources in order to successfully preserve its holdings. The strategic plan should be based on the organization's established mission, and on its

	defined values, vision and goals. Strategic plans typically cover a particular finite time period, normally in the 3-5 year range.
Notes	Examples of evidence to demonstrate this can be a Preservation Strategic Plan; meeting minutes; documentation of administrative decisions which have been made.
Terms	-
Answers	No: There is no Preservation Strategic Plan. Yes: There is a Preservation Strategic Plan.
Source	TRAC – Criterion 3.1.2 and 3.1.2.2 [43]

ID	M3.7
Title	History of the Changes to Procedures and Operations
Question	Is there an audit trail of the changes to operations and procedures of the organization?
Purpose	The purpose is to identify if the organization can provide an 'audit trail' through which stakeholders can identify and trace decisions.
Notes	Examples of evidence to demonstrate this can be file retention and disposal schedules and policies; copies of earlier versions of policies and procedures; minutes of meetings.
Terms	-
Answers	No: There is no audit trail of the changes to operations and procedures of the organization. Yes: There is an audit trail of the changes to operations and procedures of the organization.
Source	TRAC – Criterion 3.3.3 [43]

ID	M3.8
Title	Transparency and Accountability
Question	Are there transparency and accountability policies for actions related to the operation and management of the organization?
Purpose	The purpose is to identify if there is transparency in the organization, in the sense of being available to anyone who wishes to know, is the best assurance that the organization operates in accordance with accepted standards and practices.
Notes	Examples of evidence to demonstrate this can be reports of financial and technical audits and certifications; disclosure of governance documents, independent program reviews, and contracts and agreements with providers of funding and critical services.
Terms	-
Answers	No: There are no transparency and accountability policies for actions related to the operation and management of the organization. Yes: There are transparency and accountability policies for actions related to the operation and management of the organization.
Source	TRAC – Criterion 3.3.4 [43]

ID	M3.9
Title	Financial Practices and Procedures
Question	Does the organization have financial practices and procedures?
Purpose	The purpose is to identify if the organization can protect itself against malfeasance or other activity that might threaten its economic viability. Achieved by financial practices and procedures which are transparent, compliant with relevant accounting standards and practices, and audited by third parties in accordance with territorial legal requirements.
Notes	Examples of evidence to demonstrate this can be demonstrated dissemination requirements for business planning and practices; citations to or examples of accounting and audit requirements, standards, and practice; audited annual financial statements.
Terms	-

Answers	No: There are no financial practices or procedures.
	Yes: There are financial practices or procedures.
Source	TRAC – Criterion 3.4.2 [43]

ID	M3.10
Title	Financial risk, benefit, investment, and expenditure
Question	Are there procedures to analyse and report on financial risk, benefit, investment, and expenditure?
Purpose	The purpose is to identify if the organization can demonstrate that the organization has identified and documented these categories, and actively manages them, including identifying and responding to risks, describing and leveraging benefits, specifying and balancing investments, and anticipating and preparing for expenditures. (including assets, licenses, and liabilities).
Notes	Examples of evidence to demonstrate this can be a risk register; technology infrastructure investment planning documents; cost/benefit analyses; financial investment documents and portfolios; requirements for and examples of licenses, contracts, and asset management; evidence of revision based on risk analysis.
Terms	-
Answers	No: There are no procedures to analyse and report on financial risk, benefit, investment, and expenditure.
	Yes: There are procedures to analyse and report on financial risk, benefit, investment, and expenditure.
Source	TRAC – Criterion 3.4.3 [43]

ID	M3.11
Title	Change Management Process
Question	Is there a change management process that identifies changes to critical processes that potentially affect the organization's ability to comply with its mandatory responsibilities?
Purpose	The purpose is to identify if the organization can document not only the current processes, but the prior processes that were applied to its holdings.
Notes	Examples of evidence to demonstrate this can be documentation of change management process; assessment of risk associated with a process change; analysis of the expected impact of a process change; comparison of logs of actual changes to processes versus associated analyses of their impact and criticality.
Terms	-
Answers	No: There is no change management process that identifies changes to critical processes that potentially affect the organization's ability to comply with its mandatory responsibilities.
	Yes: There is a change management process that identifies changes to critical processes that potentially affect the organization's ability to comply with its mandatory responsibilities.
Source	TRAC – Criterion 5.1.1.6.1 [43]

ID	M3.12
Title	Contracts and deposit agreements
Question	Are there procedures to acquire and maintain appropriate contracts or deposit agreements for information objects that it manages, preserves, and/or to which it provides access?
Purpose	The purpose is to identify if the organization can ensure that it has the rights and authorizations needed to enable it to collect and preserve information objects over time, make that information available to its Designated Community, and defend those rights when challenged.
Notes	Examples of evidence to demonstrate this can be Properly signed and executed deposit agreements and licenses in accordance with local, national, and international laws and regulations; policies on third-party deposit arrangements; definitions of service levels and permitted uses;

	policies on the treatment of 'orphan works' and copyright dispute resolution; reports of independent risk assessments of these policies; procedures for regularly reviewing and maintaining agreements, contracts, and licenses.
Terms	-
Answers	No: There are no procedures to acquire and maintain appropriate contracts or deposit agreements for information objects that it manages, preserves, and/or to which it provides access.
	Yes: There are procedures to acquire and maintain appropriate contracts or deposit agreements for information objects that it manages, preserves, and/or to which it provides access.
Source	TRAC – Criterion 3.5.1 [43]

ID	M4.1
Title	Business Planning Processes
Question	Are there short and long-term business planning processes in place?
Purpose	The purpose is to identify if the organization performs a business planning process which can be used to ensure the viability of the organization over the period it has promised to provide access to its contents for its Designated Community.
Notes	Examples of evidence to demonstrate this can be up-to-date, multi-year strategic, operating or business plans; audited annual financial statements; financial forecasts with multiple budget scenarios; contingency plans; market analysis.
Terms	Designated Community (http://evoc.sysresearch.org/E-ARK/OAIS/Designated%20Community)
Answers	No: There are neither short nor long-term business planning processes in place.
	Yes: There are short and long-term business planning processes in place.
Source	TRAC – Criterion 3.4.1 [43]

ID	M4.2
Title	Critical Processes
Question	Is there an identification of the critical processes of the organization?
Purpose	The purpose is to identify if the critical processes can be monitored to ensure that they continue to meet the mandatory responsibilities and to ensure that any changes to those processes are examined and tested.
Notes	An example of evidence to demonstrate this is a traceability matrix between processes and mandatory requirements.
Terms	-
Answers	No: There is no identification of the critical processes of the organization.
	Yes: There is an identification of the critical processes of the organization.
Source	TRAC – Criterion 5.1.1.6 [43]

ID	M5.1
Title	Continuous improvement
Question	Is continuous improvement of information governance implemented by the organization as part of the organizational culture?
Purpose	The purpose is to identify if the organization is always striving for continuous improvement of their management policies and procedures, as well as, skills and other relevant aspects of management.
Notes	Examples of evidence to demonstrate this can be the outputs of management review, corrective action and preventive action processes. However, if all the analysis, correcting and reviewing doesn't result in changes, then there is no improvement.
Terms	-
Answers	No: Continuous improvement of information governance is not implemented by the organization as part of the organizational culture.

	Yes: Continuous improvement of information governance is implemented by the organization as part of the organizational culture.
Source	COBIT 4.1 – Page 21 [26]

ID	M5.2
Title	Organization recognition among the community
Question	Is there a publication or outreach and marketing plan for the organization outputs?
Purpose	The purpose is to identify if peers recognize the organization as a good example of information governance through the dissemination of implemented procedures and innovative approaches to information governance.
Notes	When an organization is recognized among its community for its innovative and outstanding practice of information governance this means that their practices are potentially high calibre and are continuously improving. This can be achieved through the publication of papers, keynote presentation invitations, journal articles, among other examples.
Terms	-
Answers	No: There is no publication or outreach and marketing plan for the organization outputs.
	Yes: There is a publication or outreach and marketing plan for the organization outputs.
Source	COBIT 4.1 – Page 21 [26]

5.3. Processes

This section details the questions used in the self-assessment to calculate the maturity levels for the processes dimension.

5.3.1. Pre-Ingest

“The Pre-ingest process covers the Producer’s and archivist’s activities of creating Submission Information Packages (SIP).” [58]

ID	P2.1
Title	Deposit Terms Negotiation
Question	Is there a procedure to negotiate the terms of deposit between the Producer and the Archive?
Purpose	The purpose is to identify if the Archive can negotiate the terms of deposit with Producers. Terms of deposit might include the specification of the metadata that must be included at the time of deposit, the schedule and method of deposit, the responsibilities of the Producer and the Archive regarding the information being ingested, among other examples.
Notes	An example of evidence to demonstrate is the documentation of the procedure to negotiate the terms of deposit between the Producer and the Archive.
Terms	-
Answers	No: There is no procedure to negotiate the terms of deposit
	Yes: There is a procedure to negotiate the terms of deposit
Source	E-ARK Deliverable 2.1 – Page 19 of 41 [58]

ID	P3.1
Title	Producer SIP Validation
Question	Does the Archive validate if the Producer SIP complies with the defined format and structure specifications?

Purpose	The purpose is to identify if the Archive validates the Producer SIP regarding format and structure. If the SIP has deviations the Archive might reject the SIP and request the Producer to deliver a corrected SIP.
Notes	Examples of evidence to demonstrate this can be the logs of the validation procedures; documentation of the validation procedures, among others.
Terms	Producer SIP (http://evoc.sysresearch.org/E-ARK/D7.2/Producer%20SIP)
Answers	No: The Producer SIP is not validated. Yes: The Producer SIP is validated.
Source	E-ARK Deliverable 2.1 – Page 19 of 41 [58]

ID	P3.2
Title	Provenance verification procedures
Question	Are there procedures in place to verify the provenance of all deposited objects?
Purpose	The purpose is to identify if the organization has mechanisms to guarantee the provenance of the information to be Ingested.
Notes	Examples of procedures in place to verify this can be digital processing and data verification and validation, and through exchange of ownership evidences (e.g. submission agreements, deposit agreements, etc.).
Terms	-
Answers	No: There are no procedures in place to verify the provenance of all deposited objects. Yes: There are procedures in place which are or have been used to verify the provenance of some collections of deposited objects.
Source	TRAC – Criterion 4.1.4 [43]

ID	P3.3
Title	Enhancement of the Producer SIP
Question	Is there a procedure to enhance a Producer SIP?
Purpose	The purpose is to identify if a Producer SIP is checked and completed. This can be done by adding further metadata, or restructure the SIP, among other procedures.
Notes	Examples of evidence to demonstrate this can be the outputs of the enhancement of the Producer SIP; documentation detailing the enhancement procedures in place; a comparison between the original producer SIP and the enhanced one, among others.
Terms	-
Answers	No: The Producer SIP is not enhanced. Yes: The Producer SIP is enhanced.
Source	E-ARK Deliverable 2.1 – Page 19 of 41 [58]

5.3.2. Ingest

“The Ingest process covers archival activities of creating the archival information package (AIP) from the submission information package (SIP).” [58]

ID	P2.2
Title	Ingest Producer/depositor responses
Question	Is there a procedure to provide appropriate responses to the Producer, at the agreed points, during the Ingest process?
Purpose	The purpose is to identify if the organization provides responses to the Producer at the agreed points to ensure that there are no faults in communication that might lead to loss of a SIP.

Notes	Examples of evidence to demonstrate this can be submission or deposit agreements, process documentation, operating procedures, or evidence of responses such as reports, memos, or emails.
Terms	-
Answers	No: There is no procedure to provide appropriate responses to the Producer/depositor, at the agreed points, during the Ingest process Yes: There is a procedure to provide appropriate responses to the Producer/depositor, at the agreed points, during the Ingest process
Source	TRAC – Criterion 4.1.7 [43]

ID	P2.3
Title	AIP generation procedure
Question	Is there a procedure to generate an AIP from a SIP?
Purpose	The purpose is to identify if the organization can generate and AIP from a SIP. The organization must ensure that the AIP correctly represents the SIP.
Notes	-
Terms	-
Answers	No: There is no procedure to generate an AIP from a SIP. Yes: There is a procedure to generate an AIP from a SIP.
Source	TRAC – Criterion 4.2.2 [43]

ID	P2.4
Title	AIP unique identifiers convention
Question	Is there a procedure to generate and manage persistent and unique identifiers for an AIP?
Purpose	The purpose is to identify if the organization generates persistent, unique identifier for each AIP so that an IAP can be found in the future. This also ensures that an AIP can be distinguished from all other AIP in the repository. Understand if the organization has records that detail how changes to unique identifiers are to be performed so that AIP don't lose context, are not lost and can be distinguished from all other AIP in the repository.
Notes	Examples of evidence to demonstrate this can be documentation describing naming conventions and physical evidence of its application (e.g., logs).
Terms	-
Answers	No: There is no procedure to generate and manage persistent and unique identifiers for an AIP. Yes: There is a procedure to generate and manage persistent and unique identifiers for an AIP.
Source	TRAC – Criterion 4.2.4 [43]

ID	P3.4
Title	Management of units of description
Question	Is there a procedure to create and manage units of description based on the Producer SIP?
Purpose	The purpose is to identify if the Archive can manage units of description based on the Producer SIP information, or if reuses existing ones for scoping the new SIP.
Notes	An example of evidence to demonstrate this can be the documentation detailing how units of description are managed.
Terms	-
Answers	No: There is no procedure to manage units of description. Yes: There is a procedure to manage units of description based on the Producer SIP.
Source	E-ARK Deliverable 2.1 – Page 19 of 41 [58]

ID	P3.5
Title	Ingest SIP verification mechanisms
Question	During the Ingest process, are there mechanisms to verify that each SIP is complete and correct?
Purpose	The purpose is to identify if the organization has mechanisms to detect and correct errors during the creation of a SIP or of transmission errors during an Ingest session.
Notes	SIP completeness and correctness depends on what was agreed between the Producer and the Archive during the submission agreement negotiations. A SIP is correct if it complies with the schema that was defined. A SIP is complete if all information deemed mandatory in the submission agreement is present in it. Examples of mechanisms in place to verify this can be system log files from systems performing the transfer and Ingest procedures.
Terms	-
Answers	No: There are no mechanisms in place to verify that each SIP is complete and correct.
	Yes: There are mechanisms in place to verify that each SIP is complete and correct.
Source	TRAC – Criterion 4.1.5 [43]

ID	P3.6
Title	Ingest actions and administration processes records
Question	Does the Archive produce records of the Ingest transactions between Producer and Archive to serve as evidence of the transaction according to its legal and regulatory environment?
Purpose	The purpose is to identify if the organization has the updated records of all documentation relevant for the Ingest process which may be solicited during an audit.
Notes	Examples of evidence to demonstrate this can be written documentation of decisions and/or action taken, preservation metadata logged, stored, and linked to pertinent digital objects, and confirmation receipts sent back to Producers.
Terms	-
Answers	No: There are no records to serve as evidence of the Ingest transactions between Producer and Archive.
	Yes: There are records to serve as evidence of the Ingest transactions between Producer and Archive.
Source	TRAC – Criterion 4.1.8 [43]

ID	P3.7
Title	Legal Rights
Question	Is there a procedure to manage legal rights during Ingest?
Purpose	The purpose is to identify if the Archive can manage the legal rights (copyright, data protection, and ownership) of objects during Ingest into the Archive. In this sense managing legal rights involves checking if the content being ingested has legal rights associated; check if the content is not duplicated from previous ingests or even plagiarized from other Producers. It also includes creating access restrictions to certain objects when the producer requests it.
Notes	Examples of evidence to demonstrate this can be Legally binding submission agreements/deposit agreements/deeds of gift, evidence of appropriate technological measures; logs from procedures and authentications, among others.
Terms	-
Answers	No: There is no procedure to manage legal rights during Ingest.
	Yes: There is a procedure to manage legal rights during Ingest.
Source	Based on TRAC - Criteria 4.1.2, 4.1.4 and 4.1.6 [43]

ID	P3.8
-----------	------

Title	SIP final disposition documentation
Question	Are there procedures capable of demonstrating the final disposition of a SIP?
Purpose	The purpose is to identify if the organization has defined procedures to demonstrate that a specific SIP has either accepted, incorporated as part of an AIP, or been rejected and disposed.
Notes	Examples of evidence to demonstrate this can be system processing files, disposal records, deposit agreements, provenance tracking system, system log files, process description documents, and documentation of how an AIP is derived from a SIP.
Terms	-
Answers	No: There is no procedure capable of demonstrating the final disposition of a SIP.
	Yes: There are procedures capable of demonstrating the final disposition of a SIP.
Source	TRAC – Criterion 4.2.3 [43]

ID	P3.9
Title	AIP parsing
Question	Is there a procedure to create and manage AIP Classes?
Purpose	The purpose is to identify if the organization can store a wide variety of information types and create AIP classes to describe AIPs that store the same type of information. The AIP classes are important to understand the variety of information that is stored and to enable correct parsing of all information stored in the Archive.
Notes	Examples of evidence to demonstrate this can be documentation clearly linking each AIP, or class of AIP, to its definition.
Terms	AIP Class (http://evoc.sysresearch.org/E-ARK/D7.2/AIP%20Class)
Answers	No: There is no procedure to create and manage AIP Classes.
	Yes: There is a procedure to create and manage AIP Classes.
Source	TRAC – Criterion 4.2.1 [43]

ID	P3.10
Title	Preservation Description Information (PDI) acquiring procedures (from a SIP)
Question	Are there procedures for acquiring Preservation Description Information (PDI), from the SIP?
Purpose	The purpose is to identify if the organization has defined procedures to ensure that the PDI is associated with the relevant content information. This will support authenticity of the preserved objects and enable the detection of unauthorized changes.
Notes	Examples of evidence to demonstrate this can be operating procedures, documentation of the Ingest process, and documentation on how the repository acquires and manages Preservation Description Information (PDI).
Terms	Preservation Description Information (http://evoc.sysresearch.org/E-ARK/OAIS/Preservation%20Description%20Information) Content Information (http://evoc.sysresearch.org/E-ARK/OAIS/Content%20Information)
Answers	No: There are no procedures for acquiring Preservation Description Information (PDI), from the SIP.
	Yes: There are procedures for acquiring Preservation Description Information (PDI), from the SIP.
Source	TRAC – Criterion 4.2.6 [43]

ID	P3.11
Title	Preservation Description Information (PDI) maintaining procedures
Question	Are there procedures for maintaining Preservation Description Information (PDI) in the Archive?
Purpose	The purpose is to identify if the organization has defined procedures to ensure that the PDI is maintained through its life cycle. This includes performing changes in the PDI as result from external requirements changes.

