On the Relevance of Enterprise Architecture and IT Governance for Digital Preservation

Christoph Becker, Jose Barateiro, Goncalo Antunes, Jose Borbinha, Ricardo Vieira

On the relevance of Enterprise Architecture and IT Governance for Digital Preservation

Christoph Becker[1,2], Jose Barateiro[1], Goncalo Antunes[1], Jose Borbinha[1], Ricardo Vieira[1]

[1] INESC-ID - Information Systems Group, Lisbon, Portugal
{goncalo.antunes,jose.barateiro,rjcv,jlb}@ist.utl.pt
[2] Vienna University of Technology, Austria
becker@ifs.tuwien.ac.at

Abstract. Digital Preservation has been recognized as a key challenge in providing trusted information and sustainable eGovernment services. However, there has been little convergence on aligning the technically oriented approaches to provide longevity of information in ever-changing technology environments, and the organizational problems that public bodies are facing, through a systematic framework that aligns organizational and technological issues in the social domain of eGovernment.
In this paper, we discuss the relevance of Enterprise Architecture and IT Governance for digital preservation and analyze key frameworks for digital preservation from this viewpoint. We assess the coverage of the leading criteria catalog for trustworthy repositories in terms of Enterprise Architecture dimensions and in how far these criteria align with established Enterprise Architecture and IT Governance frameworks. We discuss the analysis process we were following and present key observations that result from our work. These point to a number of steps that should be taken in order to consolidate digital preservation approaches and frameworks and align them with established frameworks and best practice models in Enterprise Architecture and IT Governance.

1 Introduction

Recent years have seen an increasing attention to the problems of trustworthy preservation of information as a fundamental part of Information Management. eGovernment efforts have increasingly turned their attention to the problems of trustworthy preservation of information as a fundamental part of their IT Governance responsibilities. An interesting example of this is Austria. In a benchmarking study in 2007, the country scored 100% for online availability and 99% for online sophistication [4] of services. Yet, this clearly did not denote the end of the country's need to focus on eGovernment:

> ... government is not only the sum of its services, it also includes other aspects of citizen-government relations such as accountability, trust, fairness, etc.; aspects that not pertain to service delivery alone but also to service specification, audit, legal rights and responsibilities etc.[16]

These responsibilities include the preservation of digital content created every day and the provision of access in a form that is understandable for a specific audience. And in fact, it took another four years until Austria's national archive acquired a digital preservation solution that enables it to not only offer citizens online services, but also ensure that this and other information will be accessible for future generations. While this primarily points to a "limited vision" of the original benchmarking scale for eGovernment [16], it is also exemplary of how digital preservation came into focus: The increasing usage of digital channels for communication caused a surge in digital material created on a daily basis; but these digital materials, unlike analog materials, require constant attention to stay accessible (and understandable) in ever-changing technology environments.

A recent survey showed that '... many organizations are beginning to make a transition from analyzing the problem to solving it. They remain concerned that mature solutions do not yet exist. Nevertheless, 85 percent of organizations with a digital preservation policy expect to make an investment to create a digital preservation system within two years. Such systems are likely to be componentized, mix-and-match solutions.' [19] Procurement of these systems is notoriously difficult without a clear understanding of the alignment of existing system services and capabilities with the specific processes and components required by a Trustworthy Digital Repository. The leading conceptual model for such an archive is the Reference Model for an Open Archival Information System (OAIS) [11]. However, the OAIS provides only a high-level and narrow view on the required capabilities of such a system and no guidance on business-IT alignment. The "solution architecture" of the OAIS does not necessarily fit in an organization's IT landscape, especially in the case of an already existing Records Management System or Enterprise Content Management System.

