Long-term Security of Digital Information

Assessment through Risk Management and Enterprise Architecture

José Barateiro, Gonçalo Antunes, José Borbinha
Information Systems Group
INESC-ID
Lisbon, Portugal
{jose.barateiro; goncalo.antunes; jlb}@ist.utl.pt

Abstract - The Digital Preservation community is used to address digital preservation in a problem centric perspective, where the expected common solution is a dedicated *Open Archival Information System Reference Model* compliant system. In this paper we raise a new perspective to address digital preservation as a long-term information security problem ideally addressed in the origin by the initial information system that has created or makes direct use of the objects where, in some scenario, they can be better protected against several threats that can affect their future interpretation and reuse. In order to achieve this goal, we suggest the use of Risk Management processes in collaboration with Enterprise Architecture processes. The relations between these two processes are detailed, showing how each phase of one process can positively influence a phase on the other process. Finally, in order to illustrate this approach, we present a risk assessment of a scenario concerning dam structural safety information.

Keywords: information security; risk management; digital preservation; information systems

I. Introduction

Digital Preservation (DP) intends to ensure that digital objects stay accessible (by users and systems) over long a period of time, guaranteeing the authenticity and integrity of digital objects. Usually, the DP community addresses this problem in a centric and closed perspective, where the expected common solution is an *Open Archival Information System Reference Model – OAIS* [1] compliant system. In this paper we raise the perspective of addressing this issue as a typical information system with specific DP requirements.

Although it is impossible to define all the DP requirements applicable, since they depend, for instance, on the type, size and amount of data, the goals of each organization, etc., the following generic requirements emerge [2]: (*i*) *reliability*, a copy or representation of the digital object must survive; (*ii*) *authenticity*, allowing the identification of the origin/authorship; (*iii*) *integrity*, assuring that the informational content was not modified; (*iv*) *dealing with obsolescence*, avoiding losses due to media, format, hardware or software obsolescence; (*v*) *scalability*, to face technology evolution and the growth of dynamic collections; and (*vi*) *heterogeneity*, also to face technology evolution and allow the refreshment of components to support other requirements.

The above mentioned requirements strongly overlap with the definition of Information Security provided by ISO/IEC 27002:2005 [3]: "preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved". Hence, we consider that DP touches the Information Security arena, in the sense that digital assets must be secured during a long time span. Considering this premise, we propose to look at DP as the Long-term Security of Digital Information.

In fact, DP solutions must "shield" digital objects against several threats, which can affect the future access to authentic digital objects [2]. Actually, protecting digital objects against threats is equivalent to reducing the risk of those threats, which is the main goal of the broad area of Risk Management (RM) [4]. Likewise, Information Security Management Systems are established on top of RM processes [5, 6] to determine and assess security requirements in specific contexts [7, 8]. Thus, the quality of risk assessment is a crucial factor to the success of the overall information security process.

Methods from brainstorming and questionnaires, to complex scenario analyses are commonly used to identify and assess specific risks [9]. However, these methods might be error-prone tasks and subject to human interpretation. To reduce these negative effects, we propose to align the RM processes with Enterprise Architecture (EA), which aims at providing rigorous descriptions of complex socio-technical systems, comprising resources of people, information and technology that must interact in their environment to support a common mission. In this paper, we propose the collaboration between RM and EA processes, showing how they can interact and facilitate the achievement of results. We illustrate this approach, presenting a scenario that deals with information concerning dam structural safety data.

The remainder of this paper is organized as follows. Section II describes the RM process. Next, we present an EA process in Section III. Section IV analyses the alignment between the RM and EA processes. In Section V we apply the proposed strategy to assess the Long-term Security of Digital Information in a scientific scenario. Finally, Section VI presents the main conclusions of this paper.

II. RISK MANAGEMENT PROCESS

RM is a continuously developing arena whose ultimate goal is to define prevention and control mechanisms to address the risks attached to specific activities and valuable assets, where risk is defined as the combination of the probability of an event (threat[1]) and its consequences when exploiting any vulnerability[2] [11].

The ISO/FDIS 31000:2009 RM standard [5] was recently published and defines the principles and implementation of RM to control the behavior of an organization with regard to risk. It is based on the principle that RM is a process operating at different levels, as shown in **Error! Reference source not found.**. The RM process is characterized as the combination of policies and procedures applied to the activities of establishing the context, assessing (identifying, analyzing and evaluating), treating, communicating, consulting, monitoring and reviewing the risks.