Notes	Examples of evidence to demonstrate this can be operating procedures, documentation of the Ingest process, and documentation on how the repository acquires and manages Preservation Description Information (PDI).
Terms	Preservation Description Information (http://evoc.sysresearch.org/E-ARK/OAIS/Preservation%20Description%20Information) Content Information (http://evoc.sysresearch.org/E-ARK/OAIS/Content%20Information)
Answers	No: There are no procedures for maintaining Preservation Description Information (PDI) in the Archive. Yes: There are procedures maintaining Preservation Description Information (PDI) in the Archive.
Source	Based on TRAC – Criterion 4.2.6.2 [43]

ID	P3.12
Title	AIP content information testing procedure
Question	Is there a procedure for testing if the content information of the AIP at its creation is understandable by the designated communities?
Purpose	The purpose is to identify if the organization has a procedure for testing if the content information of the AIP at its creation is understandable by the designated communities so that all Ingested objects are deemed relevant and usable by the designated community.
Notes	Examples of evidence to demonstrate this can be test procedures to be run against the digital holdings to ensure that they are understandable by the defined Designated Community, availability of staff with the discipline expertise.
Terms	Content Information (http://evoc.sysresearch.org/E-ARK/OAIS/Content%20Information)
Notes	-
Answers	No: There is no procedure for testing if the content information of the AIP at its creation is understandable by the designated communities. Yes: There is a procedure for testing if the content information of the AIP at its creation is understandable by the designated communities.
Source	TRAC – Criterion 4.2.7 [43]

ID	P3.13
Title	AIP completeness and correctness
Question	Is each AIP verified for completeness and correctness at the point it is created?
Purpose	The purpose is to identify if the organization verifies the completeness and correctness of each AIP when it is created to ensure that all AIP can be traced back to the SIP provided by Producers.
Notes	AIP completeness and correctness is not universal and depends on what was agreed between the Producer and Archive during the submission agreement negotiations. An AIP is correct if it complies with the schema that was defined. A SIP is complete if all information necessary to understand, identify and retrieve the AIP is present. Examples of evidence to demonstrate this can be a description of the procedure that verifies completeness and correctness of the AIP and logs of the procedure.
Terms	-
Notes	-
Answers	No: An AIP is not verified for completeness and correctness at the point it is created. Yes: There is a procedure to verify each AIP for completeness and correctness at the point they are created.
Source	TRAC – Criterion 4.2.8 [43]

ID	P3.14
Title	AIP creation records

Question	Does the Ingest process produces records, according to their legal and regulatory environment, to serve as evidence of the actions performed to create an AIP?
Purpose	The purpose is to identify if the organization has records, according to their legal and regulatory environment, to serve as evidence of the actions performed to create an AIP, as to ensure that nothing is omitted from AIP records which might be needed to verify that all AIP have been properly created and in accordance with the documented procedures.
Notes	Examples of evidence to demonstrate this can be documentation of decisions and/or action taken with timestamps; preservation metadata logged, stored, and linked to relevant digital objects.
Terms	-
Answers	No: There are no records, according to their legal and regulatory environment, to serve as evidence of the actions performed to create an AIP.
	Yes: There are records, according to their legal and regulatory environment, to serve as evidence of the actions performed to create an AIP.
Source	TRAC – Criterion 4.2.10 [43]

5.3.3. Archival Storage and Preservation

“The Archival Storage Functional Entity contains the services and functions used for the storage and retrieval of Archival Information Packages.” [44]

ID	P2.5
Title	AIP Storage Procedures
Question	Are there procedures to define how the AIP is stored down to the bit level?
Purpose	The purpose is to identify if there are procedures that define how the AIP is stored down to the bit level, that ensure that information can be extracted from an AIP.
Notes	Examples of evidence to demonstrate this can be documentation of the format of the AIP, Data Entity Dictionary Specification Language descriptions of the data components, number of copies, security measures, and technical documentation of the archival procedures.
Terms	-
Answers	No: There are no procedures to define how the AIP is stored down to the bit level.
	Yes: There are procedures to define how the AIP is stored down to the bit level.
Source	TRAC – Criterion 4.4.1 [43]

ID	P2.6
Title	AIP actions records
Question	Does the archival process produces records, according to their legal and regulatory environment, to serve as evidence of the actions performed during storage and preservation of the AIP?
Purpose	The purpose is to identify if there are records, according to their legal and regulatory environment, to serve as evidence of the actions performed during storage and preservation of the AIP, to ensure that documentation is up to date, valid and authentic.
Notes	Examples of evidence to this can be documentation of decisions and actions taken, preservation metadata logged, stored, and linked to pertinent digital objects.
Terms	-
Answers	No: There are no AIP actions records.
	Yes: There are AIP actions records.
Source	TRAC – Criterion 4.4.2 [43]

ID	P2.7
Title	AIP Linking/resolution services

Question	Is there a system of reliable linking/resolution services to find a uniquely identified object, regardless of its physical location?
Purpose	The purpose is to identify if the organization has a system of reliable linking/resolution services to find a uniquely identified object, regardless of its physical location so that all actions related to an AIP can be traced over time, system and storage changes.
Notes	Examples of evidence to demonstrate this can be documentation describing naming convention and physical evidence of its application (e.g., logs).
Terms	-
Answers	No: There is no system of reliable linking/resolution services to find a uniquely identified object, regardless of its physical location.
	Yes: There is a system of reliable linking/resolution services to find a uniquely identified object, regardless of its physical location.
Source	TRAC – Criterion 4.2.4.2 [43]

ID	P3.15
Title	AIP integrity monitoring
Question	Is the integrity of an AIP monitored?
Purpose	The purpose is to identify if AIP integrity is monitored, which is necessary to protect the integrity of an AIP over time.
Notes	Examples of evidence to this can be checksums for each Ingested AIP; logs of checksum checks, documentation of how AIP and integrity information are kept separate, documentation of how AIP and access registers are kept separate.
Terms	-
Answers	No: The integrity of an AIP is not monitored.
	Yes: The integrity of an AIP is monitored.
Source	TRAC – Criterion 4.4.1.2 [43]

ID	P3.16
Title	AIP Designated Community Requirements
Question	Is there a procedure to gather and review the AIP requirements from the designated community?
Purpose	The purpose is to identify if there is a procedure to gather and review the AIP requirements from the designated community.
Notes	Examples of evidence to demonstrate this can be written documentation on how to engage with the designated community and extract new requirements.
Terms	-
Answers	No: There is no procedure to gather and review the AIP requirements from the designated community.
	Yes: There is a procedure to gather and review the AIP requirements from the designated community.
Source	Based on TRAC – Criterion 4.5.1 and OAIS – Page 4-14 [43] [44]

ID	P3.17
Title	Independent mechanism for content integrity checking
Question	Is there an independent mechanism for verifying the integrity of the Archives' content?
Purpose	The purpose is to identify if the organization has mechanism for content integrity checking that enables independent audits.
Notes	Examples of evidence to demonstrate this can be logs of material received and associated action (e.g., receipt, action) dates, logs of periodic checks.
Terms	-

Answers	No: There is no independent mechanism for verifying the integrity of the Archives' content.
	Yes: There is an independent mechanism for verifying the integrity of the Archives' content.
Source	TRAC – Criterion 4.2.9 [43]

ID	P3.18
Title	Tools and resources to provide representation information
Question	Are there tools and resources to generate Representation Information for the digital objects in the Archive?
Purpose	The purpose is to identify if the organization has tools or methods to identify the file type of all submitted objects, to determine what other more representation information is necessary to make each object understandable, and the ability to ensure that all that Representation information is associated with the relevant objects.
Notes	Examples of evidence to demonstrate this can be subscription or access to registries of representation information (e.g., format registries); records in local registries with links to digital objects, database records that include representation information and a link to relevant digital objects.
Terms	Representation Information (http://evoc.sysresearch.org/E-ARK/OAIS/Representation%20Information)
Answers	No: There are no tools or resources to provide Representation Information for all the digital objects in the Archive.
	Yes: There are tools or resources to provide Representation Information for all the digital objects in the Archive.
Source	Based on TRAC – Criterion 4.2.5.4 [43]

5.3.4. Data Management

“According to the OAIS model Data Management is a collection of independent processes that aim to manipulate the descriptive metadata (and in some implementations the inner structure of the AIP) theoretically resulting in a new manifestation or new version of the AIP.” [58]

ID	P3.19
Title	Designated Community information requirements
Question	Are the minimum information requirements specified to enable the Designated Community to discover and identify material of interest?
Purpose	The purpose is to identify if the Archive enables discovery of its holdings.
Notes	Examples of evidence to demonstrate this can be retrieval and descriptive information, discovery metadata, such as Dublin Core, and other documentation describing the objects.
Terms	-
Answers	No: The minimum information requirements are not specified.
	Yes: The minimum information requirements are specified.
Source	TRAC – Criterion 4.5.1 [43]

ID	P3.20
Title	Descriptive information association with the AIP
Question	Is the minimum descriptive information captured or created and associated with the AIP?
Purpose	The purpose is to identify if the Archive ensures that descriptive information is associated with the AIP. The archive must evidence that it associates with each AIP, the minimum descriptive

	information that was received from the producer or created by the archive. Associating the descriptive information with the AIP is important, although it does not require one-to-one correspondence, and may not necessarily be stored with the AIP. Hierarchical schemes can allow some descriptive information to be associated with many AIP.
Notes	Examples of evidence to demonstrate this can be descriptive metadata; internal or external persistent, unique identifier or locator that is associated with the AIP; system documentation and technical architecture; depositor agreements; metadata policy documentation; process workflow documentation.
Terms	Descriptive Information (http://evoc.sysresearch.org/E-ARK/OAIS/Descriptive%20Information)
Answers	No: The minimum descriptive information is neither captured or created nor associated with the AIP.
	Yes: The minimum descriptive information is captured or created and associated with the AIP.
Source	TRAC – Criterion 4.5.2 [43]

ID	P3.21
Title	Bi-directional linkage between the AIP and descriptive information
Question	Is there a procedure to maintain bi-directional linkage between each AIP and its descriptive information?
Purpose	The purpose is to identify if the Archive ensures that all AIP can be located and retrieved. An archive must have procedures on how to establish and maintain relationships between the descriptive information and the AIP, and should ensure that every AIP has descriptive information associated with it and that all descriptive information must point to at least one AIP.
Notes	Examples of evidence to demonstrate this can be descriptive metadata; unique, persistent identifier or locator associated with the AIP; documented relationship between the AIP and its metadata; system documentation and technical architecture; process workflow documentation.
Terms	Descriptive Information (http://evoc.sysresearch.org/E-ARK/OAIS/Descriptive%20Information)
Answers	No: There is no procedure to maintain bi-directional linkage between each AIP and its descriptive information.
	Yes: There is a procedure to maintain bi-directional linkage between each AIP and its descriptive information.
Source	TRAC – Criterion 4.5.3 [43]

5.3.5. Access

“According to the OAIS model the Access process covers the activities of requesting and creating the Dissemination Information Package (DIP) from the AIP.” [58]

ID	P2.8
Title	Creation of a DIP
Question	Is there a procedure to create a DIP from an AIP?
Purpose	The purpose is to identify if there is a procedure to create a DIP from an AIP.
Notes	Examples of evidence to demonstrate this can be the outputs of the procedure to generate a DIP; documentation on the procedure to generate a DIP, among others.
Terms	-
Answers	No: There is no procedure to create a DIP from an AIP.
	Yes: There is a procedure to create a DIP from an AIP.
Source	E-ARK Deliverable 2.1 – Page 35 of 41 [58]

ID	P3.22
-----------	-------

Title	Access policies
Question	Are there access policies defined with the designated communities?
Purpose	The purpose is to identify if the organization has access policies defined with the designated communities.
Notes	An example of evidence to demonstrate this can be documentation of policies that are available to the user communities.
Terms	-
Answers	No: There are no access policies defined with the designated communities.
	Yes: There are access policies defined with the designated communities.
Source	Based on TRAC – Criterion 4.6.1 [43]

ID	P3.23
Title	Access policies compliance
Question	Are there procedures to verify if the organization complies with the access policies defined with the designated communities?
Purpose	The purpose is to identify if the organization complies with access policies defined with the designated communities. Failure to comply might affect the trust that designated community has on the organization about the support of the user community.
Notes	Examples of evidence to demonstrate this can be documentation of policies that are available to the user communities, logs and audits of access requests.
Terms	-
Answers	No: There are no procedures to verify if the organization complies with the access policies defined with the designated communities.
	Yes: There are procedures to verify if the organization complies with the access policies defined with the designated communities.
Source	TRAC – Criterion 4.6.1 [43]

ID	P3.24
Title	Access failures and errors
Question	Is there a mechanism to log and review all access failures and errors?
Purpose	The purpose is to identify if the organization maintains a log and reviews all access failures and errors, which can help identify security threats and access system failures.
Notes	Examples of evidence to demonstrate this can be access logs, capability of the system to use automated analysis/monitoring tools and generate problem/error messages; notes of reviews undertaken or action taken because of reviews.
Terms	-
Answers	No: There is no mechanism to log and review access failures and errors.
	Yes: There is a mechanism to log and review all access failures and errors.
Source	TRAC – Criterion 4.6.1.1 [43]

ID	P3.25
Title	Access Data Reports
Question	Is there a mechanism to record the access to the contents?
Purpose	The purpose is to identify if the organization records access to the contents, as a measure to detect abuses or misuses.
Notes	An example of evidence to demonstrate this can be process definitions or logs of access orders.
Terms	Consumer (http://evoc.sysresearch.org/E-ARK/OAIS/Consumer)
Answers	No: There is no mechanism to record the access to the contents.
	Yes: There is a mechanism to record the access to the contents.

Source	Based on TRAC – Criterion 4.6.1.1 [43]
---------------	--

ID	P3.26
Title	Access Data Problem/Error Reports
Question	Is there a mechanism to solve problem reports about errors in data or responses from Consumers?
Purpose	The purpose is to identify if the organization investigates and resolves both incident and problem reports about errors in data or responses from Consumers essential to become a trustworthy source of information.
Notes	Examples of evidence to demonstrate this can be system design documents, work instructions (if a DIP involves manual processing), process definitions, documentation of the actions taken.
Terms	Consumer (http://evoc.sysresearch.org/E-ARK/OAIS/Consumer)
Answers	No: There is no mechanism to solve problem reports about errors in data or responses from Consumers.
	Yes: There is a mechanism which focuses only on incident reports about errors in data or responses from Consumers but does not seek to identify and resolve underlying issues.
Source	TRAC – Criterion 4.6.2.1 [43]

ID	P3.27
Title	Access Policies and Procedures
Question	Does the organization have records of policies and procedures that enable the dissemination of digital objects while maintaining traceability to the originals and evidence supporting their authenticity?
Purpose	The purpose is to identify if the organization maintains an auditable chain of authenticity from the AIP to a DIP.
Notes	Examples of evidence to demonstrate this can be system design documents, work instructions (if a DIP involve manual processing), process definitions, production of a sample copy with evidence of authenticity, documentation of the designated community requirements for evidence of authenticity; PREMIS Events.
Terms	-
Answers	No: There are no records of policies and procedures that enable the dissemination of digital objects while maintaining traceability to the originals and evidence supporting their authenticity.
	Yes: There are records of policies and procedures that enable the dissemination of digital objects while maintaining traceability to the originals and evidence supporting their authenticity.
Source	TRAC – Criterion 4.6.2 [43]

5.4. Infrastructure

This section details the questions used in the self-assessment to calculate the maturity levels for the infrastructure dimension.