The social domain of digital preservation, as it is encountered in eGovernment, embodies a significant amount of Business-IT alignment problems in specific enterprise contexts. In order to preserve digital information, technology must provide adequate support to assure the integrity, authenticity, and understandability of this information through time in an ever changing technological landscape. DP solutions must always be a mix of organizational structures with the related set of activities and services, supported by an adequate IT infrastructure fully aligned with the vision for preservation. The conceptual and technical models developed in the DP community are of tremendous value as focused custom frameworks and documented domain knowledge for a specific community. However, they are not without internal inconsistencies, and many of the aspects covered overlap with well-established areas such as Information Security, Risk Management and IT Governance. There has been little convergence on aligning the technically oriented approaches to provide longevity of information and the organizational concerns that public institutions are facing through a systematic framework that aligns organizational and technological issues. This, however, is the essential focus of Enterprise Architecture (EA), which has received increasing attention in the eGovernment field [3, 16].

	DATA What	FUNCTION How	NETWORK Where	PEOPLE Who	TIME When	MOTIVATION Why
SCOPE (contextual)	List of things important in the business	List of business processes	List of business locations	List of important organizations	List of events	List of business goals and strategies
ENTERPRISE (business model)	Conceptual data/object model	Business process model	Business logistics system	Work flow model	Master schedule	Business plan
SYSTEM (logical model)	Logical data model	System architecture model	Distributed systems architecture	Human interface architecture	Processing structure	Business rule model
TECHNOLOGY (physical model)	Physical data/class model	Technology design model	Technology architecture	Presentation architecture	Control structure	Rule design
COMPONENTS (detailed)	Data definition	Program	Network architecture	Security architecture	Timing definition	Rule specification
INSTANCES (functioning enterprise)	Usable data	Working function	Usable network	Functioning organization	Implemented schedule	Working strategy

Fig. 1. The Zachman Framework

In this paper, we discuss the relevance of EA and IT Governance for digital preservation and analyze key frameworks for digital preservation from this perspective. We assess the EA coverage of a leading criteria catalog for trustworthy repositories, through the Zachman Framework [22]. We further explore in how far these criteria align with established IT Governance frameworks. We discuss the analysis process we were following and present key insights that resulted from our work. These point to a number of steps that should be taken into account in order to consolidate digital preservation approaches and frameworks and align them with established practice in Enterprise Architecture.

The remainder of the paper is structured as follows. The next section outlines related work in the areas of EA and IT Governance. Section 3 discusses frameworks currently dominating the digital preservation discourse. Section 4 uses established frameworks to assess the coverage of concerns in compliance criteria for digital preservation and analyze concerned stakeholders and responsibilities. Section 5 draws conclusions and points to consequences and future work.

2 Enterprise Architecture and IT Governance

Our analysis is scoped by the holistic framework of Enterprise Architecture and strategic alignment. Based on this, we take a closer look at IT Governance and its relevance to the long-term preservation of digital information.

Enterprise architecture (EA) models the role of information systems and technology on organizations in a system architecture approach in order to align enterprise-wide concepts, business processes and information with information systems. The core driver is planning for change and providing self-awareness to the organization [20]. EA strives to provide complete coverage of an organization and as such received significant attention in the defense domain [8] and in eGovernment research [3]. The leading EA frameworks today are The Open Group Architecture Framework (TOGAF) [20] and the Department of Defense Architecture Framework (DODAF) [8]. The Zachman framework is a very influential early EA approach [22]. It describes the elements of an enterprise's systems architecture in a table where each cell is related to the set of models, principles, services and standards needed to address a specific concern of a specific stakeholder, as shown in Figure 1. The rows represent different levels of

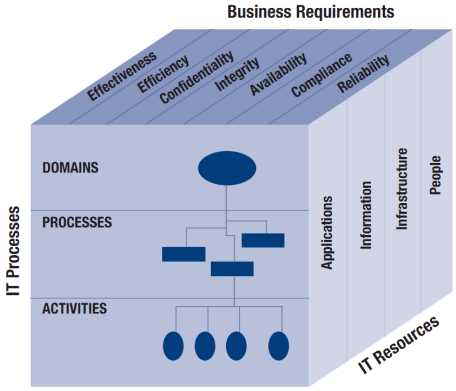

Fig. 2. The COBIT Cube [5]

viewpoints of the organization (Scope, Business Model, System Model, Technology Model, Components, and Instances), while each column expresses a different focus (Data, Function, Network, People, Time, Motivation). This spatial layout and its visual nature makes the Zachman Framework very accessible to a wide range of stakeholders and thus a powerful, yet simple tool for analyzing the scope of domain-specific models.