First, establishing the risk management context is crucial to identify strategic objectives and define criterions (both internal and external parameters) to determine which consequences are acceptable to this specific context. Second, today's organizations are continuously exposed to several threats and vulnerabilities that may affect their normal behavior. The identification recognizes the existence of risks; analysis examines the nature and severity of the identified risks; and evaluation compares the severity of risks with the defined risk criterions, to decide if the risks are acceptable, tolerable or define the appropriate techniques/controls to handle them.

The identification of threats, vulnerabilities and risks is based on events that may affect the achievement of goals identified in the establishing the risk management context phase. After that, the risk analysis and evaluation estimates the likelihood and impact of risks to the strategic goals, in order to be able to decide on the appropriate techniques to handle these risks (Treat Risks).

The RM process requires a continuous monitor and review activity to audit the behavior of the whole environment allowing, for instance, the identification of changes in risks, or the suitability of implemented risk treatment procedures and activities. Finally, the communication and consultation activities are crucial to engage and dialog with stakeholders.

Indeed, the DP community also recognizes the utility of RM concepts to assess repositories. The Trustworthy Repositories Audit and Certification - TRAC Criteria and Checklist[3] is meant to identify potential risks to digital contents held in repositories. It takes OAIS as its intellectual foundation, and as the benchmark for measuring success in terms of trustworthiness. It establishes appropriate methodologies for determining the soundness and sustainability of digital repositories. The Digital Repository Audit Method Based on Risk Assessment – DRAMBORA [13] process focuses on risks, and their classification and evaluation according to the activities, assets and contextual constraints of individual repositories.

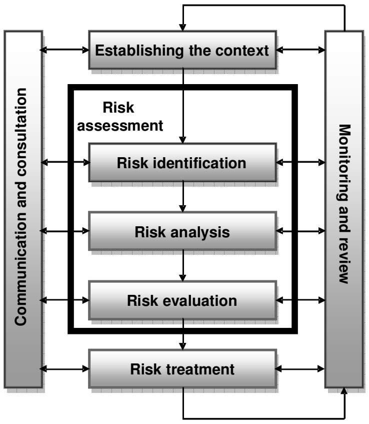

Figure 1. Risk Management Process (ISO 31000)

III. ENTERPRISE ARCHITECTURE PROCESS

The Open Group Architecture Framework (TOGAF) specification [12] provides a detailed method for the development of architectures. Based on the TOGAF principles, we proposed a Reference Architecture Development Method (ADM) for digital preservation [14], comprising six different phases (Figure 2).

The Preservation Strategic Planning phase deals, among other activities, with the definition of the enterprise scope, organizational context, business principles and the architecture principles. Next, the Business Governance phase is concerned with the development of the business governance policies that support the Strategic Preservation Planning.

The Acting and Operation phase models the processes involving stakeholders of the overall environment. The System Building and Support is divided in three sub-phases. The Data Architecture phase determines the data needed to support the effective execution of the activities identified in the Acting and Operation phase, while the Applications and Technology phases define the applications and technology architecture required to support those activities. Finally, the Architecture Realization phase is concerned with the architecture evolution and implementation processes.

The Requirements and Conformance activities must be a continuous practice throughout the application of the ADM. The management of requirements should be dynamic and preservation requirements at all levels shall be identified and stored, fed into and out of all the phases of the development cycle.

[1] Threat is any circumstance or event with the potential to adversely impact an asset through unauthorized access, destruction, disclosure, modification of data, and/or denial of service [10].

[2] Vulnerability is the existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of the computer system, network, application, or protocol involved [10].

[3] The TRAC checklist is available at http://www.crl.edu/PDF/trac.pdf

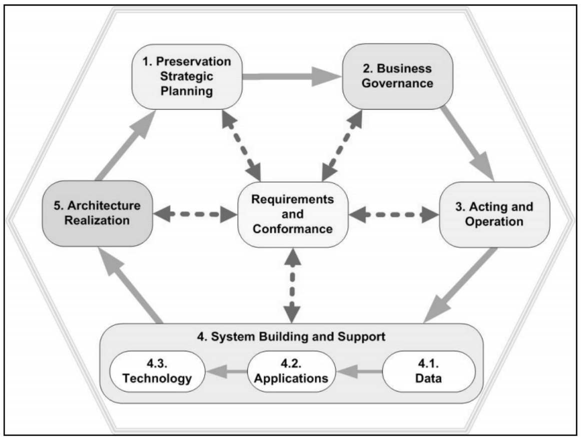
1. Preservation Strategic Planning
2. Business Governance
3. Acting and Operation
Requirements and Conformance
5. Architecture Realization
4. System Building and Support
4.3. Technology
4.2. Applications
4.1. Data

Figure 2. Reference architecture development method

IV. RISK MANAGEMENT VS. ENTERPRISE ARCHITECTURE

Following the proposed approach, Table 1 shows the relationships between Risk Management and Enterprise Architecture processes.