ID	I2.1
Title	Archival infrastructure management
Question	Are there archival infrastructure management procedures in place?
Purpose	The purpose is to identify if the organization manages the infrastructure that supports its business.
Notes	Examples of evidence to demonstrate this can be a collection of all the infrastructure management procedures, documentation of the identified infrastructure management procedures, examples of application of the documented procedures.
Terms	-
Answers	No: The infrastructure is not managed.

	Yes: The infrastructure is managed using defined infrastructure management procedures.
Source	COBIT 4.1 – A12 - Pages 77-80 [26]

ID	I2.2
Title	Information Objects Location and Quantity
Question	Are there procedures to manage the number and location of copies of all Information objects?
Purpose	The purpose is to identify if the organization can assert that it is providing an authentic copy of a particular information object.
Notes	Examples of evidence to demonstrate this can be Random retrieval tests; validation of object existence for each registered location; validation of a registered location for each object on storage systems; provenance and fixity checking information; location register/log of information objects compared to the expected number and location of copies of particular objects.
Terms	-
Answers	No: There are no procedures to manage the number and location of copies of all Information objects.
	Yes: There are procedures to manage the number and location of copies of all Information objects.
Source	TRAC – Criterion 5.1.2 [43]

ID	I2.3
Title	Synchronization Mechanisms
Question	Are there mechanisms in place to ensure any/multiple copies of information objects are synchronized?
Purpose	The purpose is to identify if the organization can ensure that multiple copies of an information object remain identical, within a time established as acceptable by the organization, and that a copy can be used to replace a corrupted copy of the object.
Notes	Examples of evidence to demonstrate this can be Synchronization workflows; system analysis of how long it takes for copies to synchronize; procedures/documentation of synchronization processes.
Terms	-
Answers	No: There are no mechanisms in place to ensure any/multiple copies of information objects are synchronized.
	Yes: There are mechanisms in place to ensure any/multiple copies of information objects are synchronized.
Source	TRAC – Criterion 5.1.2.1 [43]

ID	I3.1
Title	Infrastructure changes
Question	Are infrastructure changes addressed in the organization?
Purpose	The purpose is to identify how the infrastructure is upgraded and maintained so that it continues to remain operational and meet the customers' requirements.
Notes	Examples of evidence to demonstrate this can be documentation on the procedure to address infrastructure changes in the organization; documentation on infrastructure changes that resulted from the application of the procedure, among others.
Terms	-
Answers	No: There are no procedures to address infrastructure changes.
	Yes: There are procedures to address infrastructure changes.
Source	COBIT 4.1 – A12 - Pages 77-80 [26]

ID	I3.2
Title	Infrastructure security procedures
Question	Are there infrastructure security procedures implemented in the organization?
Purpose	The purpose is to identify if the organization has security procedures for the infrastructure and how these procedures are implemented.
Notes	An example of evidence to demonstrate this can be a set of indicators defined that are used to measure the performance of the infrastructure security procedures in place. These indicators can then be measured through automatic means which works by defining a threshold value that when is reached automatically alerts for a security event.
Terms	-
Answers	No: There are no infrastructure security procedures in place.
	Yes: There are infrastructure security procedures in place.
Source	COBIT 4.1 – A12 - Pages 77-80 [26]

ID	I3.3
Title	Technology watches/monitoring
Question	Are there technology watches/monitoring implemented in the organization?
Purpose	The purpose is to identify if the organization has mechanisms for technology watch/monitoring and how they are implemented in the organization.
Notes	Technology watches/monitoring works by identifying new technologies and technologies that are in risk of becoming obsolete. It also identifies conflicts between old and new version of a technology and advises possible courses of action to guarantee that the infrastructure remains available and relevant for the designated communities. Examples of evidence to demonstrate this can be management of periodic technology assessment reports; comparison of existing technology to each new assessment, among others.
Terms	-
Answers	No: There are no technology watches/monitoring implemented in the organization.
	Yes: There are technology watches/monitoring implemented in the organization.
Source	TRAC – Criterion 5.1.1.1 [43]

ID	I3.4
Title	Infrastructure risk management process
Question	Is there an infrastructure risk management process implemented?
Purpose	The purpose is to identify how risk management is performed in the organization.
Notes	A risk management process helps identifying and assessing risks, which in turn will help identifying controls to mitigate these risks.
Terms	-
Answers	No: There is no risk management process for the infrastructure of the organization.
	Yes: There is a risk management process for the infrastructure of the organization.
Source	COBIT 4.1 – PO9 - Pages 63-66 [26]

ID	I3.5
Title	Disaster preparedness and recovery plan
Question	Is there a disaster preparedness and recovery plan?
Purpose	The purpose is to identify if the organization maintains a suitable disaster preparedness and recovery plan(s).
Notes	The disaster preparedness and recovery plan(s) should include at least one off-site backup of all information together with an offsite copy of the recovery plan(s). Examples of evidence to demonstrate this can be evidence that the organization employs the codes of practice found in the

	ISO 27000 series of standards; disaster and recovery plans; information about and proof of at least one off-site copy of preserved information; service continuity plan; documentation linking roles with activities; local geological, geographical, or meteorological data or threat assessments; ISO 17799 certification, among others.
Terms	-
Answers	No: There is no disaster preparedness and recovery plan.
	Yes: There is a disaster preparedness and recovery plan developed.
Source	TRAC – Criterion 5.2.4 [43]

ID	I3.6
Title	History of the Changes to Software and Hardware
Question	Is there a history of the changes to software and hardware of the organization?
Purpose	The purpose is to identify if the organization can provide an ‘audit trail’ through which stakeholders can identify and trace decisions.
Notes	Examples of evidence to demonstrate this can be capital equipment inventories; documentation of the acquisition, implementation, update, and retirement of critical software and hardware; minutes of meetings.
Terms	-
Answers	No: There is no history of the changes to software and hardware of the organization.
	Yes: There is a history of the changes to software and hardware of the organization.
Source	TRAC – Criterion 3.3.3 [43]

ID	I3.7
Title	Preservation Policies
Question	Are there Preservation Policies in place to ensure the organization’s Preservation Strategic Plan will be met?
Purpose	The purpose is to identify if the organization can fulfil the part of its mission related to preservation.
Notes	Examples of evidence to demonstrate this can be Preservation Policies; Mission Statement; Current and past written documentation in the form of Preservation Policies, Preservation Strategic Plans and Preservation Implementation Plans, procedures, protocols, and workflows; specifications of review cycles for documentation; documentation detailing reviews, surveys and feedback. If documentation is embedded in system logic, functionality should demonstrate the implementation of policies and procedures.
Terms	-
Answers	No: There are no Preservation Policies in place to ensure the organization’s Preservation Strategic Plan will be met.
	Yes: There are Preservation Policies in place to ensure the organization’s Preservation Strategic Plan will be met.
Source	TRAC – Criterion 3.3.2 and 3.3.2.1 [43]

ID	I3.8
Title	Information Integrity Measurements
Question	Are there procedures to define, collect, track, and appropriately provide information integrity measurements?
Purpose	The purpose is to identify if the organization can provide documentation that it has developed or adapted appropriate measures for ensuring the integrity of its holdings.
Notes	Examples of evidence to demonstrate this can be written definition or specification of the organization’s integrity measures (for example, computed checksum or hash value);

	documentation of the procedures and mechanisms for monitoring integrity measurements and for responding to results of integrity measurements that indicate digital content is at risk; an audit process for collecting, tracking, and presenting integrity measurements; Preservation Policy and workflow documentation.
Terms	-
Answers	No: There are no procedures to define, collect, track, and appropriately provide information integrity measurements.
	Yes: There are procedures to define, collect, track, and appropriately provide information integrity measurements.
Source	TRAC – Criterion 3.3.5 [43]

ID	I3.9
Title	Intellectual Property Rights and Restrictions
Question	Are there procedures to track and manage intellectual property rights and restrictions on use of information?
Purpose	The purpose is to identify if the organization can track, act on, and verify rights and restrictions related to the use of the information within the organization, as required by deposit agreement, contract, or license.
Notes	Examples of evidence to demonstrate this can be Preservation Policy statement that defines and specifies the organization's requirements and process for managing intellectual property rights; depositor agreements; samples of agreements and other documents that specify and address intellectual property rights; documentation of monitoring by the organization over time of changes in status and ownership of intellectual property in digital content held by the organization; results from monitoring, metadata that captures rights information.
Terms	-
Answers	No: There are no procedures to track and manage intellectual property rights and restrictions on use of information.
	Yes: There are procedures to track and manage intellectual property rights and restrictions on use of information.
Source	TRAC – Criterion 3.5.2 [43]

ID	I4.1
Title	Infrastructure performance
Question	Is the infrastructure performance monitored in the organization?
Purpose	The purpose is to identify if the organization monitors the infrastructure performance.
Notes	Examples of evidence to demonstrate this can be a document detailing the collection of indicators used to measure infrastructure performance; examples of the application of these indicators to specific scenarios.
Terms	-
Answers	No: Infrastructure performance is not monitored in the organization.
	Yes: Infrastructure performance is monitored.
Source	COBIT 4.1 – A12 - Pages 77-80 [26]

5.5. General

This section details the general questions used to assess maturity levels 4 and 5 of A2MIGO. These questions are based on the process areas of CMMI [31] for maturity levels 4 and 5.

ID	G4.1
Title	Process quality and performance objectives.
Question	Are process quality and process performance objectives established and maintained?
Purpose	The purpose is to identify if objectives for quality and process performance are established and negotiated at an appropriate level of detail to permit an overall evaluation of the objectives and risks at the process level.
Notes	Process quality and performance objectives can be updated as the processes actual performance becomes known and more predictable, and to reflect changing needs and priorities of relevant stakeholders. This includes quality and process performance objectives, and assessment of the risk of not achieving the organizations' objectives.
Terms	-
Answers	No: There are no established and maintained process quality and process performance objectives. Yes: There are established and maintained process quality and process performance objectives.
Source	CMMI for Development 1.3– Quantitative Project Management [31]

ID	G4.2
Title	Measures and analytic techniques for quantitative management
Question	Is there a selection of measures and analytic techniques to be used in quantitative management?
Purpose	The purpose is to identify if the organization selects measures and analytic techniques to be used in quantitative management.
Notes	Examples of evidence to demonstrate this can be definitions of measures and analytic techniques to be used in quantitative management; traceability of measures back to the organizations' quality and process performance objectives; Process performance baselines and models for use by the organization.
Terms	-
Answers	No: There is no selection of measures and analytic techniques to be used in quantitative management. Yes: There is a selection of measures and analytic techniques to be used in quantitative management.
Source	CMMI for Development 1.3 – Quantitative Project Management [31]

ID	G4.3
Title	Process Performance Analysis
Question	Is Process Performance analysed?
Purpose	The purpose is to identify if the selected measures are analysed to characterize the performance of the organizations' processes.
Notes	Analyse the collected measures to establish a distribution or range of results that characterize the expected performance of the organizations' processes. This analysis should include the stability of the process, and the impacts of associated factors and context. Related factors include inputs to the process and other attributes that can affect the results obtained. The context includes the business context (e.g., domain).
Terms	-
Answers	No: Process Performance is not analysed. Yes: Process Performance is analysed.
Source	CMMI for Development 1.3 – Organizational Process Performance [31]

ID	G4.4
Title	Process Performance Baselines
Question	Are there Process Performance Baselines established?

Purpose	The purpose is to identify if process performance baselines are established and compared to the organization's quality and process performance objectives to determine if the quality and process performance objectives are being achieved.
Notes	The process performance baselines are a measurement of performance for the organization's set of standard processes at various levels of detail. The processes that the process performance baselines can address include the following: Sequence of connected processes; Processes that cover the entire lifecycle of information; Processes for developing specific outputs.
Terms	-
Answers	No: There are no Process Performance Baselines established.
	Yes: There are Process Performance Baselines established.
Source	CMMI for Development 1.3 – Organizational Process Performance [31]

ID	G5.1
Title	Potential Areas for Improvement
Question	Are potential areas for improvements identified?
Purpose	The purpose is to identify if the organization identifies potential areas for improvement that could contribute to meeting business objectives.
Notes	Potential areas for improvement are identified through a proactive analysis to determine areas that could address process performance shortfalls. Causal Analysis and Resolution processes can be used to diagnose and resolve root causes. The output from this activity is used to evaluate and prioritize potential improvements, and can result in either incremental or innovative improvement suggestions.
Terms	-
Answers	No: Potential areas for improvements are not identified.
	Yes: Potential areas for improvements are identified.
Source	CMMI for Development 1.3 – Organizational Performance Management [31]

ID	G5.2
Title	Select and Implement Improvements
Question	Are there procedures in place to select and implement improvements for deployment in the organization?
Purpose	The purpose is to identify if there is a selection and implementation of improvements for deployment throughout the organization based on an evaluation of costs, benefits, and other factors.
Notes	Selection of suggested improvements for deployment is based on cost-to-benefit ratios with regard to quality and process performance objectives, available resources, and the results of improvement proposal evaluation and validation activities. Examples of evidence to demonstrate this can be a list of improvements selected for deployment, and updated process documentation and training.
Terms	-
Answers	No: There are no procedures in place to select and implement improvements for deployment in the organization.
	Yes: There are procedures in place to select and implement improvements for deployment in the organization.
Source	CMMI for Development 1.3 – Organizational Performance Management [31]

ID	G5.3
Title	Improvement Effects Evaluation

Question	Are there procedures to evaluate the effects of improvements on quality and process performance?
Purpose	The purpose is to identify if the organization evaluates the effects of deployed improvements on quality and process performance using statistical and other quantitative techniques.
Notes	An example of evidence to demonstrate this can be the existence of documented measures of the effects resulting from deployed improvements.
Terms	-
Answers	No: There are no procedures to evaluate the effects of improvements on quality and process performance.
	Yes: There are procedures to evaluate the effects of improvements on quality and process performance.
Source	CMMI for Development 1.3 – Organizational Performance Management [31]

ID	G5.4
Title	Determine Causes of Selected Outcomes
Question	Is there a selection and analysis of outcomes to determine root causes?
Purpose	The purpose is to identify if the organization systematically determines the root causes of selected and analysed outcomes.
Notes	A root cause is an initiating element in a causal chain which leads to an outcome of interest. The selection of outcomes could be triggered by an event (reactive) or could be planned periodically, such as at the beginning of a new phase or task (proactive). The purpose of outcome analysis is to define actions that will address selected outcomes by analysing relevant outcome data and producing action proposals for implementation.
Terms	-
Answers	No: There is no selection and analysis of outcomes to determine root causes.
	Yes: There is selection and analysis of outcomes to determine root causes.
Source	CMMI for Development 1.3 – Causal Analysis and Resolution [31]

ID	G5.5
Title	Address Causes of Selected Outcomes
Question	Are action proposals implemented and its effects evaluated?
Purpose	The purpose is to identify if the organization implements and evaluates selected action proposals developed in causal analysis.
Notes	Action proposals describe tasks necessary to address root causes of analysed outcomes to prevent or reduce the occurrence or recurrence of negative outcomes, or incorporate realized successes. Action plans are developed and implemented for selected action proposals. Only changes that prove to be of value should be considered for broad implementation. Once the changed process is deployed, the effect of changes is evaluated to verify that the process change has improved process performance.
Terms	-
Answers	No: Action proposals are not implemented and its effects are not evaluated.
	Yes: Action proposals are implemented and its effects are evaluated.
Source	CMMI for Development 1.3 – Causal Analysis and Resolution [31]

6. Conclusions

This deliverable presents the E-ARK Maturity Model for Information Governance that follows a DSR development method and is based on requirements defined in relevant standards. This deliverable marks the final iteration of the E-ARK Maturity Model for Information Governance in the scope of the E-ARK project. However, further iteration can be performed as the domains built around Information Governance evolve.