IT Governance is a key discipline for decision making and communication within IT-supported organizations. The goal is to identify potential managerial and technical problems before they occur, so that actions can be taken to reduce the likelihood and impact of these problems. IT Governance received increasing attention partly because of arising needs of meeting regulatory requirements such as privacy, security, or financial reporting (e.g. Sarbanes-Oxley [14]).

The key IT Governance framework is COBIT: *Control Objectives for Information and related Technology* [5]. COBIT is a set of best practices, measures and processes to assist the management of IT systems. Figure 2 shows the COBIT cube: "IT resources are managed by IT processes to achieve IT goals that respond to the business requirements . . . If IT is to successfully deliver services to support the enterprise's strategy, there should be a clear ownership and direction of the requirements by the business (the customer) and a clear understanding of what needs to be delivered, and how, by IT (the provider)." [5] The framework is not specific to a technological infrastructure nor business area and aims to bridge requirements, technical issues and risks by combining a set of control goals, audit maps, tools and guidance for IT management. This management guide provides a set of processes organized in the domains of (*i*) Planning and Organization; (*ii*) Acquisitions and Implementation; (*iii*) Delivery and Support; and (*iv*) Monitoring and Evaluation. The governance cycle contains processes that address the areas of strategic alignment of IT with the business; value delivery (creation of business value); resource management (proper management of IT resources); risk management; and performance management.

Enterprise Risk Management (ERM) provides a framework that defines prevention and control mechanisms to manage uncertainty and associated risks

Vulnerabilities	**Process**	Software faults	T		
		Software obsolescence	T		
	Data	Media faults	T		
		Media obsolescence	T		
	Infrastructure	Hardware faults	T		
		Hardware obsolescence	T	O	
		Communication faults	T		C
		Network service failures	T	O	
Threats	**Disasters**	Natural disasters	T		C
		Human operational errors	T	O	
	Attacks	External attacks	T	O	C
		Internal attacks	T	O	C
	Management	Organizational failures		O	
		Economic failures		O	C
	Business requirements	Legal requirements			C
		Stakeholders' requirements		O	C

Table 1. Taxonomy of vulnerabilities and threats to digital preservation [2]

and opportunities from an integrated organization-wide perspective. ERM is part of corporate and IT governance, providing risk information to the board of directors and audit committees. It supports performance management by providing risk adjustment metrics to internal control and external audit firms. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) view of ERM is that "Every entity exists to provide value for its stakeholders" [6]. In fact, all entities can face several types of uncertainty, raising a challenge to management on how to deal with such uncertainty in a way that maximizes the value of those entities for the interested stakeholders. The COSO ERM Framework [6] provides a common accepted model for evaluating and aligning effective enterprise-wide approaches to ERM. It defines essential ERM components, discusses key ERM principles and concepts, and suggests a common ERM language.

3 Digital Preservation

Digital preservation aims at optimizing the information life-cycle management, from the creation to the dissemination and use of the information objects, to maintain the knowledge contained in the digital objects accessible over long periods of time, beyond the limits of media failure or technological change, while ensuring its authenticity and integrity [15]. In DP, IT problems and solutions intersect with organizational policies and missions. The complexity of digital preservation increases with the fact that each organizational scenario contains different types of digital objects, each having its own specific requirements.