First, establishing the internal and external context involves the perception of key values for stakeholders, trends, organizational culture, legal environment, etc., which are also addressed by the three EA processes: requirements and conformance, when defining/refining the overall requirements; strategic preservation planning, when defining the business and application principles; and business governance, when defining the policies. In this case, both processes can be used as inputs for the other process (e.g., results from a RM Establish the context process can be used when performing the EA Strategic preservation planning).

Second, identifying risks through a systematic analysis approach can be done using the business governance and acting and operation results, to analyze vulnerabilities in current information entities, processes and technology infrastructure, against threats driven from the specified requirements and context. Similarly, risk analysis (e.g., likelihood estimation, consequences) and evaluation (e.g., identify options, establish priorities) can also make use of the rigorous descriptions provided by the EA.

Third, the risk treatment options and plans provided by the RM treat risks process can be used by the EA Architecture Realization process to establish an implementation/migration plan for the overall architecture (this can include the redesign of business processes, replacement of hardware components, etc.).

Fourth, the RM continuous monitoring and review activity is strongly connected to the EA Requirements and conformance that requests information from other activities to update the conformance of the specified requirements with existing deployed solutions

Finally, since the goal of the RM communicate and consult is to establish a communication channel with all the involved stakeholders, this activity crosses all the EA processes, as EA is organized from a high-level planning to the systems' implementation, where each phase is connected to specific stakeholders.

V. DAM SAFETY INFORMATION SYSTEM ASSESSMENT

The safety of large civil engineering structures like dams, bridges or nuclear facilities require a comprehensive set of efforts. The consequences of failure of one of these structures may be catastrophic in many areas. These risks can be reduced by a number of structural and non-structural preventive measures. To support these requirements, the behavior of structures is continuously monitored by (often thousands) instruments (e.g., plumb lines, piezometers) installed in strategic points of the structure. Along with the fact that these monitoring systems can save lives and protect goods, they can also prevent costly repairs and help to save money in maintenance. Thus, it is fundamental to assure the long-term security of the dam safety information.

As proposed in ISO/IEC 27005 [15], we use of a taxonomy of threats and vulnerabilities to digital preservation [2] to accomplish consistent risk assessments and posterior analysis [10]. This taxonomy classifies vulnerabilities in: (*i*) process vulnerabilities, affecting the execution of processes (manual or supported by computational services) that control information entities; (*ii*) data vulnerabilities, affecting the information entities; and (*iii*) infrastructure vulnerabilities, enclosing the technical problems in the infrastructure's components. Threats to digital preservation are classified in disasters, attacks, management and legislation. Management failures are the consequences of wrong decisions that produce several threats to the preservation environment. Disasters and attacks correspond, respectively, to non-deliberate and deliberate actions affecting the system or its components. Finally, legislation threats occur when digital preservation processes or preserved data violate new or updated legislation.

In the scope of the SHAMAN[4] project, the EA process illustrated in Section III was applied to a dam safety scenario managed by the National Laboratory for Civil Engineering[5]. As a result, a set of documents provide a tailored and rigorous description of the overall environment, from the top decision-level to the deployed systems. In order to evaluate the log-term security of this scenario, assessing the risks that can affect its requirements, experts used the taxonomy of threats and vulnerabilities (as a ground basis), and applied the RM process using a system analysis approach [9]. The risk ranking was done using a consequence/probability matrix[6].

The top five risks are summarized in Table II. Using the proposed approach, the identification of the business processes with vulnerabilities that can be exploited (a common requirement, especially in Enterprise Risk Management [10]) is directly obtained from the EA[7].

[4] http://shaman-ip.eu/ (European Commission, ICT-216736)

[5] LNEC – http://www.lnec.pt

[6] Annex B.29 of ISO 31010 [9]

[7] Business process models will be published as a technical report of the SHAMAN project.