6.1. Scope and Method


The E-ARK Maturity Model for Information Governance developed in this deliverable primarily focuses on Archival references namely the **Open archival information system – Reference model (OAIS/ISO14721)**, the **Trustworthy Repositories Audit and Certification (TRAC/ISO16363)** and the **Producer-Archive Interface Methodology Abstract Standard (PAIMAS/ISO20652)**.

This deliverable focuses on the second iteration of the first four stages of the development method (see section 3) that concentrate on the design and development of the maturity model, as presented in Table 10. To use this maturity model an organization first needs to position itself in the maturity matrix in each of the dimensions. This step is called self-assessment. The self-assessment consists of following a series of predetermined steps in which the organization answers a series of questionnaires that will result in the determination of a maturity level. This deliverable details the revision of the self-assessment questionnaire and contains the questions for all the dimensions of the maturity model. D7.6 will focus on the application of the self-assessment that will be used on the use cases after the project pilot. This constitutes the next three stages of the second iteration of the development method. Deliverable 7.6 will conduct a new self-assessment using the final version of the maturity model after the project pilot. Table 10 defines the focus of each deliverable based on the development method and represents the maturity model roadmap.

Table 10. Roadmap of the maturity model development and application according to project deliverables

Deliverable	Development Method Stages						
	Problem Definition	Comparison of existing maturity models	Determination of development strategy	Iterative maturity model development	Conception of transfer and evaluation	Implementation of transfer media	Evaluation
D7.1: A Maturity Model for Information Governance – initial version [Deliverable date: M12]							
D7.2: Initial Assessment and Evaluation [Deliverable date: M18]							
D7.5: A Maturity Model for Information Governance – final version [Deliverable date: M36]							
D7.6: Final Assessment and Evaluation [Deliverable date: M36]							

 To be used in the deliverable

 Focus of the deliverable

6.2. Changes from the first version of the Maturity Model

This section details the changes from the first version of the E-ARK Maturity Model for Information Governance. There are changes in several aspects of the maturity model as will be presented in detail.

- Information Governance Maturity Models

This section was previously one of the sections of the main document in D7.1. In this deliverable it was converted into an appendix (Appendix A) to ease the understanding of the main document and to focus on the E-ARK Maturity Model for Information Governance.

In the Risk Management Maturity models two new maturity models were added, the RIMS Risk Management Maturity Model and the Deloitte Risk Maturity Model. This is because the maturity model detailed in D7.1 (Hilson Risk Maturity Model) must be seen as an earlier example of a risk management maturity model which was developed before the publication of important risk management standards such as the ISO31100 family of standards. The Information Governance section was divided into several sections. There is a section for general information governance maturity models, another for data management, another for records management and finally a new section was added for Digital Preservation which now includes three maturity models, (1) Digital Preservation Capability Maturity Model, (2) Preservica Digital Preservation Maturity Model, and (3) Adrian Brown's Digital Preservation Maturity Model. This section was created as Digital Preservation is one of the aspects of information governance that is one of the focus domains of the E-ARK project and its importance is vital in the development of the maturity model presented in this deliverable.

- E-ARK Maturity Model for Information Governance

To facilitate the communication and presentation of the E-ARK Maturity Model for Information Governance an acronym was created, the acronym is A2MIGO (which can be spelled as “amigo”, and stands for “e-Ark Maturity Model for Information Governance”).

- A2MIGO Maturity Table

A figure representation of the overall maturity model was developed to facilitate the presentation of maturity model, depicted in section 4.5 as Figure 4. This image presents the maturity stages for information governance, as well as, the dimensions, some key aspects of each dimension and maturity level. Then, new sections (4.5.1 to 4.5.3) were added to describe in detail each dimension and maturity level. For each dimension, the aspects being evaluated are detailed and then for each maturity level the key aspects of that specific level are presented.

- A2MIGO Self-Assessment Questionnaire

The Self-assessment questionnaire detailed in D7.2 was revised according to the post-assessment results and other considerations that resulted from meetings and conferences presentations and workshops. In D7.2 one of the main issues with the assessment was that questions to assess the Management and Infrastructure dimensions were not detailed. In this deliverable the questions for the management and infrastructure dimensions were added to the self-assessment questionnaire. These questions will be used in the final assessment and evaluation of the E-ARK pilots.

References

- [1] R. L. Nolan, "Managing the Computer Resource: A Stage Hypothesis", *Communications of the ACM*, vol. 16, pp. 399-405, 1973.
- [2] C. F. Gibson, R. L. Nolan, "Managing the Four Stages of EDP Growth," *Harvard Business Review*, vol. 52, no. 1, pp. 76-88, 1974.
- [3] F. W. McFarlan, I. L. McKenney, "Corporate Information Systems Management," Homewood, 1983.
- [4] F. W. McFarlan, I. L. McKenney, P. Pyburn, "The information archipelago-Plotting the course," *Harvard Business Review*, vol. 61, no. 1, pp.145-156, 1982.
- [5] C. H. Sullivan, "Systems Planning in the Information Age", *Sloan Management Review*, vol. 26, no. 2, pp. 3-12, 1985.
- [6] M. J. Earl, "Management Strategies for Information Technology," Prentice-Hall, 1989.
- [7] M. J. Earl, "Approaches to Strategic Information Systems Planning Experience in Twenty-One United Kingdom Companies," In *Proceedings of the Eleventh International Conference on Information Systems*, 1990.
- [8] R.D. Galliers, A.R. Sutherland, "Information systems management and strategy formulation: the 'stages of growth' model revisited", *Journal of Information Systems*, vol. 1, no. 2, pp. 89-114, 1991.
- [9] Open Management Group, "Business Process Maturity Model (BPMM) - Version 1.0," 2008.
- [10] M. J. Melenovsky, J. Sinur, "BPM Maturity Model Identifies Six Phases for Successful BPM Adoption," Gartner, 2006.
- [11] J. Luftman, "Assessing Business-IT Alignment Maturity," In *Strategies for Information Technology Governance*, Idea Group Publishing, 2004.
- [12] F. Niessink, V. Clerc, H. Vliet, "The IT Service Capability Maturity Model," IT Service CMM Release L2+3-0.3, 2002.
- [13] D. Newman, D. Logan, "Gartner Introduces the EIM Maturity Model," Gartner, 2008.
- [14] M. Visconti, C. R. Cook, "Evolution of a maturity model - critical evaluation and lessons learned," *Software Quality Journal*, vol. 7, pp. 223-237, 1998.
- [15] J. Jacobs, J. Trienekens, "Towards a Metrics Based Verification and Validation Maturity Model," In *Proceedings of the 10th International Workshop on Software Technology and Engineering Practice*, pp. 123-128, 2002.
- [16] I. Sommerville, "Software Engineering - 9th Edition," Addison Wesley, Reading, MA, 2010.
- [17] J. Lee, D. Lee, S. Kang, "An overview of the Business Process Maturity Model (BPMM)," In *Proceedings of the APWeb/WAIM 2007 International Workshops*, pp. 384-395, 2007.
- [18] E. Rios, T. Bozheva, A. Bediaga, N. Guilloreau, "MDD Maturity Model: A Roadmap for Introducing Model-Driven Development," In *Proceedings of the Second European Conference ECMDA-FA 2006*, pp. 78-89, 2006.
- [19] D Hillson, "Towards a Risk Maturity Model," *The International Journal of Project & Business Risk Management*, vol. 1, no. 1, pp. 35-45, 1997.. A.
- [20] Stanford University, "Data Governance Maturity Model." [Online]. Available: <http://web.stanford.edu/dept/pres-provost/cgi-bin/dg/wordpress/>
- [21] T. Lei, A. Ligtoet, L. Volker, P. Herder, "Evaluating Asset Management Maturity in the Netherlands: A Compact Benchmark of Eight Different Asset Management Organizations," In *Proceedings of the 6th World Congress of Engineering Asset Management*, 2011.
- [22] JISC InfoNet, "Records Management Maturity Model." [Online]. Available: <http://www.jiscinfonet.ac.uk/tools/maturity-model/>
- [23] Real Story Group, DAM Foundation, "The DAM Maturity Model." [Online]. Available: <http://dammaturitymodel.org/>
- [24] A. Pelz-Sharpe, A. Durga, D. Smigiel, E. Hartmen, T. Byrne, J. Gingras, "Ecm Maturity Model - Version 2.0," Wipro - Real Story Group - Hartman, 2010.
- [25] ARMA International, "Generally Accepted Recordkeeping Principles - Information Governance Maturity Model." [Online]. Available: <http://www.arma.org/principles>
- [26] IT Governance Institute, "COBIT 4.1 – Framework, Control Objectives, Management Guidelines, Maturity Models," 2007.
- [27] Syracuse University, "A Capability Maturity Model for Research Data Management." [Online]. Available: <http://rdm.ischool.syr.edu/xwiki/bin/view/Main/>
- [28] Innovation Value Institute, "The IT-CMF Framework." [Online]. Available: <http://ivi.nuim.ie/it-cmf>.
- [29] M. Carcary, "Design Science Research: The Case of the IT Capability Maturity Framework (IT CMF)," *Electronic Journal of Business Research Methods*, 2011, vol. 9, issue 2.
- [30] D. M. Ahern, A. Clouse, R. Turner, "CMMI Distilled: A Practical Introduction to Integrated Process Improvement, Third Edition," Addison Wesley Professional, 2008.
- [31] CMMI Product Team, "CMMI for development, version 1.3," Software Engineering Institute - Carnegie Mellon University, Tech. Rep. CMU/SEI-2010-TR-033, 2010.
- [32] CMMI Product Team, "CMMI for acquisition, version 1.3," Software Engineering Institute - Carnegie Mellon University, Tech. Rep. CMU/SEI-2010-TR-032, 2010.
- [33] CMMI Product Team, "CMMI for services, version 1.3," Software Engineering Institute - Carnegie Mellon University, Tech. Rep. CMU/SEI-2010-TR-034, 2010.
- [34] F. Hamel, T. P. Herz, F. Uebernickel, W. Brenner, "IT Evaluation in Business Groups: A Maturity Model," In *Proceedings of the 28th Symposium on Applied Computing*, 2008.

- [35] R. Kohli, V. Grover, "Business Value of IT: An Essay on Expanding Research Directions to Keep up with the Times," *Journal of the Association for Information Systems*, vol. 9, pp. 23-39, 2008.
- [36] D. Remenyi, F. Bannister, A. Money, "The Effective Measurement and Management of ICT Costs and Benefits," Elsevier, 2007.
- [37] U. Frank, "Evaluation of Reference Models," In P. Fettke and P. Loos: *Reference modelling for business systems analysis*, Idea Group Inc., 2007.
- [38] SPICE Project Organization, "Software Process Assessment (SPICE)." [Online]. Available: <http://www.sqi.gu.edu.au/SPICE/>.
- [39] ISO/IEC 15504:2004, "Information technology - Process assessment," International Organization for Standardization and International Electrotechnical Commission Std. 2004.
- [40] ISO/IEC 15504-3:2004, "Information technology - Process assessment - Part 3: Guidance on performing an assessment," International Organization for Standardization and International Electrotechnical Commission Std. 2004.
- [41] J. Becker, R. Knackstedt, J. Pöppelbuß, "Developing Maturity Models for IT Management – A Procedure Model and its Application," In *Business & Information Systems Engineering*, vol.1, issue 3, pp. 212-222. 2009.
- [42] ISO 9001:2008. Quality management systems – Requirements. , International Organization for Standardization Std. 2008.
- [43] ISO 16363:2012. Space data and information transfer systems – Audit and certification of trustworthy digital repositories. 2012.
- [44] ISO 14721:2010. Space data and information transfer systems – Open archival information system – Reference model. 2010.
- [45] ISO 20652:2006 Space data and information transfer systems – Producer-archive interface – Methodology abstract standard. 2006.
- [46] Röglinger, M., Pöppelbuß, J. and Becker, J., "Maturity models in business process management", *Business Process Management Journal*, Vol. 18 No. 2, pp.328 – 346. 2012.
- [47] ISO 38500:2008. Corporate governance of information technology. 2008.
- [48] ISO 31000:2009, Risk management – Principles and guidelines.
- [49] ISO/DIS 9001:2014, "Quality Management Systems – Requirements," International Organization for Standardization and Draft International Std. 2014.
- [50] Digital Preservation Coalition, "Introduction: Definition and Concepts", 2008.
- [51] A. Brown, *Practical Digital Preservation - A how-to guide for organizations of any size*, Facet Publishing. 2013.
- [52] C. M. Dollar, L. J. Ashley, "Assessing Digital Preservation Capability Using a Maturity Model Process Improvement Approach", Technical Report, February 2013.
- [53] Preservica, "Digital Preservation Maturity Model", White Paper, 2014.
- [54] Risk and Insurance Management Society, Inc. (RIMS) and Logic Manager, "About the RIMS Risks Maturity Model", Executive Report, 2015.
- [55] M. Röglinger, J. Pöppelbuß, "What makes a useful maturity model? A framework for general design principles for maturity models and its demonstration in business process management," In *proceedings of the 19th European Conference on Information Systems*, Helsinki, Finland, June. 2011.
- [56] Deloitte & Touche LLP, "Risk Intelligent Governance: Lessons for state-of-the-art board practices", Technical Report, 2014.
- [57] CMMI Institute, "Data Management Maturity (DMM) Model," Version 1.0, August 2014.
- [58] E-ARK Project, "D2.1: General Pilot Model and Use Case Definition," 2014.
- [59] IT Governance Institute, COBIT 5 – A business Framework for the Governance and Management of Enterprise IT. 2012.

Appendices

A. Information Governance Maturity Models

According to ISO 38500 [47], Governance is “the system by which organizations are directed and controlled”. In other words, Governance is the set of policies, processes, activities, rules, etc. that direct, manage and act on an organization. One of most known fields of Governance is IT Governance - the governance of IT systems and resources. In fact, the rising interest and the proliferation of IT Governance references has led to definition of similar fields such as Information Governance (IG). IG is an emerging term used to define the multi-disciplinary field of effectively and efficiently manage information. In fact, IG covers either in whole or in part many sub-disciplines such as Content Management, Document Management, Records Management, Digital Asset Management, Risk Management, among others.

Figure 8 depicts where A2MIGO is positioned among the domains analysed in this Appendix. There is some overlap between domains as can be seen. A2MIGO is position within the Digital preservation perspective of information governance. Then, Table 11 shows for each of the maturity models analysed their position within the analysed domains, as well as, where A2MIGO is positioned. ‘X’ depicts the Maturity Model primary domain, while ‘x’ depicts secondary domains of the Maturity Model. A2MIGO builds on the knowledge of both the general and the digital preservation perspectives of information governance.

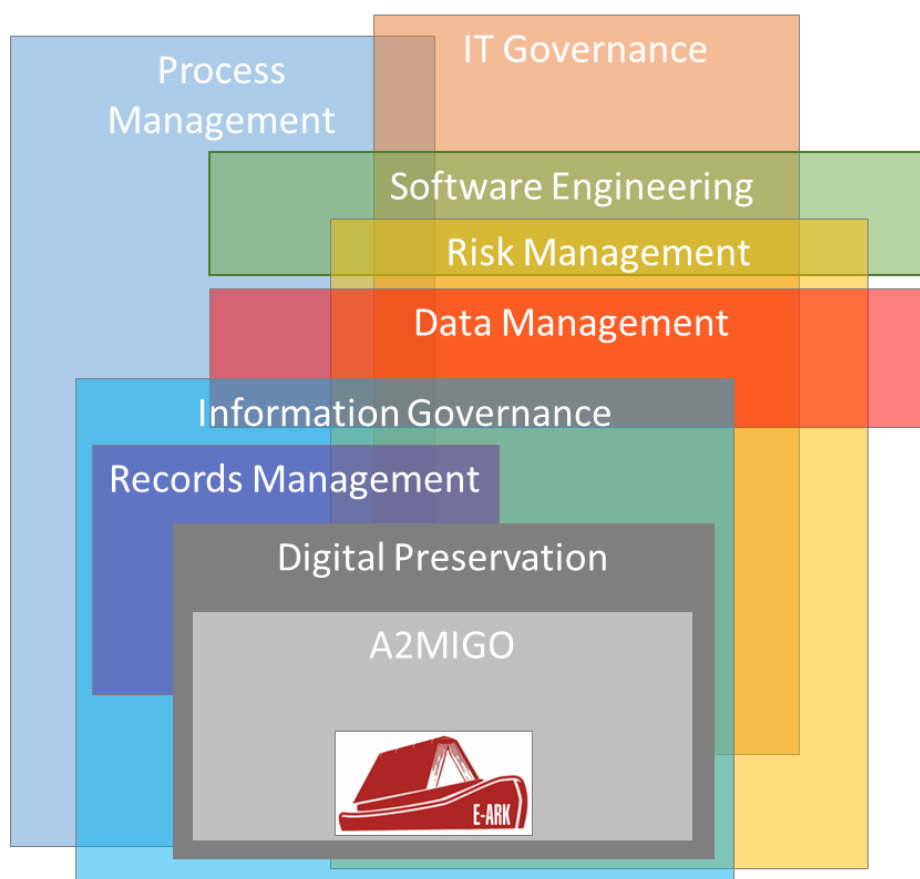


Figure 8. A2MIGO Domain Positioning Diagram

E-ARK project focus on three major processes of an archive: Ingest, Archival Preservation and Dissemination of information. One can say that E-ARK project focus on a sub-discipline of IG – Archival Management. The maturity model developed in this deliverable focus on Archival Management. However, the deliverable takes into account that Archival Management is only a subset of IG and others exist. Therefore, it compares existing maturity models on the various

subsets of Information Governance. Additionally, it also analyses generic and well-known maturity models to identify and understand the basic principles behind those models. Each maturity model is described by the following information: (1) A short **description** of the model; (2) **Aim** and purpose of the model; (3) **Scope** of the model; (4) **How to assess** (apply) the model; (5) **Term used to name the Attributes** of the model; (6) The **Attributes** of the model; and (7) A summary of the levels of the maturity model.