Digital objects are threatened by *Disasters* caused by operational errors or natural disasters; *Attacks* from inside or outside the organization; *Management* failures of economic or organizational nature; or new or updated *Business Requirements* of legal nature or imposed by stakeholders. To address these threats, an organization needs to manage potential points of failure. *Preservation Processes* can be vulnerable due to faults or obsolescence of software; *Data* can be

vulnerable due to storage media faults or obsolescence; and *Infrastructure* can be vulnerable to hardware faults or obsolescence, communication faults, or failures in network services. Table 1 represents a taxonomy of threats and vulnerabilities with a holistic view on digital preservation[2]. Each threat or vulnerability might be triggered by one or more Technological (**T**), Organizational (**O**), or Contextual issues (**C**).

Digital preservation presents a problem faced by all types of organizations that have to manage information, but initiatives on digital preservation have been pushed largely by cultural heritage institutions [21]. The OAIS Model [11] is a conceptual model, combining an information model with a model of key functional entities. It has provided a common language for the domain and guided the design of preservation systems. The OAIS includes a high-level contextual view of an archival organization and its key stakeholders. It provides a high-level and narrow view of the main functions of a preservation system and prescribes a certain solution architecture that may not be adequate for certain organizations. In particular, it is difficult to reconcile these views with scenarios where an Electronic Records Management System or an Enterprise Content Management System is in place. In Records Management, ISO 15489 [10] and the "Model Requirements for Records Systems' (MoReq2010) have been very influential [9]. The Preservation Metadata Implementation Strategies (PREMIS) working group produced a technically neutral data dictionary for digital preservation linking intellectual entities, objects, rights, events, and agents [17].

Efforts to standardize criteria catalogs for trustworthy repositories with the declared goal of providing audit and certification facilities have led to the "Trusted Digital Repositories: Attributes and Responsibilities' report (TDR) [18], a key milestone for establishing trust in national and international information infrastructures building on the OAIS model. Continuing this path, the Trustworthy Repositories Audit and Certification Criteria and Checklist (TRAC) is currently undergoing ISO standardization. It provides criteria for trustworthiness in the areas of Organizational Infrastructure; Digital Object Management; and Technologies, Technical Infrastructure, and Security [7, 12].

These references are of tremendous value for the preservation community, but they are not without internal inconsistencies and lack conceptual alignment with established IT frameworks. Some even venture into domains such as Risk Management and Information Security, while neglecting a considerable body of knowledge already existing in those areas. From a different system architecture perspective, the project SHAMAN has presented an Information Systems approach to analyzing DP [1]. This first Reference Architecture (SHAMAN-RA) has strong foundations in EA, but is not based on existing domain models to a degree that enables their convergence in a transparent manner.

4 Analyzing Digital Preservation Concerns

Taking an EA viewpoint towards DP, Section 4.1 analyses compliance criteria for trustworthy digital repositories from the perspective of the Zachman Framework.

	Data	Function	Network	People	Time	Motivation	sum
Scope	42	48	2	50	15	97	*254*
Business	253	451	7	115	92	130	*1048*
System	286	408	28	22	62	15	*821*
Technology	31	144	78	13	25	5	*296*
Components	0	23	0	5	0	1	*29*
Instances	41	8	0	20	3	0	*72*
sum	*653*	*1082*	*115*	*225*	*197*	*248*	*2520*

(a) Sum over all criteria

	Data	Function	Network	People	Time	Motivation	Sum
Scope	0	0	0	1	0	2	3
Business	26	31	0	1	10	3	71
System	20	14	0	1	8	2	45
Technology	0	0	0	0	0	0	0
Components	0	0	0	0	0	0	0
Instances	1	0	0	0	0	0	1
Sum	47	45	0	3	18	7	120

(b) Sum over criteria in B4

Fig. 3. Mapping of TRAC in the Zachman Framework.

Section 4.2 takes an IT Governance viewpoint and relates the responsibilities and concerns of key stakeholders to digital preservation compliance criteria.