TABLE I. ANALYSIS OF RISK MANAGEMENT AND ENTERPRISE ARCHITECTURE PROCESSES

		Enterprise Architecture Process					
		Requirements and Conformance	Strategic preservation planning	Business governance	Acting and operation	System building and support	Architecture realization
Risk Management Process	Establish the context	M	M	M			
	Identify risks	M			EA2RM	EA2RM	
	Analyze risks	M			EA2RM	EA2RM	
	Evaluate risks	M			EA2RM	EA2RM	
	Treat risks	M					RM2EA
	Monitor and review	M					
	Communicate and consult	M	M	M	M	M	M

M: Mutual influence; EA2RM: EA influences RM; RM2EA: RM influences EA

Moreover, the EA also provides the tracking from the business processes level, to the implementation. Though, the summarized results can be extended with related system components, which simplify the evaluation of potential treatment plans.

TABLE II. TOP FIVE RISKS IN THE DAM SAFETY INFORMATION SYSTEM

Risk	Business Processes	Treatment
Loss of Key staff	N/A	Diversifying
Loss of integrity	Manual Data Synchronization; Automatic Data Synchronization; Submission Process; Central Data Store	Preservation Metadata; Secure communications
Loss of authenticity	Local data gathering; Submission Process	Provenance metadata
Media obsolescence	Central Data Validation; Central Data Transform; Central Data Store	Descriptive metadata; Technical metadata; Format migration;
SW obsolescence	N/A	Refreshing; Diversifying; Avoid vendor solutions/technical infrastructure dependences

VI. CONCLUSIONS

This paper intended to motivate the DP community that there is a large spectrum of application of DP concerns outside the traditional “cultural heritage” sector. We believe that in the potential scenarios of application, business requirements have a strong impact within the overall environment, motivating us to address the problem as an Information Security Management System (with long-time requirements), instead of a traditional DP specific system.

A common way to model and address complex business systems is the use of EA descriptions. Thus, we intend to bring the concepts and strategies of Enterprise Architecture into the DP community, using an Architecture Development Method for DP, based on the TOGAF framework. On the other hand, RM is also a prominent technique when considering systems with information security requirements. Thus, we propose to merge the EA and RM to identify the main risks when considering complex scenarios with long-term preservation requirements. The presented work is being successfully applied in several scenarios (cultural heritage, engineering, and *e-Science)* in the scope of the European funded project SHAMAN.

ACKNOWLEDGMENT

This work was partially supported by the project SHAMAN, by the individual grant to José Barateiro from FCT (SFRH/BD/23405/2005) and LNEC, and by FCT (INESC-ID multiannual funding) through the PIDDAC Program funds.

VII. REFERENCES

[1] ISO 14721:2003. Consultative Committee on Space Data Systems. Reference model for an open archival information system (OAIS).

[2] Barateiro, J., Antunes, G., Freitas, F. and Borbinha, J. Designing Digital Preservation Solutions:A Risk Management-Based Approach. In International Journal of Digital Curation. Volume 5(1). pp,4-17, 2010.

[3] ISO/IEC 27002:2005. Code of practice for Information Security Management.

[4] Institute of Risk Management, Association of Insurance and Risk Managers & Public Risk Management Association. A Risk Management Standard. 2002.

[5] ISO/FDIS 31000:2009. Risk Management principles and guidelines.

[6] Stoneburner, G. Goguen, A. and Feringa. A. Risk Management Guide for Information Technology Systems - Recommendations of the National Institute of Standards and Technology. NIST – National Institute of Standards and Technology. 2002.

[7] ISO/IEC 27001:2005. Information security management systems – Requirements.

[8] The Open Web Application Security Project. The Ten Most Critical Web Application Security Risks. 2010.

[9] ISO/FDIS 31010:2009. Risk Assessment Techniques.

[10] Thoits, M. Risk and Insurance Management Society Executive Report on Enterprise Risk Management Technology Solutions. 2009.

[11] ISO/IEC Guide 73:2002. Risk management. Vocabulary. Guidelines for use in standards.

[12] The Open Group. TOGAF Version 9. Zaltbommel, Netherlands: Van Haren Publishing. 2009.

[13] McHugh, A., Ruusalepp, R. Ross, S. & Hofman, H. (2007). The Digital Repository Audit Method Based on Risk Assessment (DRAMBORA). DCC and DPE, Edinburgh. 2007.

[14] Antunes, G., Barateiro, J. and Borbinha, J. 2010. A Reference Architecture for Digital Preservation. iPRES 2010 - 7th International Conference on Preservation of Digital Objects (September 19th – 24th 2010, Vienna, Austria).

[15] ISO/IEC 27005:2008. Information security risk management.