Table 11. Analysed Maturity Models and A2MIGO Domain Positioning

Maturity Model	Information Governance - General	Information Governance – Digital Preservation	Information Governance – Data Management	Information Governance – Records Management	Process Management	IT Governance	Risk Management	Software Engineering Governance
A.1.1 DAM Maturity Model	X		x					
A.1.2 ECM Maturity Model	X							
A.1.3 Asset Management Maturity Model	X							
A.1.4 Gartner Enterprise Information Management Maturity Model	X							
A.2.1 Digital Preservation Capability Maturity Model (DPCMM)		X						
A.2.2 Brown Digital Preservation Maturity Model		X						
A.2.3 Preservica Digital Preservation Maturity Model		X						
A.3.1 CMM for RDM			X					
A.3.2 Stanford Data Governance Maturity Model			X					
A.3.3 Data Management Maturity (DMM) Model			X					
A.4.1 ARMA Information Governance Maturity Model	x			X				
A.4.2 JISC Records Management Maturity Model				X				
A.5.1 ISO/ IEC 15504					X	x	x	x
A.5.2 Software Engineering Institute Capability Model Integration (CMMI)					X	x	x	x
A.5.3 OMG Business Process Maturity Model					X			
A.5.4 Gartner BPM Maturity Model					X			
A.5.5 Business Process Maturity Model (BPMM)					X			
A.6.1 Business-IT Alignment Maturity Model					x	X		
A.6.2 The IT Service CMM					x	X		
A.6.3 COBIT 4.1 Maturity Model					x	X	x	
0 IT Capability Model Framework (IT-CMF)					x	X	x	
A.6.5 Group IT Controlling (GITC) Maturity Model					x	X		
A.7.1 Hillson Risk Maturity Model							X	
A.7.2 RIMS Risk Maturity Model							X	
A.7.3 Deloitte Risk Maturity Model							X	
A.8.1 Documentation Process Maturity Model								X
A.8.2 Metrics Based Verification and Validation Maturity Model (MB-V2M2)								X
A.8.3 Model-driven Development (MDD) Maturity Model								X
The E-ARK Maturity Model for Information Governance (A2MIGO)	x	X					x	

A.1. Information Governance – General

This section analyses general IG maturity models. As described previously, IG is a multi-disciplinary field therefore the models analysed also represent disciplines that are considered relevant to IG.

A.1.1 DAM Maturity Model

Description: The Digital Asset Management (DAM) maturity model builds on the ECM3 maturity model [23]. This model was developed having in mind that the successful implementation of DAM in organizations goes beyond the use of technology. It requires a holistic approach which includes people, systems, information and processes. This maturity model provides a description of where an organization is, where it needs to be so that it can perform gap analysis and comprehend what it needs to do to achieve the desired state of DAM implementation. To assess the DAM ecosystem of an organization the DAM maturity model is divided into 15 dimensions that are structured into four categories.

Aim: Improve the success rate of DAM projects in organizations by providing a way of assessing the current state of the current implementation, as well as, an improvement path for enhancement of DAM.

Scope: Information Governance (Digital Asset Management perspective).

How to Assess: There is a description on how to do a self-assessment. It should begin by identifying the stakeholders who identified the need for DAM and can advocate in favour of it. Then, a set of questionnaires must be created and administered to each of the stakeholders identified. Then the levels can be determined using the answers to the questionnaires.

Term used to name of the Attributes: Categories / Dimensions.

Attributes (4/15): People (Technical Expertise; Business Expertise; Alignment); Information (Asset; Metadata; Reuse; Findability; Use Cases); Systems (Prevalence; Security; Usability; Infrastructure); Processes (Workflow; Governance; Integration).

Table 12. Summary of the Digital Asset Management (DAM) Maturity Model levels

Level	Name	Description
1	Ad-Hoc	Ad-hoc approaches to DAM, unorganized, with no policies in place. There are no reuse procedures and instead of using existing digital assets people choose to recreate them. Organizational needs are unstructured and there is no value applied to user scenarios. There are exceptional or no procedures for asset lifecycle. Regarding Governance, there are no procedures in place. There is no intentional integration.
2	Incipient	There is casual technical expertise, business expertise and alignment. Metadata management is inconsistent, as well as, reuse of existing assets. Asset discovery is incipient with search engines being used and indexing started. Use cases requirements are gathered at the project-level. There are incipient security measures in place, being system-specific. Single platform tools with no customization are being used. There are some informal workflows, some policies and formal procedures. Integration is not planned although there are some forced integrations between systems and processes.
3	Formative	There is demonstrated technical and business expertise, as well as, alignment. Assets are centralized. Metadata obeys to organizational vocabulary in use. There is a reuse strategy of assets. Asset discovery is improved, indexing is complete, and vocabulary terms are used to refine metadata. Requirements are now gathered at the program-level. There are efforts to combine and adopt DAM across the organization. There are centralized security

Level	Name	Description
		controls. There is some degree of multi-platform support. There is informal Business-IT coordination. There are workflows in place with limited automation. Regarding governance, there are structure and codification guidelines for defining procedures. Integration vision is complete and there is understanding of the common standards.
4	Operational	There is operational technical and business expertise, and there is organized knowledge transfer. Regarding alignment, there are collaborations between organizational units to improve assets management. All new assets types are registered and linked to standards and best practices. Regarding metadata, there are taxonomies and assets types are registered and related. There is a reuse strategy for all assets. There is a federated search mechanism. Assets use cases are structured organized and prioritised. Security controls are enforced across the organization at the asset level. There is remote multi-platform that collects feedback from users. Change management and governance are integrated which leads to proactive implementations. There are automated processes for both systems and organizational units. Policies and procedures are disseminated and enforced. Responsibility and ownership is accepted. The integration visions uses defined and documented paradigms.
5	Optimal	Technical and business expertise is optimal and helps in understanding and participating in forecasting of future DAM needs and capabilities to improve future asset value. Alignment is optimal as there is pre-emptive use and enhancement of DAM capabilities to reveal present and prospect asset value. Assets are prepared and authorized for use and reuse. Assets are being used to manage metadata, there is enterprise taxonomy and metadata is complete and embedded with the asset. There is discovery of new uses for the assets past the original aim. Asset search and classification is a central service. There is a framework in place to define, measure and manage existing and new use cases. Security is implemented and enforced throughout the organization. There is a multilingual, multi-platform system in place. Workflows are standard practice with performance indicators in place. There is proactive refinement of governance procedures. Integration occurs in real time and is seamless.

A.1.2 ECM Maturity Model

Description: A strategy Enterprise Content Management (ECM) must encompass the human, information and systems aspects [24]. If we look from a practical view, organizations cannot deal with all the ECM challenges at the same time. As such organizations need to enhance their ECM implementation step-by-step wise, by following a roadmap for ECM improvement. This maturity model provides the tools to build this roadmap by providing the current state of ECM implementation as well as a roadmap to reach the required maturity level.

Aim: Build a roadmap for ECM improvement, in a step-by-step fashion ranging from basic information collection and simple control to refined management and integration.

Scope: Information Governance (Enterprise Content Management perspective).

How to Assess: No assessment method described, the way of getting the current level is done by the organization itself by checking if the organization possesses all the requirements for a given level regarding a specific dimension.

Term used to name of the Attributes: Categories / Dimensions.

Attributes (3/13): Human (Business Expertise; IT; Process; Alignment); Information (Context/Metadata; Depth; Governance; Re-Use; Findability); Systems (Scope; Breadth; Security; Usability)

Table 13. Summary of the Enterprise Content Management (ECM) Maturity Model levels

Level	Name	Description
1	Unmanaged	Content is not managed formally. There are distributed share drives, documents are stored in local hard drives. There is redundant data; content discovery is not possible which results in people need to create the same content over and over.
2	Incipient	Particular sets of content are managed through projects driven approaches. There are redundant products being used, although insufficiently applied and not commonly used.
3	Formative	There is an inventory of content. Plans, policies and procedures are in place, although still in the implementation phase. There are several projects in development although might fail due to the absence of a strategy. Information lifecycle management principles are being implemented.
4	Operational	There is universal content management across the organization, although it is scattered through several systems. There are retention schedules. There is a decision on what content is excluded from management. There is collaborative content management in place.
5	Pro-Active	Content management is available across the organization and is a shared service. The organization can implement new technologies such as digital asset management as a result of a flexible architecture in place. Information management issues and the business drivers are fully understood.

A.1.3 Asset Management Maturity Model

Description: This maturity model originated from an evaluation in the Netherlands to investigate how asset managers deal with long-term investment decisions [21]. This evaluation took into consideration organizations that control infrastructures, such as, networks, roads and waterways and focus on the strategy, tools, environment and resources. The maturity model consists of five maturity levels and is detailed through four dimensions.

Aim: Understand how asset managers deal with long-term investment decisions and provide an improvement path for organization to improve the long-term investment decisions.

Scope: Asset Management.

How to Assess: An interview protocol is provided which consists of eleven questions in total, two or three for each of the dimensions.

Term used to name of the Attributes: Dimensions / Category.

Attributes (4): Strategy; Tools; Environment; Resources.

Table 14. Summary of the Asset Management Maturity Model levels

Level	Name	Description
1	Initial	Strategy and goals do not exist and are not agreed. Tools are used occasionally and there is no communication of uncertainty. Regarding the environment, answers are sought in an ad-hoc way. There is no separate funding for replacement.
2	Repeatable	Management has not defined a plan and there is no responsibility assignment. There is a small set of tools being used, and uncertainty is occasionally communicated. Regarding the environment, occasionally there are external parties who are consulted. There are funds for replacement of assets that are regularly deployed.
3	Defined	There are procedures at the organization unit level to set both policies and goals for asset management. Also at the organizational unit level, there are standard tools being used.

Level	Name	Description
		Regarding the environment, there is a standard the unit level on how to negotiate with third parties. There is a way to allocate funds for replacement of assets.
4	Managed	The processes and responsibilities between organizational units are set. Standard methods and techniques are being used organization-wide. Uncertainties are shared and discussed. Regarding the environment, there are protocols to negotiate with external parties organization-wide. There is an allocation method for asset replacement funds which is implemented throughout the organization.
5	Optimizing	Management fully supports policies and strategy; and asset management is integrated in the organization. Tools used for asset management are continuously improved, updated and communicated. Uncertainties are now shared with business partners. Regarding environment, there is a coordination with policy makers and business partners. The method for allocation of resources is now flexible and oriented to future use.

A.1.4 Gartner Enterprise Information Management Maturity Model

Description: Enterprise Information Management (EIM) is defined by Gartner as the organizational commitment to “structure, secure and improve the accuracy and integrity of enterprise information; solve semantic inconsistencies across boundaries and; support the objectives of enterprise architecture and the business strategy” [13]. Before organizations begin to implement this commitment, they must first identify the current state of the information management practices and then plan to further improve these practices. Gartner proposes six phases of maturity regarding EIM. Where in level 0 there are no EIM activities in place and in level 5 EIM is fully implemented in the organization. The main aim of using maturity phases for implementing EIM in organizations is that EIM cannot be implemented as a single project as it requires an ongoing building of skills and awareness that must occur in iterative phases.

Aim: Raise awareness of the current state of EIM practices in organizations and provide a list of actions to improve to the next level.

Scope: Information Governance.

How to Assess: It provides examples on how to get questions from the maturity criteria. However, it does not provide a method or guidelines for assessment using this maturity model.

Term used to name of the Attributes: No attributes defined.

Attributes (0): No attributes defined.

Table 15. Summary of the Gartner Enterprise Information Management Maturity Model levels

Level	Name	Description
0	Unaware	IT and Business Leaders are educated on the value EIM and the risks of not having it in place in the organization.
1	Aware	Strategies to align EIM with Enterprise Architecture and other activities are drafted.
2	Reactive	Top management recognizes the need for EIM; the business case for EIM is prepared.
3	Proactive	The business case for EIM is now presented to management and other relevant stakeholders.
4	Managed	The information management activities and resources from the various departments are compiled and linked to the EIM strategy for the organization. EIM should now be regarded as a service instead of a project. There must be a balanced scorecard for information management.

Level	Name	Description
5	Effective	Technical controls and procedures are in place to guarantee that there isn't a false sense of security on the EIM procedures in place, as these can easily turn ineffective due to business changes.

A.2. Information Governance – Digital Preservation

Digital Preservation “refers to the series of managed activities necessary to ensure continued access to digital materials for as long as necessary. Digital preservation [...] refers to all of the actions required to maintain access to digital materials beyond the limits of media failure or technological change” [50]

A.2.1 Digital Preservation Capability Maturity Model (DPCMM)

Description: The Digital Preservation Capability Maturity model is a model that draws upon the overall framework of the CMM development model but is not intended to be a rigorous model with precisely defined parameters. [52] The DPCMM is a systematic tool to chart the evolution from a disorganized and undisciplined electronic records management program, or one that does not exist, into increasingly mature stages of digital preservation capability. The DPCMM is designed to help identify, protect and provide access to long-term and permanent digital assets.

Aim: The goal of the DPCMM is to support the management of a digital preservation program that Identifies and monitors at a high level where the program is in relation to an optimal digital preservation program; establishes priorities and an improvement roadmap to achieve enhanced digital preservation capabilities over time; and reports digital preservation capability gaps and achievements to resource allocators and stakeholders.

Scope: Information Management (Digital Preservation perspective).

How to Assess: Consists of 75 statements where which has an integer value ranging from zero to four designated as an index value. [52] These index values are then mapped to a certain capability level. There is an on-line assessment tool available at <http://www.digitalok.org>.

Term used to name of the Attributes: Domains / Components.

Attributes (3/15): Infrastructure (Policy, Strategy, Governance, Collaboration, Technical Expertise, Open Standard Technology Neural Formats, Designated Community); Digital Repositories; Services (Electronic Records Survey, Ingest, Storage, Device/Media Renewal, Integrity, Security, Preservation Metadata, Access).

Table 16. Summary of the Digital Preservation Capability Maturity Model (DPCMM) levels [52]

Level	Name	Description
1	Nominal	A systematic digital preservation program has not been undertaken and most, if not all, electronic records that merit long-term retention are at risk.
2	Minimal	Digital preservation capabilities are rudimentary and do not rise to the level of ISO 14721/ISO 16363 specifications. Consequently, most electronic records that merit long-term retention are at risk.
3	Intermediate	The organization supports ad-hoc initiatives and projects that approach but do not conform fully to ISO 14721/ISO 16363 specifications. There is an established basis for proactive and sustainable digital preservation improvement actions over time.

Level	Name	Description
		Nevertheless, it is likely that some electronic records that merit long term retention remain at risk.
4	Advanced	The organization has a robust infrastructure and the preservation of electronic records is undertaken with a framework that conforms to most of the ISO 14721 specifications and the criteria of ISO 16363. Few electronic records that merit long-term preservation are at risk.
5	Optimal	Represents the highest level of sustainable conforming ISO 14721/ISO 16363 digital preservation capability and repository “trustworthiness” that an organization can achieve. No records that merit long-term retention are at risk.

A.2.2 Brown Digital Preservation Maturity Model

Description: The Brown Digital Preservation Maturity Model examines the notion of “trusted” digital repositories and proposes a maturity model for digital preservation. The author begins by defining the basic maturity levels for digital preservation building on the knowledge of the Prince 2 Maturity Model from the UK Office of Government Commerce. [51] Then the author defined the digital preservation process perspectives, which are the set of processes that together establish the digital preservation capability. Then, for each of these processes there are a set of requirements that organizations must achieve to reach a certain maturity level for a certain process.