4.1 Coverage of TRAC concerns in the Zachman Framework

To develop an understanding of the concerns a model covers, the Zachman Framework can be used as a projection space. For instance, TRAC consists of 84 statements of the kind '*B3.2 Repository has mechanisms in place for monitoring and notification when representation information (including formats) approaches obsolescence or is no longer viable.*', each with associated explanation and examples, grouped in 14 areas. In a group exercise, every participant got 10 points for every statement to distribute across the cells of the Zachman framework. Summing these scores over participants, one can obtain a common understanding of the maximum coverage of concerns of single statements, groups, and the totality of statements. Figure 3 displays a visualization of the overall result of such an exercise with 3 participants for the complete TRAC document and for the area B4: 'Archival storage and preservation/maintenance of archival objects' (see Table 4 for the list criteria). This level does not provide a detailed view on specific statements, but it clearly shows that TRAC focuses on functions on data on the business and system levels.

In some cases, an apparent lack of separation of concerns makes the operationalization of criteria a challenge. An interesting example is posed by *B4.4: "'Repository actively monitors integrity of archival objects"'*, which poses the requirement that integrity of content needs to be monitored. This is of course a fundamental concern, which strongly overlaps with the definition of Information Security provided by ISO/IEC 27002:2005: "'preservation of confidentiality, integrity and availability of information"' [13]. The description makes no mention of this standard, but instead describes technical details on the *implementation* approach down to the level of checksums in log files[3]. This one prescriptive criterion alone furthermore spans several rows and columns of the Zachman Framework, affecting 10 cells in a rather direct way. Moreover, instead of simply defining *ends* to achieve, e.g. Key Performance Indicators and thresholds, TRAC often prescribes *means*, i.e. mechanisms on how to achieve desired goals (without being explicit about the goals). By prescribing solutions instead of the core domain requirements, some criteria mix the problem domain with the solution

[3] Cf. [7], p. 34

Name	Description	Sources
Producer/ Depositor	The entity responsible for the ingestion of the objects to be preserved. It may be the owner of the object, but it can also be any other entity entitled to perform this action.	OAIS, TDR, PREMIS, TRAC
Consumer	The entity representing the user accessing to the preserved objects, with a potential interest in its reuse and a certain background in terms of knowledge and technical environment.	OAIS, TDR, PREMIS, TRAC
Designated Community	Defined in OAIS as 'an identified group of potential Consumers who should be able to understand a particular set of information' [11]. This group can be characterized not only by domain knowledge, but also by technical means that are available to it, preferred usage scenarios, etc.	OAIS
Executive Management	The entity responsible for strategic decision making on an organization level, ensuring that the mandate is fulfilled and the repository continues to serve its designated community.	OAIS, COBIT
Repository Manager	The entity responsible for ensuring repository business continuity, defining business strategies and thus setting goals and objectives. That means it defines ends to be achieved by the repository and operates on the business domain, interacting with the designated communities, legal environment and constraints, etc.	SHAMAN-RA
Technology Manager	The entity responsible for technological system continuity and the deployment of technological means to achieve the ends set by the repository business.	SHAMAN-RA, COBIT
Operational Manager	The entity that is responsible for continuous policy-compliant operation of the repository, which involves balancing ends and means and resolving conflicts between them, i.e. constraints as set from Technology Management and Preservation Management.	SHAMAN-RA
Regulator	The entity responsible for external imposing rules concerning the preservation of digital assets, such as legislation and standards. These can apply to the organization, the system's technology, or the systems' usage.	SHAMAN-RA, TRAC
Auditor	The entity responsible for the certification if the organization practices, the system's properties and the operational environments are complying with established standards, rules and regulations.	SHAMAN-RA, TRAC
Repository Operator	The entity responsible for the operation of the repository. This business worker may be aware of the details of the design and deployment of the system, but its mission is to assure the direct support to the business, with no concerns about infrastructure management or strategic alignment.	SHAMAN-RA
System Architect	The entity responsible for the design and update of the architecture of the system, aligned with the business objectives.	SHAMAN-RA, TOGAF
Technology Operator	The entity responsible for the regular operation and maintenance of the components of the technical infrastructure (hardware and software) and their interoperability, according to specified service levels.	SHAMAN-RA

Table 2. Key stakeholders in DP (adapted from [1])

domain, which makes it difficult to address a concern in a systematic way within frameworks of controlled change.