Aim: Enable organizations to assess their digital preservation capabilities and create a roadmap for developing them to the required maturity level. [51]

Scope: Information Governance (Digital Preservation perspective).

How to Assess: Not defined. The organization should assess themselves against the requirements of the maturity model and position themselves among the maturity levels. However, there is no method or tool to facilitate this assessment.

Term used to name of the Attributes: Process perspective.

Attributes (10): Organizational Viability; Stakeholder Engagement; Legal Basis; Policy Framework; Acquisition and Ingest; Bitstream Preservation; Logical Preservation; Metadata Management; Dissemination; Infrastructure.

Table 17. Summary of the Brown Digital Preservation Maturity Model levels [51]

Level	Name	Description
0	No Awareness	There is no awareness of the need for the process or the underlying principles for implementing it in the organization.
1	Awareness	There is awareness of the need to implement the process and there is an understanding of the basic principles.
2	Roadmap	There is a defined roadmap for implementing the process.
3	Basic Process	There is a basic process implemented in the organization. This level marks the turning point from the awareness stage (the first three levels) to the capability stage (the last three levels).
4	Managed Process	There is a comprehensive and managed process. This process reacts to varying settings.
5	Optimized Process	There is continuous process improvement with proactive management in the organization.

A.2.3 Preservica Digital Preservation Maturity Model

Description: The Preservica Digital Preservation Maturity Model was created on the premise that organizations have realized that it is critical for their business that information is retained over a long period of time. Information can be retained for different reasons, such as, to avoid risks or to create value. Nonetheless, this information must be accessible when it is needed. Preservica defines three main sections for the maturity model. The first section is durable storage which comprehends levels 1 to 3, where raw bits storage increases in safety and security. The second section comprehends levels 4 to 5, where the raw bits in storage become preserved and organized. The third and last section is information preservation which comprehends level 6, where the information survives the lifetime of the application that created it.

Aim: Provide a way of categorizing the many different types of solutions from the fields of “Digital Preservation” and “Digital Archiving” to enable organizations to understand the differences and to select the best solution for them.

Scope: Information Management (Digital Preservation perspective).

How to Assess: Not described.

Term used to name of the Attributes: No attributes defined.

Attributes (0): No attributes defined.

Table 18. Summary of the Preservica Digital Preservation Maturity Model levels

Level	Name	Description
1	Safe Storage	Simple bit-level storage on magnetic or optical storage with some level of reassurance that the bits are protected against simple storage failure. This includes storage on protected spinning disks using RAID techniques, optical media with long-term storage and managed locations, or long-life tape storage.
2	Storage Management	Active storage management is added which moves the bits to the most appropriate location. The decision on which bits are located where may be done based on storage durability, cost reduction or performance. The criteria are flexible to balance these drivers. Information must be held in at least two locations, for example disc and backup tape or multiple disc replicas.
3	Storage Validation	Multiple object storage plus fixity checking is added to validate storage durability. Object fixity is checked on storage, access and at regular intervals to confirm objects have not been tampered with. If bit failure is identified, self-healing from an alternative copy will occur.
4	Information Organisation	The ability to turn raw bit level files into information is incorporated, which results in a dramatic increase in the usefulness of the information.
5	Information Processes	Efficient and flexible business processes are added to automate the activities associated with information management. These include interfaces to the information sources and dissemination to information consumers using flexible workflows and interfaces. They also include high-throughput capabilities and integration with a third-party identity management system.
6	Information Preservation	Digital information is now usable by the person who wants it at the time it is needed. A mature system now incorporates Information Preservation tools to counter the threat of obsolescence.

A.3. Information Governance – Data Management

This section analyses IG maturity models from the Data Management perspective. As described previously, IG is a multi-disciplinary field therefore the models analysed also represent disciplines that are considered relevant to IG.

A.3.1 CMM for RDM

Description: The Capability Maturity Model for Research Data Management (RDM) was developed by the school of information studies at the University of Syracuse in the USA⁵. It is based on the number and name of levels of CMMI, as well as, the principles of each level. It makes several references throughout the levels to CMMI and contains five levels spread among five key process areas specific to RDM. RDM has become a trending topic in data management as increased importance from government agencies, such as, the US National Science Foundation. These funding agencies are raising the issue of maintaining good RDM practices for the projects that are funded by them.

Aim: Raise awareness on RDM among research projects, such as, small science projects. Provide a conceptual model upon which policies, practices, and performance/impact assessment for FDM can be based.

Scope: Information Governance (Data Management perspective).

How to Assess: Not specified.

Term used to name of the Attributes: Key Process Areas.

Attributes (5): Data Management in general; Data acquisition, processing and quality assurance; Data descriptions and representation; Data dissemination; Repository services and preservation.

Table 19. Summary of the Research Data Management (RDM) Maturity Model levels

Level	Name	Description
1	Initial	RDM focuses on projects, and there are no goals or practices defined. Also, there are no defined Processes, and if defined they are not stable. Organization is immature regarding processes, as individuals perform these intuitively. Skills and knowledge is low, often from students. Personnel changes might endanger RDM.
2	Managed	RDM still focuses on projects and has a reactive nature. There are processes at the project level, with policies and procedures. There is a RDM plan, however new projects mean that the existing processes, policies and procedures must be redeveloped. Also, sharing between projects is difficult due to the different practices and processes among projects.
3	Defined	RDM processes have a proactive nature and are documented for the whole organization; these can then be specifically tailored to different projects. These processes include inputs, standards, work and validation procedures, as well as, compliance criteria. Organizations at this level can employ the similar metadata standards across projects.
4	Quantitatively Managed	RDM processes are now quantitatively measured; these have established “quantitative objectives for quality and process performance” [27][31]. These objectives are based on RDM user requirements and goals. The quantitative management of RDM processes means that there is better forecast of process performance as this is measured through “statistical and other quantitative techniques” [27][31].
5	Optimizing	The focus is now on continuously improve the RDM processes, by identifying weaknesses and defects and addressing them in a proactive manner.

⁵ <http://rdm.ischool.syr.edu/xwiki/bin/view/CMM+for+RDM/WebHome>

A.3.2 Stanford Data Governance Maturity Model

Description: This maturity model is based on the Data Governance Program from Stanford and is centred on the institution as it was developed having in mind the goals, priorities and competences of Stanford. It focuses on both the foundations and the project aspects of data governance and measures the core data governance capabilities and development of the program resources [20]. The foundation aspects are Awareness, Formalization and Metadata. The project components are Stewardship, Data Quality and Master Data; this enables the maturity model to measure the effectiveness of the data governance concepts application on funded projects. The data governance maturity model is divided into dimensions namely people, policies and capabilities. It consists of a five-level maturity grid for each of the foundation aspects and project components making a distinction to each dimension for every one of the aspects and components. The name for each of the maturity levels is not described in this model and is depicted in Table 20 as “-”.

Aim: Measure the foundational aspects and project components of the Stanford’s Data Governance program.

Scope: Information Governance (Data Management perspective).

How to Assess: It contains a catalogue of both qualitative and quantitative metrics that are used to calculate the maturity level.

Term used to name of the Attributes: Dimensions.

Attributes (3): People; Policies; Capabilities.

Table 20. Summary of the Stanford Data Governance Maturity Model levels

Level	Name	Description
1	-	There is limited awareness of data governance, policies are not documented. There are no defined roles. Metadata is not collected consistently.
2	-	Management is aware of the data governance program. There are data governance roles and responsibilities defined and agreed upon. There is metadata on structured data and best practices are collected and available.
3	-	Knowledge workers are aware of the data governance program and management understands how data governance impacts each unit of the organization. Common data policies are documented and available. There are some roles that support data governance needs and individuals understand their responsibilities.
4	-	Management understands the long-term goals of the data governance program and their role to attain them, they also promote the program. Knowledge workers understand the benefits and impacts of data governance in their units. Data policies are managed through a common system available to stakeholders on a selective basis. Roles are organized into schemas. Metadata collection and validation responsibilities are assigned to specific people.
5	-	Management and knowledge workers fully understand their roles in the data governance program, as well as, their contribution to the attainment of the long-term goals of the program. There is history of all data policies which are managed through a common system available to all stakeholders. The data governance organizational schemas are maintained as defined, there are regular meetings and activities are documented. There is a dedicated metadata management group, which aim is to enhance metadata capabilities.

A.3.3 Data Management Maturity (DMM) Model

Description: The Data Management Maturity (DMM) Model is a reference model for data management process improvement created by the CMMI Institute. The DMM defines the fundamental business processes of data management and specific capabilities that constitute a path to maturity. [57] It allows organizations to evaluate themselves against documented best practices, determine gaps, and improve data management across functional, business, and geographic boundaries.

Aim: The DMM Model facilitates an organization's understanding of data management as a critical infrastructure, through increasing capabilities and practices.

Scope: Information Governance (Data Management perspective).

How to Assess: There are two types of measurement within the model, capability measurement and maturity measurement. [57] In capability measurement, for each process area, functional capabilities are measured. These are based on the performance of functional practices defined for each process area. Then, in maturity measurement, maturity is measured based on the achievement of each process area using both the functional and infrastructure support practices for each capability level all levels below.

Term used to name of the Attributes: Categories / Process Areas.

Attributes (6/25): Data Management Strategy (Data Management Strategy; Communications; Data Management Function; Business Case; Program Funding); Data Governance (Governance Management; Business Glossary; Metadata Management); Data Quality (Data Quality Strategy; Data Profiling; Data Quality Assessment; Data Cleansing); Data Operations (Data Requirements Definition; Data Lifecycle Management; Provider Management); Platform & Architecture (Architectural Approach; Architectural Standards; Data Management Platform; Data Integration; Historical Data, Archiving and Retention); Supporting Processes (Measurement and Analysis; Process Management; Process Quality Assurance; Risk Management; Configuration Management).

Table 21. Summary of the Data Management Maturity Model levels [57]

Level	Name	Description
1	Performed	Processes are performed ad hoc. Processes are typically not applied across business areas. Process discipline is primarily reactive; for example, data quality processes emphasize repair over prevention. Foundational improvements may exist, but improvements are not yet extended within the organization or maintained.
2	Managed	Processes are planned and executed in accordance with policy; employ skilled people with adequate resources to produce controlled outputs; involve relevant stakeholders; are monitored and controlled and evaluated for adherence to the defined process.
3	Defined	Set of standard processes is employed and consistently followed. Processes to meet specific needs are tailored from the set of standard processes according to the organization's guidelines.
4	Measured	Process metrics have been defined and are used for data management. These include management of variance, prediction, and analysis using statistical and other quantitative techniques. Process performance is managed across the life of the process.
5	Optimized	Process performance is optimized through applying level 4 analysis for target identification of improvement opportunities. Best practices are shared with peers and industry

A.4. Information Governance – Records Management

This section analyses IG maturity models from the Records Management perspective. As described previously, IG is a multi-disciplinary field therefore the models analysed also represent disciplines that are considered relevant to IG.

A.4.1 ARMA Information Governance Maturity Model

Description: This maturity model builds on the generally accepted recordkeeping principles developed by ARMA⁶. The principles provide high-level guidelines of good practice for recordkeeping although they do not go into detail to the implementation of these principles and do not have further details on policies, procedures, technologies and roles. The point of this maturity model is to address this gap by detailing what a successful implementation of information governance is at different levels of maturity. It consists of five maturity levels for each of the principles [25].

Aim: Support organizations understand the standards, best practices and regulatory requirements that enclose information governance, so that they can understand the successful information governance characteristics at differing levels of maturity.

Scope: Information Governance (records management perspective).

How to Assess: There are a series of steps to assess the current maturity level and identify the desired level. These steps are not formal and consist of simple statements of what to do without defined guidance on how to perform the steps.

Term used to name of the Attributes: Principles.

Attributes (8): Accountability; Transparency; Integrity; Protection; Compliance; Availability; Retention; Disposition.

Table 22. Summary of the Information Governance Maturity Model levels

Level	Name	Description
1	Sub-standard	Information Governance is not addressed or is addressed ad-hoc. Organizations at this level might not meet legal or regulatory inspection.
2	In Development	Information governance is starting to be recognized in the organization as essential to meet legal, regulatory, and business requirements. Organizations at this level are still susceptible to legal or regulatory inspection due to incomplete practices.
3	Essential	An organization at this level has the essential requirements necessary to meet the legal, regulatory and business requirements. There are clear policies and procedures. Process implementation takes into consideration the improvement of Information Governance. Organizations at this level might miss substantial opportunities for restructuring business and improve cost controls. These organizations are compliant, at a minimum, with legal and regulatory scrutiny.
4	Proactive	There is a proactive information governance program in place throughout the organization and there is continuous improvement of information governance. Information governance concerns are taken in consideration when taking business decisions. These organizations meet legal and regulatory requirements and are compliant with good practices.
5	Transformational	Information governance is embedded into the business infrastructure and process. Legal and regulatory responsibilities are routine. Information governance is a way to contain costs, gain competitive advantage, and improve the services provided.

⁶ www.arma.org/principles

A.4.2 JISC Records Management Maturity Model

Description: This maturity model was created by JISC infoNet and stands as a self-assessment tool for higher education institution in England and Wales [22]. It is based on a code of practice and its aim is to help in the compliance with this code although it is independent from the code and the future plans are to continue development and enhancement independent from this code.

Aim: Help higher education institutions to assess their current approach on records management regarding recommendations issued by the United Kingdom government and benchmark against other similar organizations.

Scope: Information Governance (records management perspective).

How to Assess: Self-assessment using a spreadsheet, consisting of statements for each of the nine sections. Users should choose the level that best suits the organization for each statement.

Term used to name of the Attributes: Section.

Attributes (9): Organizational arrangements to support records management; Records management policy; Keeping records to meet corporate requirements; Records systems; Storage and maintenance of records; Security & access; Disposal of records; Records created in the course of collaborative working or through out-sourcing; Monitoring and reporting on records management.

Table 23. Summary of the Records Management Maturity Model levels

Level	Name	Description
0	Absent	There is no evidence of awareness of the need to have a strategic approach to records management.
1	Aware	There are uncoordinated efforts to improve records management in reaction to identified issues.
2	Defined	Efforts are now coordinated in an attempt to enhance records management organization-wide.
3	Embedded	There is effective records management which is fully unified within the organization's strategic and operational activities.

A.5. Process Management

This sections analyses generic maturity models for process improvement. In theory, these models can be used to improve processes independently of the domain and context of those processes.

A.5.1 ISO/ IEC 15504

Description: The ISO/IEC 15504 [39] was born as the “Software Process Improvement and Capability Evaluation” (SPICE) [38] in 1993. The acronym is still used today by the user groups of the standard and in the title of the annual conference. ISO 15504 is a reference model for maturity models that consist of capability levels that consist of the process attributes and further consist of generic practices. The standard is divided into nine components or parts which are, (1) Concepts and introductory guide; (2) A model for process management; (3) Rating processes; (4) Guide to conducting assessment; (5) Construction, selection and use of assessment instruments and tools; (6) Qualification and training of assessors; (7) Guide for use in process improvement; (8) Guide for use in determining supplier process capability; and (9) Vocabulary.

Aim: Determine the organization’s current capabilities for delivering software and IT systems in order to benchmark organizations.

Scope: Business Process Management (process improvement perspective)

How to Assess: The standard provides a detailed assessment process in Part 3. [40] This assessment guides the whole assessment, from initiation to reporting.

Term used to name of the Attributes: Process Groups.

Attributes (9): Acquisition Process Group; Supply Process Group; Engineering Process Group; Operation Process Group; Management Process Group; Process Improvement Process Group; Resource and Infrastructure Process Group; Reuse Process Group; Support Process Group.

Table 24. Summary of the ISO/ IEC 15504 levels

Level	Name	Description
0	Incomplete Process	The process is not implemented. If implemented, the process does not achieve the purpose. There is little or no evidence of achievement of the process purpose.
1	Performed Process	The process is implemented and achieves its purpose.
2	Managed Process	The process is implemented and managed, which means that it is planned, monitored and enhanced. The inputs and outputs are defined, controlled and maintained.
3	Established Process	The process is now implemented using a defined process that includes guidelines to define the process and deploying it.
4	Predictable Process	The process now operates within defined limits, can be measured and controlled.
5	Optimizing Process	The process is now continuously improved to achieve current and future business goals.

A.5.2 Software Engineering Institute Capability Model Integration (CMMI)

CMMI is divided into three constellations, which can be applied to different kinds of organizations. A constellation is “a collection of components that are used to construct models, training material, and appraisal materials in an area of interest.” [31] There are two constellations in CMMI 1.3, (1) Development [31], which supports organizations that develop products and (2) Acquisition [32] which supports an organization in getting products or services from external suppliers. There is also material to another constellation, Services [33], which is intended to support organizations that primarily deliver services rather than products. This analysis will focus on the development constellation of CMMI.

Description: The Capability Maturity Model Integration (CMMI) was developed in sponsorship by the US Department of Defence teamed up with the National Defence Industrial Association (NDIA). Then in 2000, the Software Engineering Institute (SEI) at Carnegie Mellon University created a stewardship to produce the first integrated CMMI models, with the companion appraisal and training material. In the year 2002 the CMMI version 1.1 was released, then in 2006 the version 1.2 was released and in 2010 version 1.3 was released. The CMMI Suite contains information and guidance to help an organization improve its processes. The CMMI models are composed of two kinds of materials, (1) Materials that help in the evaluation of organization processes, which provides essential information to the management, support and technical activities and (2) Materials which help improve process performance, which provides information which can be used to increase the capability level of an organization’s activities.

Aim: The main objectives of CMMI are to reduce the cost of implementing several process improvement models for each discipline accomplished by the eliminating inconsistencies, reducing duplication, increasing clarity and understanding, providing common terminology, providing consistent style, establishing uniform construction rules [30].

Scope: Business Process Management (process improvement perspective).

How to Assess: SEI developed a complementary document to assess CMMI. This document is SCAMPI for CMMI. SCAMPI stands for Standard CMMI Appraisal Method for Process Improvement. This document contains a very detailed method to use for appraisal using CMMI. It covers the whole assessment cycle from planning and preparing the assessment to the packaging and archiving of the appraisal assets used.

Term used to name of the Attributes: Process Areas.

Attributes (22): Causal Analysis and Resolution; Configuration Management; Decision Analysis and Resolution; Integrated Project Management; Measurement and Analysis; Organizational Process Definition; Organizational Process Focus; Organizational Performance Management; Organizational Process Performance; Organizational Training; Product Integration; Project Monitoring and Control; Project Planning; Process and Product Quality Assurance; Quantitative Project Management; Requirements Development; Requirements Management; Risk Management; Supplier Agreement Management; Technical Solution; Validation; Verification.

Table 25. Summary of the Software Engineering Institute Capability Model Integration (CMMI) levels

Level	Name	Description
1	Initial	The process is unpredictable, weakly controlled and reactive.
2	Managed	The process is specific for a certain process and is still reactive.
3	Defined	The process is now defined for the whole organization and is proactive.
4	Quantitatively Managed	The process is now measured and controlled.
5	Optimizing	The process focus is now on continuous improvement.

A.5.3 OMG Business Process Maturity Model

Description: The Open Management Group (OMG) created the Business Process Maturity Model (BPMM) in 2008 to address the following five challenges of enterprise systems success (1) The lack of standards for appraisal of the maturity of the business process workflows and the lack of methods for identifying process weaknesses and the risks they pose for achieving business goals and successfully deploying projects; (2) The lack of methods for the appraisal of the alignment between how tasks are performed and how they are described in model representations of process workflows; (3) The unawareness of the extent to which growth and acquisitions have resulted in multiple ways of performing similar tasks; (4) The lack of methods for the appraisal of a supplier's capability for delivering outsourced IT and other business services within the parameters defined in a proposal or contract; and (5) The lack of guidance on how to implement the foundations of business processes required in order to guarantee organizational agility and lower operating costs [9].

Aim: Improve the success of business process management implementations in organizations by guiding business process improvement programs, assessing the risk of developing and deploying applications, assessing the supplier's capability and benchmarking.

Scope: Business Process Management

How to Assess: Not specified.

Term used to name of the Attributes: Process Areas.

Attributes (30): Organizational Improvement Planning; Organizational Performance Alignment; Defect and Problem Prevention; Continuous Capability Improvement; Organizational Innovative Improvement; Organizational Improvement Deployment; Organizational Common Asset Management; Organizational Capability and Performance Management; Product and Service Process Integration; Quantitative Product and Service Management; Quantitative Process Management; Organizational Process Management; Organizational Competency Development; Organizational Resource Management; Organizational Configuration Management; Product and Service Business Management; Product and Service Work Management; Product and Service Preparation; Product and Service Deployment; Product and Service Operations; Product and Service Support; Organizational Process Leadership; Organizational Business Governance; Work Unit Requirements Management; Work Unit Planning and Commitment; Work Unit Monitoring and Control; Work Unit Performance; Work Unit Configuration Management; Sourcing Management; Process and Product Assurance.

Table 26. Summary of the OMG Business Process Maturity Model levels

Number	Level	Description
1	Initial	Business processes are performed in inconsistent and sometimes ad-hoc ways with results that are difficult to predict.
2	Managed	The work is stabilized within local units to ensure it is performed in a repeatable way. Despite this, units performing similar tasks are using different procedures.
3	Standardized	Processes begin to emerge, based on information collected from best practices.
4	Predictable	The capabilities delivered by standard processes are used and provided to the units. Process performance is managed using statistical analysis and can be measured during intermediate states of a process.
5	Innovating	Improvement actions for the processes are focused on closing gaps between the organization's current capability and the capability necessary for the organization to meet its goals.

A.5.4 Gartner BPM Maturity Model

Description: Gartner created a Business Process Management (BPM) maturity model in an attempt to show organizations where they are positioned in relation to the critical success factors of a successful BPM implementation [10]. This maturity model consists of six phases and details the critical success factors for each phase, the competencies needed, the challenges and the triggers that make an organization transition from one phase to another.

Aim: Raise awareness of the current implementation of BPM in organizations.

Scope: Business Process Management.

How to Assess: Not specified.

Term used to name of the Attributes: Critical Success Factors.

Attributes (6): Strategic Alignment; Culture and Leadership; People; Governance; Methods; Information Technology.

Table 27. Summary of the Gartner BPM Maturity Model levels

Level	Name	Description
0	Acknowledge Operational Inefficiencies	The organization monitors and measures the business activities
1	Process Aware	The organization models and analyses business processes. It also establishes process performance metrics and identifies process owners and the overall governance structure.
2	Intraprocess Automation and Control	There is a direct link from process model and rules to execution. There is a comparison of alternatives motivated by a variety of optimization techniques in real time. There is also integration between activity-based accounting and process steps.
3	Inter-process Automation and Control	There is realignment between process and market strategy. There is process automation and control across the organizations, the clients and partners.
4	Enterprise Valuation Control	There is a business performance framework that links the valuation of the business and process execution. There are goal-driven processes.
5	Agile Business Structure	There is a culture of innovating new businesses, products and services through and agile business structure.

A.5.5 Business Process Maturity Model (BPMM)

Description: The Business Process Maturity Model (BPMM) provides a roadmap for organizations and adapts to the process areas for different business processes [17]. The BPMM aids the organizations to set priorities for improving their Business Process Management practices by using an established strategy and achieving the capability necessary to achieve its business strategy. The BPMM also helps analyse whether the processes meet stakeholders needs and expectations comparing the current maturity level to the desired level by performing gap analysis. The BPMM is based on many elements of the Key Performance Areas (KPA) of CMM/CMMI, IS12207 and IS15288.

Aim: Regarding business process management, compare the maturity of an organization to the industry standard.

Scope: Business Process Management.

How to Assess: Not specified.

Term used to name of the Attributes: Elements.

Attributes (4): Focus of KPAs; Measurement & Analysis; Monitoring & Control; Organizational Process Improvement.

Table 28. Summary of the Business Process Maturity Model (BPMM) levels

Level	Name	Description
1	Initial	The process is monitored and controlled in an ad-hoc way.
2	Management	The process is not defined or partially defined; process performance is measured partially; Process Performance is monitored and controlled for a work unit; Performance data is not used for process improvement.
3	Defined	The process is defined; process and mechanism performance is measured for the whole organization; process performance is monitored and controlled for the whole organization; partial performance data is used in an ad hoc way for process improvement.
4	Quantitatively Managed	Process Performance is measured quantitatively; Process performance is controlled systematically; Performance data is used in an ad-hoc way for process improvement.

Level	Name	Description
5	Optimizing	Process performance is monitored and controlled in a proactive way; performance data is systematically used to improve and optimize the process.

A.6. IT Governance

As described above, IT Governance is responsible for the rising of several fields such as IG. Additionally, IG comprises all policies, processes, activities, rules, etc. that support the governance of information. Among those processes are the governance of IT systems and resources related to IG such as, for example, records management systems or content management systems.

A.6.1 Business-IT Alignment Maturity Model

Description: Business-IT alignment implies applying IT in a relevant, timely and appropriate way that is in line with business needs, goals and strategy. It has been one of the main concerns of both business and IT experts and there is even a field dedicated on this problem, Enterprise Architecture. Its relevance has been further elevated by evidence that IT can influence and enhance industries and markets. [11]

Aim: Raise awareness of the alignment between business and IT in an organization.

Scope: IT Management.

How to Assess: There is an assessment process to evaluate an organization, but there are no details on it.

Term used to name of the Attributes: IT-business alignment criteria.

Attributes (6): Communications Maturity; Competency/Value Measurement Maturity; Governance Maturity; Partnership Maturity; Scope & Architecture Maturity; Skills Maturity.

Table 29. Summary of the Business-IT Alignment Maturity Model levels

Level	Name	Description
1	Initial/Ad-Hoc process	Business and IT lack understanding; there are some technical measurements on competency and value. There are no formal processes, cost centre and no reactive priorities. There is a conflict between IT and business as business sees IT as a cost of doing business. There is a traditional scope and architecture based on emails and accounting. Regarding skills, the IT takes risk and there is little reward. There is technical training.
2	Committed Process	There is limited business and IT understanding. Regarding value and competency there is functional cost efficiency. Governance is tactical at the functional level and occasionally responsive. IT is emerging as business asset and process enabler. The scope and architecture is based on transactions and the skills differ across functional units.
3	Established Focused Process	There is good understanding between IT and business. Regarding competency and value there is some cost effectiveness and a dashboard is established. Regarding Governance there is a relevant process across the organization. IT is seen as a business asset and process driver. Regarding scope and architecture, IT is integrated across the organizations. It is seen as an emerging value service provider and there is balanced technology and business hiring.
4	Improved/Managed Process	IT and Business are bonded/unified. Regarding competency and value IT is seen as cost effective, and is dashboard managed. In the governance aspect, IT is managed across the organization. IT enables and drives business strategy. The

Level	Name	Description
		scope and architecture is integrated with partners. IT and business share risk and rewards.
5	Optimized Process	There are informal and pervasive communications. Value is extended to external partners. Governance is integrated across organizations and partners. There is an IT-business co-adaptive partnership. The scope and architecture evolves with partners. There are education, careers and rewards across the organization.

A.6.2 The IT Service CMM

Description: The objectives of the IT Service CMM are to allow providers to assess their capabilities of delivering IT services and provide guidelines and phases/levels for improvement of their IT service capability. To accomplish these goals, the IT Service CMM measures the capability of the IT service processes implemented in the organization. [12]

Aim: Raise awareness of the current IT Service capabilities and provide an improvement path for organizations.

Scope: IT Services (perspective of providers).

How to Assess: Not described.

Term used to name of the Attributes: Process Areas.

Attributes (21): Subcontract Management; Service Tracking and Oversight; Service Delivery Planning; Service Commitment Management; Service Quality Assurance; Event Management; Configuration Management; Problem Management; Resource Management; Intergroup Coordination; Training Program; Organization Process Focus; Organization Process Definition; Organization Service Definition; Service Delivery; Integrated Service Management; Quantitative Process Management; Service Quality Management; Process Change Management; Problem Prevention; Technology Change Management.

Table 30. Summary of the IT Service CMM levels

Level	Name	Description
1	Initial	The process of delivering IT service is ad hoc, and sometimes chaotic. Only few processes are defined and success relies on individual effort.
2	Repeatable	There are basic service management processes established. There is some degree of repeatability based on past experience.
3	Defined	IT service processes are documented, standardized and integrated in standard service processes. All the services provided by the organization use approved, personalized versions of the standard service processes used by the organization.
4	Managed	There are meticulous measurements for the IT service delivery process and service quality. Service processes and delivered processes are controlled quantitatively.
5	Optimizing	Process improvement is continuous and made possible by using quantitative feedback techniques from both the processes and innovative ideas and technologies.

A.6.3 COBIT 4.1 Maturity Model

Description: This maturity model follows the approach from the Software Engineering Institute CMMI. However, the implementation differs considerably from CMMI that focuses on engineering principles for software development. The model provides a generic scale, which is then specialized for each one of the 34 COBIT 4.1 processes⁷. This maturity

⁷ COBIT 5, which succeed to COBIT .1 does not provide a maturity model. Instead it adopts the ISO/IEC 15504 maturity model.

model enables management to easily place the organization on the maturity scale of six levels and understand what is necessary to improve to the next maturity level if needed [26].

Aim: Enable the comparison of an organization's current implementation of IT processes against industry standards, as well as, the identification of needed maturity improvement.

Scope: IT Management.

How to Assess: Either using the ISO15504 assessment method or using the COBIT's Process Assessment Model. There are IT goals and metrics that define what is expected from IT and how to measure it; then there are process goals and metrics that define what processes must achieve and how to measure it; and finally, there are activity goals and metrics the detail what should happen within each process and how to measure it.

Term used to name of the Attributes: Attributes.

Attributes (6): Awareness and Communication; Policies, Plans and Procedures; Tools and Automation; Skills and Expertise; Responsibility and Accountability; Goal Setting and Measurement.

Table 31. Summary of the COBIT 4.1 Maturity Model levels

Level	Name	Description
0	Non-existent	There are no IT processes implemented and this issue has not been recognized.
1	Initial/Ad hoc	The lack of process definition is recognized as an issue that needs to be addressed. Despite this there are no standard processes. Instead, there are ad hoc approaches undertaken on an individual basis that are unrepeatable. Management is not organized.
2	Repeatable but intuitive	There are comparable procedures being performed by different individual for the same task. No formal training and communication of procedures is in place. Knowledge is concentrated on individuals, which results in errors.
3	Defined Process	There are standardized and documented processes, which are communicated across the organization through training. Process deviation will most likely not be detected.
4	Managed and Measurable	Process compliance and monitoring is in place and acts when processes are not working effectively. There is constant improvement of processes and contains good practice procedures. There is limited tools and automation.
5	Optimized	Processes now fully integrate good practices, based on continuous improvement and maturity modelling examples from other organizations. Workflows are automated in an integrated way by IT, which provides tools that enable the organization to adapt quickly to changes.

A.6.4 IT Capability Model Framework (IT-CMF)

Description: Initially developed by Intel's IT division, the IT capability maturity framework (IT-CMF) is now owned by the Innovation Value Institute (IVI) consortium based in NUI, Maynooth, Ireland [28]. IVI and Intel continue to work closely on joint development of the IT-CMF but now this activity happens under the support of the Intel Labs Europe (iLE) rather than Intel IT division. IVI's membership spans academic, industry, consulting, analyst, and professional bodies around the world. More than 200 companies around the world currently use the IT-CMF. It consists of four main pillars that can viewed as process areas that are then decomposed into critical capabilities (CCs) [29].

Aim: Enable better management and continual development of an organization’s IT capability to deliver higher business value. It consists of four inter-related strategies for improving IT capability, identifying and prioritizing opportunities, reducing costs, and optimizing the business value of IT investments.

Scope: IT Management.

How to Assess: There are two types of assessment, a preliminary first assessment consisting of a questionnaire that can be filled on-line. There is a second type of assessment where a competent assessor that possesses a certification goes to the organization and performs an in-depth assessment of the organizations IT processes.

Term used to name of the Attributes: Main Pillars.

Attributes (4): Managing IT like a business; Managing the IT budget; Managing IT for business value; Managing the IT Capability.

Table 32. Summary of the IT Capability Model Framework (IT-CMF) levels

Level	Name	Description
1	Initial	Management of CCs at this level is ad-hoc and based on individual efforts with no systematic improvement attempts. IT may be viewed somewhat negatively as a necessary expense whose return on investment is hard to measure. Budget planning is almost non-existent.
2	Basic	Some effort has gone into understanding the IT landscape. This may be documented informally or in silos. Some tactical-level shared-thinking is beginning to emerge but not on a joined-up, organizational or strategic basis. IT is viewed as a “cost centre” and seen simply as a technology supplier to the business. Focus is on predictable IT service performance and total cost of ownership.
3	Intermediate	Formal organization-wide documented processes are in place to help understand the IT landscape. It is often possible to identify and address gaps. IT is viewed as a “service centre” and a technology expert. There is a systematic approach to cost reduction. Return on investment is easier to measure and is based clearly on individual business cases.
4	Advanced	Well-established, effective and proven processes exist, which yield a comprehensive picture of the IT landscape. Efficiency is evident; gaps are systematically identified and pro-actively addressed. IT is aligned to business strategies. IT is viewed as an “investment centre”. As a strategic business partner, IT engages actively in long-term strategic budget planning to meet the needs of the organization.
5	Optimizing	IT is enabling and influencing future business strategies. Documented IT processes are optimized for efficiency and regularly reviewed. IT is viewed as a “value centre” and a core competency of the organization.