Finally, the flat representation of the TRAC criteria constrains DP to be analyzed in silos, limiting a multidimensional view of the same problem by different stakeholders (from the executive to the operational level). However, DP should be seen as a an enabler to the organizations, where a complete view of the overall concerns becomes visible to the involved stakeholders, making it possible to incorporate this information into strategic and operational planning. The need to have a common knowledge of the same problem by different stakeholders is currently recognized and addressed by established standards in the domains of IT Governance and Enterprise Risk Management.

TRAC group	Responsible	Accountable	Consulted	Informed
A1. Governance and organizational viability	Executive Management, Repository Manager	Executive Management	Technology Manager, Operational Manager, Regulator	Producer, Consumer, Auditor, Repository Operator, System Architect, Solution Provider, Technology Operator
A2. Organizational structure and staffing	Executive Management	Executive Management	Repository Manager, Technology Manager, Operational Manager	Auditor
A3. Procedural accountability and policy framework	Repository Manager, Technology Manager, Operational Manager	Repository Manager, Executive Management	Executive Management, Technology Manager, Operational Manager, Regulator, Auditor, Producer, Consumer	Producer, Consumer, Executive Management, Regulator, Repository Operator, System Architect, Solution Provider, Technology Operator
A4. Financial sustainability	Executive Management, Technology Manager	Executive Management	Repository Manager, Regulator	Auditor
A5. Contracts, licenses, and liabilities	Repository Manager	Repository Manager, Executive Management	Producer, Consumer, Regulator	Auditor

Table 3. Stakeholders concerned with TRAC A: Organizational Infrastructure

Criterion	Responsible	Accountable	Consulted	Informed
B4.1 Repository employs documented preservation strategies	Operational Manager	Executive Management	Repository Operator, Solution Provider	Producer, Consumer, Auditor
B4.2 Repository implements/responds to strategies for archival object storage and migration.	Operational Manager	Executive Management	Repository Manager, Technology Manager, Solution Provider, System Architect	Producer, Consumer, Auditor
B4.3 Repository preserves the content information of archival objects.	Repository Operator	Operational Manager	Repository Manager, Technology Manager, Solution Provider	Producer, Consumer, Auditor
B4.4 Repository actively monitors integrity of archival objects.	Repository Operator	Operational Manager	Technology Manager, Technology Operator	Auditor
B4.5 Repository has contemporaneous records of actions and administration processes that are relevant to preservation (Archival storage).	Operational Manager	Executive Management	Regulator, System Architect	Producer, Consumer, Auditor

Table 4. TRAC criteria in group B4 and concerned stakeholders

4.2 Stakeholders and Responsibilities in Digital Preservation

As COBIT emphasizes, 'Understanding the roles and responsibilities for each process is key to effective governance'[5]. To enable us to establish responsibilities, Table 2 presents key stakeholders generally concerned with digital preservation in an organization that has a responsibility to preserve information. These stakeholders are based on a substantial analysis of domain references in the DP domain that goes beyond the common stakeholders as they are referred to within standard references in DP. They are essentially the result of a reconciliation of established governance frameworks, specialized to cover the variety of concerns specifically relevant in a DP environment.