A.6.5 Group IT Controlling (GITC) Maturity Model

Description: GITC focuses on performing IT controlling to business groups. IT controlling involves using management accounting techniques to the IT domain. These techniques can be calculating the business value of IT, the costs, quality, functionality, as well as, time to delivery. [34][35][36] Applying these techniques to business groups results in GITC which applies these techniques across organizations pertaining to a certain group. This model was developed by the Institute of Information Management at the University of St. Gallen and uses the Design Science Research Method throughout the whole development. This method takes into consideration both the practical and scientific approaches to the maturity model development by following a maturity model development method [41], which is based on Design Science Research and will be described further on in section 5.

Aim: Enable cross-industry benchmarking, as well as, providing an instrument to assess the current state of GITC in organizations and a way to identify improvement opportunities.

Scope: IT Management.

How to Assess: An assessment procedure or method is not described. However, there are succinct examples of how the authors performed an assessment using the framework of Frank [37], as well as, expert interviews.

Term used to name of the Attributes: Dimension / Sub-dimension

Attributes (3/6): Strategy; Process; Information System / Group-wide standardized terms and methodologies; Controlling objects; Utilization of core controlling processes; Repetition of core controlling processes; Data Integration; Data quality.

Table 33. Summary of the Group IT Controlling (GITC) Maturity Model levels

Level	Name	Description
0	GITC not existing	GITC is not in place in the organization.
1	GITC prepared	No standardized terms or methodologies. No performance indicators. No process for IT cost and performance. Data is collected in an ad-hoc basis. No data quality assurance.
2	GITC engaged	Basic standardized terms. GITC focuses on financial performance. There is monitoring of IT costs and performance. Data is collected manually. Basic data quality assurance.
3	GITC established	Standardized terms and basic methodologies. In addition to financial, non-financial performance indicators are also used. There are processes to monitor and plan IT cost and performance. Data collection is partly automated. Quality assurance now takes into consideration various organizational units.
4	GITC managed	Standardized terms and methodologies aligned across organizations. Financial and non-financial performance indicators are balanced. There are processes to plan, monitor, and steer IT cost and performance. Data collection is fully automated. Quality assurance now takes into consideration various systems.
5	GITC optimized	Standardized terms and methodologies aligned and adjusted across organizations. Objects controls are reviewed frequently according to stakeholders' objectives. IT cost and performance, planning, monitoring and steering are continuously improved and aligned. Data collection is fully automated and continuously optimized. Data quality is continuously improved and measured.

A.7. Risk Management

Risk Management is a vital component of Governance. Governance, Risk Management and Compliance (GRC) is a discipline that defends that to effectively manage an organization it is necessary to align the practices of GRC.

A.7.1 Hillson Risk Maturity Model

Description: This maturity model is an earlier example of a risk management maturity model which was created to address the gap found on the implementation of risk management in organizations. [19] At the time this maturity model was developed, despite there being unanimity on the relevance of risk management, successful implementations of risk processes in organizations were sparse. This maturity model consists of four maturity levels which are then linked to four attributes detailing specific criteria for culture, process, experience and application.

Aim: Provide a framework to which organizations that are implementing formal risk management or wish to improve their current approach can benchmark their current state of risk management practice.

Scope: Risk Management.

How to Assess: Self-assessment questionnaire.

Term used to name of the Attributes: Attributes.

Attributes (4): Culture; Process; Experience; Application.

Table 34. Summary of the Risk Maturity Model levels

Level	Name	Description
1	Naïve	The organization does not recognize the need for risk management. There is no approach to deal with uncertainty. Management processes are reactive and repetitive. There is no effort or just little effort to learn from the past and prepare to the future.
2	Novice	There are a minimal number of individuals testing risk management. There is no generic approach to uncertainty being used. The organization is now aware of the benefits of risk management; however, there is an ineffective implementation which hinders the realization of the full benefits.
3	Normalized	Risk management is now a routine business process. Most, if not all projects, have now implemented risk management. Generic risk processes are formalized. The benefits of risk management are understood across the organization, but are not always achieved.
4	Natural	The organization has a risk-aware culture and there is proactive risk management business-wide. Risk information is actively used to improve business processes and obtain a competitive edge. There is now emphasis on opportunity management, the positive approach to risk.

A.7.2 RIMS Risk Maturity Model

Description: The RIMS Risk Maturity Model builds on the knowledge from Enterprise Risk Management (ERM) which aim is to reduce uncertainty and improve the probability of organizations to reach success in their risk management implementation. [54] This maturity model can be applied to any organization irrespective of other risk management related standards that are currently used for guidance. It provides a gap analysis report that can be used as guidance for organizations to prioritize future improvements in their ERM implementation.

Aim: The aim of the RIMS Maturity Model is to provide a structured way of high-lighting aspects that define an effective ERM implementation. This maturity model provides benefits for risk professionals and practitioners, benefits for ERM stakeholders, benefits for organizations, aids in reducing costs and increasing efficiency, has framework compatibility with ISO31000, COSO and ISACA's COBIT, and finally aims at increasing revenue. [54]

Scope: Risk Management.

How to Assess: There is an on-line free self-assessment tool that enables organization to understand where they fit on the maturity scale, available at <http://www.rims.org/rmm>. This model has seven core attributes that describe the fundamental characteristics of an effective ERM process. Each attribute contains subgroups referred to as “competency drivers.” [54] Each competency driver contains supporting key readiness indicators that drive risk management competency in ERM programs. There are 25 competency drivers and 68 key readiness indicators within the seven core attributes. Possible scores for each factor range from high success to low success. Each competency driver scored on a scale of 1-10 for each of three the following assessment dimensions: (1) Capability of ERM activities; Degree of proactivity; and (3) Coverage. Based on the results of the competency driver assessments on the assessment dimensions, the organization is placed on the maturity scale from an informal “Ad hoc” level to a fully realized “Leadership” maturity level.

Term used to name of the Attributes: Attributes / Competency Drivers.

Attributes (7/25): Adoption of ERM-based approach (Executive support of ERM; Business process definition and risk ownership; Far-sighted risk management vision; Front line and support process owner participation); ERM process management (Repeatability and scalability; ERM program oversight; ERM process steps; Risk culture, accountability and communication; Risk management reporting); Risk appetite management (Risk portfolio view; Risk-reward trade-offs); Root cause discipline (Dependencies and consequences; Indicator classifications; Risk (uncertainties) and opportunity information collection; Root cause consideration); Uncovering risks (Formalized risk indicators and measures; Adverse (potential) outcomes as opportunities; Follow-up reporting; Risk ownership by business areas); Performance management (ERM information and planning; Communicating goals; ERM process goals and activities); Business resilience and sustainability (Analysis-based planning; Resilience and operational planning; Understanding consequences).

Table 35. Summary of the RIMS Risk Maturity Model levels [54]

Level	Name	Description
1	Ad-hoc	The organization may be compliant with legal and regulatory requirements, but without consistent, formalized or documented risk management arrangements or processes. Risk management depends on the actions of specific individuals, with improvised procedures and poorly understood processes.
2	Initial	The organization is aware of the need for a formal risk management approach. Risk management processes are structured, but incompletely put into practice. Formalization is on-going but not fully accepted in the organization. Risk is managed independently, with little integration or risk gathering from all parts of the organization. Processes typically lack discipline and rigor. Risk definitions often vary across the organization.
3	Repeatable	Risk management processes are standardized with defined and documented procedures. Risk management awareness may be included in organizational training. A standardized procedure is generally in place with the senior levels of the organization being provided with risk overviews/reports. Risk management is aligned with the organization’s external and internal environment, as well as the organization’s risk profile. The risk management processes are established and repeatable as a standard organizational approach. Risk assessments are conducted throughout departments with the goal of gathering input from the frontline.
4	Managed	Enterprise-wide risk management activities, such as monitoring, measurement and reporting are integrated with measures and controls established. Measurement metrics are standardized and incorporated into the organization’s performance metrics. Mechanisms are in place for alerting management about changes in the organization’s risk profile that may affect the organization’s objectives.
5	Leadership	Risk procedures are communicated and fully understood throughout the organization. Risk-based discussions are embedded to a strategic level, such as long-term planning, capital

Level	Name	Description
		allocation and decision-making. Risk appetite (risk/reward) and tolerances are clearly understood with alerts in place to ensure the board of directors and executive management is made aware when set thresholds are exceeded. There are planned reviews of the risk management program that provide guidance for adjusting/improving application of the risk management principles and processes across the organization.

A.7.3 Deloitte Risk Maturity Model

Description: The Deloitte Risk Maturity Model builds on the premise that there is no definitive maturity level that all organizations should achieve. Instead, there is a level of maturity that is right for each organization, and it depends on how capable that organization needs to be able to manage its risk profile. [56] As such this maturity model recommends regular assessments that can help organizations determine their current maturity level, the level they aspire to reach, and whether the board is getting the amount of information it needs to fulfil its role.

Aim: Help organizations understand where they reside in the maturity path from an initial state towards risk intelligence.

Scope: Risk Management.

How to Assess: Not clearly defined. Some guidelines are provided for the assessment; executives interviews should be performed and a report should be compiled which detail the assessment of the risk management initiative in six areas.

Term used to name of the Attributes: Areas.

Attributes (6): Risk governance, Risk identification and response, Risk assessment criteria, Risk tracking and reporting, the integration of risk management into company processes, Risk-aware culture.

Table 36. Summary of the Deloitte Risk Maturity Model levels [56]

Level	Name	Description
1	Initial	Ad hoc/chaotic. Depends primarily on individual heroics, capabilities, and verbal wisdom.
2	Fragmented	Risk defined differently at different levels of the organization. Risk managed in silos, and risk interactions identified in limited manner. Limited alignment of risk to strategies. Disparate monitoring and reporting functions.
3	Top-Down	Common risk assessment, program statement, policy. Enterprise-wide integrated risk assessments. Communication of top strategic risks to the board. Executive/steering committee. Knowledge sharing across risk functions. Awareness activities. Dedicated team to manage risk.
4	Integrated	Coordinated risk management activities across silos. Risk appetite fully defined. Enterprise-wide risk monitoring, measuring, and reporting. Technology-enabled processes. Contingency plans and escalation procedures. Risk management training.
5	Risk Intelligent	Risk discussion embedded in strategic planning, capital allocation, product development, etc. Risk sensing and early warning risk indicators used. Linkage to performance measures and incentives. Risk modelling/scenarios. Industry benchmarking used regularly.

A.8. Software Engineering Governance

Software Engineering Governance is another subset of Governance that is defined as the set of structures, processes and policies by which and organization manage and control software.

A.8.1 Documentation Process Maturity Model

Description: The Documentation Process Maturity Model is a way of describing in terms of process maturity, capability and practices the way that an organization generates system documentation in a software development process. [14] This maturity model contains four maturity levels and provides an assessment method for the assessment of the maturity level. A level four maturity represents an ideal implementation of the documentation process in an organization. The model and assessment method were based on and influenced by the SEI CMMI as there are key practices, indicators and challenges identified for each of the four levels of the model [31]. The assessment process consists of a questionnaire delivered to each member of the software project team that takes 30 minutes to complete. Then, the answers are used to create an assessment report which shows the current maturity level, as well as, the identification of improvement points and challenges to improve to the next level.

Aim: Raise awareness on the importance of well-established and complete documentation processes and procedures for software engineering projects.

Scope: Generic for Software Engineering.

How to Assess: This maturity model provides an assessment method using 30 minutes interviews with an entire software development team.

Term used to name of the Attributes: No attributes defined.

Attributes (0): No attributes defined.

Table 37. Summary of the Documentation Process Maturity Model levels

Level	Name	Description
1	Ad-hoc	There is chaos and variability, documentation is not a high priority.
2	Inconsistent	There is a documentation policy or standards; there is a mechanism to check that the required documentation is done and there is adherence to the defined documentation policy or standards.
3	Defined	There is a defined process for the creation of documents; there are methods to assure the quality of documentation; there is an assessment of the usefulness of documentation.
4	Controlled	There are measures and analysis of documentation process quality and usefulness; there is a process improvement feedback loop.

A.8.2 Metrics Based Verification and Validation Maturity Model (MB-V2M2)

Description: Software verification and validation (V&V) is the process of checking whether a software product conforms to its specification and whether the software does what the user wants. [16] Despite V&V being a process that has been in use for ages, many organizations still struggle and sometimes fail to implement a comprehensive verification and validation process. Having this in mind, MB-V2M2 aims at providing (1) a set of steps and activities to improve the V&V process; (2) precise V&V maturity models; (3) a method to assess the V&V maturity; (4) measurements to determine the efficiency of improvement activities and (5) metrics to track and control the execution of improvement actions and focus process improvement. [15]

Aim: Create an understanding of what a sound V&V process is, how should V&V process improvement be organized and implemented. Raise awareness of the risks of not having a sound V&V process in place.

Scope: Software Engineering.

How to Assess: Several checklists have been developed to assess the maturity level.

Term used to name of the Attributes: Fundamental Factors.

Attributes (4): People; Technology; Process; Organization.

Table 38. Summary of the Metrics Based Verification and Validation Maturity Model levels

Level	Name	Description
1	Initial	V&V shows that software products work. V&V is performed in an individual and ad-hoc way when time allows and only after coding. V&V works by finding and correcting issues, there is a lack of resources, tools and trained staff.
2	Repeatable	Basic V&V practices are in place but still works as a detection of defects. V&V is performed by executing code but is now achieved in a systematic and managed way.
3	Defined	V&V is embedded into the development life cycle. V&V now verifies the requirements defined in the specification documentation using a defined and repeatable process, documented in methods, standards and procedures. V&V now starts at the requirements phase and is recognized as a profession having a training and career development plan.
4	Managed & Aligned	V&V practices are measured and aligned and is considered as a quality measurement of software products. V&V is controlled using measurements and statistical analysis.
5	Optimizing	V&V is now a full-fledged software product quality control. It is modernized, clear, managed and a repeatable process. V&V is continuously improving. V&V now prevents defects from occurring. Costs, efficiency, and effectiveness are now quantitatively measured.

A.8.3 Model-driven Development (MDD) Maturity Model

Description: The MDD Maturity model is a model that aims at helping organizations introduce MDD. It builds from the fact that several organizations have successfully applied MDD as reported by the Open Management Group [18]. Despite the findings of this report, introducing MDD methods and tools is not a simple task. Implementing MDD in an organization requires organizational change in processes and the overall culture. The purpose of this maturity model is to help organizations in the implementation of MDD by providing an improvement path that organizations can follow to improve their MDD implementation [18]. This improvement path consists of five levels. Each level is then associated to practices, which are activities both specific to MDD and general to software engineering. Each level is also associated with MDD elements which are the artefacts used in MDD, such as, models, transformations, tools and documentation. This maturity model is in line with CMMI and although independent from CMMI it works as complement to it.

Aim: Help organizations implementing MDD so that they reach a level where there are reusable models being used in development.

Scope: Software Engineering.

How to Assess: Not explicitly described. The assessment method is not described, however the assessment will be based in two aspects, for each maturity level, (1) whether the practices and elements are present and (2) whether the elements attributes have the values consistent with the maturity level being assessed.

Term used to name of the Attributes: MDD Practices.

Attributes (3): Engineering; Project Management; Support.

Table 39. Summary of the Model-driven Development (MDD) Maturity Model levels

Level	Name	Description
1	Ad-hoc Modelling	Modelling activities are occasionally used or not used. Individuals may use some models for their own work. There are no policies or common understanding of these models. There are no specific goals on modelling activities or artefacts.
2	Basic MDD	Modelling techniques are identified. The Technical model are defined. Code and documentation is generated from the technical model. The code is completed in order to comply with all the requirements. At a project level modelling tools are selected based on the project objectives.
3	Initial MDD	A business model is defined. Transformations from the Technical model to text are defined. There is separation from generated and non-generated code. Models are checked for well-formed rules; metrics are defined, gathered and analysed. At a project level, a workflow is defined for the MDD projects and modelling activities coverage is decided. There are repositories for models and transformations. Measures of the modelling activities are defined, gathered and analysed.
4	Integrated MDD	An architecture centric metamodel is defined. The domain model is defined. Transformations from the business model to the technical model are defined. Models are simulated. There is a separation from the technical models of the product and the system.
5	Ultimate MDD	Domain specific languages are defined. The metamodels are continuously validated and improved. Transformations from the domain model to the business model are defined. There is a model-based Validation and Verification. Strategic MDD elements are established and maintained.