On this basis, we can analyze which core issues in DP are of concern to which stakeholders, using the common tool of a RACI chart that provides mappings between concerns and the stakeholders that are (R)esponsible, (A)ccountable,

(C)onsulted and (I)nformed. Table 3 provides an overall view of 5 of 14 areas covered by TRAC and associates corresponding responsibilities to the stakeholders of Table 2. In more detail, Table 4 describes all criteria of group B4 (Archival storage and preservation/maintenance of archival information packages) and the concerned stakeholders. Applying this model of stakeholder involvement is seen as a key success factor for effective governance and an essential enabler for improved communication.

4.3 Observations

While space does not allow an in-depth discussion of all criteria and aspects covered by frameworks such as TRAC, the analysis presented in the last section allows us to draw some observations:

- The growing acceptance of standardized frameworks such as COBIT and the COSO ERM framework has not yet had a visible impact on digital preservation practice. In fact, the most prominent risk management approach for repositories, DRAMBORA[4], proposes a generic risk management life cycle and uses the OAIS Model and TRAC for a functional decomposition of repository activities to facilitate risk identification. An integration of these risks into a multi-dimensional enterprise view is required to achieve a common vision of risks and strategic planning in an organization-wide perspective.
- Domain-specific models are very appealing to stakeholders in the domain, since they involve the community, use its terminology, and explicitly address concerns voiced by key stakeholders. However, considering the wider picture of EA and IT Governance, it appears that the coverage of these catalogs and models is often overlapping with established models. Moreover, some criteria are a mix of requirements and solutions and as such not always aligned with best practices (such as a clear separation of concerns) which are considered essential enablers of successful change processes in Enterprise Architecture and IT Governance.
- Analyzing the overlap of TRAC with the ISO 27000 family of standards and COBIT, it seems that several areas of TRAC may benefit from a closer alignment and stronger references to these standards.
- In contrast to best-practice IT Governance, the definition of responsibilities for processes and goals in digital preservation is yet rather vague and informal. Since this is a key success factors for effective governance, it seems advisable to elaborate on explicit responsibilities in future revisions of conceptual domain models for DP.
- For COBIT, capability assessment based on a maturity model is a key part of implementing IT governance: "... maturity modeling enables gaps in capability to be identified and demonstrated to management. Action plans can then be developed to bring these processes up to the desired capability target level." COBIT also defines six information criteria that describe business requirements for information: Effectiveness (timely, correct, consistent and

[4] `http://www.repositoryaudit.eu/`

usable); Efficiency (productive and economical); Confidentiality (protection from disclosure); Availability; Compliance (with laws, regulation and contracts); and Reliability. For an organization that already follows COBIT, a close inspection of these criteria will clarify that DP is in its essence addressing the effectiveness and integrity of information. An extension of COBIT could explicitly address information longevity and integrate DP capabilities into the organization's Enterprise Architecture.

5 Conclusion and Outlook

Meeting DP requirements is in its very nature close to information security and privacy. For many organizations, it is a cross-cutting capability orthogonal to the value chain. However, it has been increasingly found of fundamental importance for enabling the actual value delivery, and intersecting with information, services and technology across the enterprise.

This paper analyzed key frameworks for digital preservation from the perspectives of Enterprise Architecture and IT Governance frameworks. We discussed the coverage and overlaps of the OAIS-based criteria catalog for trustworthy repositories, TRAC, in terms of established frameworks, and discussed stakeholders and responsibilities for DP.

In the light of the observations drawn, a sole reliance on domain-specific models appears a risky endeavor. It seems advisable to rely primarily on established governance models and feed into these the particular knowledge represented in domain-specific models. This should ensure not only strategic alignment between business and IT responsibilities and goals, but also consolidate domain-specific concerns and reconcile potential conflicts between them.

A formal grounding and alignment of DP concerns in terms of EA and IT Governance frameworks is needed to bring together these very distinct communities and enable communication between domain stakeholders responsible for solutions procurement and potential solution providers with a much more IT-focused background. Current work motivated by these conclusions is applying established Enterprise Architecture frameworks to develop a coherent architecture vision for DP *capabilities*. Based on this, we aim to express TRAC criteria as goals and constraints on such a DP architecture and develop an assessment model for DP capabilities in a maturity model aligned with COBIT.

Acknowledgments

This work was supported by FCT (INESC-ID multiannual funding) through the PIDDAC Program funds and by the projects SHAMAN (Sustaining Heritage Access through Multivalent Archiving) and TIMBUS (Timeless Business Processes), partially funded by the EU under the FP7 contracts 216736 and 269940, respectively.

References

1. Gonçalo Antunes, José Barateiro, and Jose Borbinha. A reference architecture for digital preservation. In *Proc. iPRES2010*, Vienna, Austria, 2010.

2. José Barateiro, Gonçalo Antunes, Filipe Freitas, and José Borbinha. Designing digital preservation solutions: A risk management-based approach. *International Journal of Digital Curation*, 5(1), 2010.
3. Beryl Bellman and Felix Rausch. Enterprise architecture for e-government. In Roland Traunmüller, editor, *Electronic Government*, volume 3183 of *LNCS*, pages 48–56. Springer Berlin / Heidelberg, 2004.
4. CapGemini. *7th Measurement*, chapter The User Challenge. Benchmarking The Supply Of Online Public Services. European Commission Directorate General for Information Society and Media, 2007.
5. IT governance institute. CobiT 4.1. framework – control objectives – management guidelinces – maturity models, 2007.
6. Committee of Sponsoring Organizations of the Treadway Commission. Enterprise Risk Management - Integrated Framework, 2004.
7. CRL and OCLC. Trustworthy Repositories Audit & Certification: Criteria and Checklist (TRAC). Technical report, The Center for Research Libraries and Online Computer Library Center, February 2007.
8. Department of Defense, Washington D.C. *DoD Architecture Framework, Version 2.0*, 2009.
9. DLM Forum Foundation. *MoReq2010 - Model Requirements for Records Systems. Draft - v0.92*, 2010.
10. ISO. *Information and documentation: Records management (ISO 15489-1:2001)*, 2001.
11. ISO. *Open archival information system – Reference model (ISO 14721:2003)*, 2003.
12. ISO. *Space data and information transfer systems - Audit and certification of trustworthy digital repositories (ISO/DIS 16363). Standard in development*, 2010.
13. ISO/IEC 27002:2005. Information technology – Security techniques – Code of practice for information security management, 2005.
14. IT Governance Institute. *IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition*, 2006.
15. Maggie Jones and Neil Beagrie. *Preservation Management of Digital Materials: A Handbook*. Digital Preservation Coalition, London, UK, November 2008.
16. Åke Grönlund. Ten years of e-government: the 'end of history' and new beginning. In *Proceedings of the 9th IFIP WG 8.5 international conference on Electronic government*, EGOV'10, pages 13–24, Berlin, Heidelberg, 2010. Springer-Verlag.
17. PREMIS Editorial Committee. *PREMIS Data Dictionary for Preservation Metadata version 2.1*, January 2011.
18. RLG/OCLC Working Group on Digital Archive Attributes. *Trusted Digital Repositories: Attributes and Responsibilities*. Research Libraries Group, 2002.
19. Pauline Sinclair, Clive Billenness, James Duckworth, Adam Farquhar, Jane Humphreys, Lewis Jardine, Ann Keen, and Robert Sharpe. Are you ready? Assessing whether organisations are prepared for digital preservation. In *Proc. iPRES2009*, 2009.
20. The Open Group. *TOGAF Version 9*. Van Haren Publishing, 2009.
21. Colin Webb. *Guidelines for the Preservation of Digital Heritage*. UNESCO Information Society Division – National Library of Australia, 2005.
22. John Zachman. A framework for information systems architecture. *IBM Systems Journal*, 12(6):276–292, 1987.