Leveraging DP in Commercial Contexts through ERM

José Barateiro
National Laboratory for Civil Engineering – LNEC
Av. Brasil, 101
1700-066 Lisbon, Portugal
jbarateiro@lnec.pt

Daniel Burda
SAP Research
Althardstrasse 80
8105 Regensdorf, Switzerland
daniel.burda@sap.com

Daniel Simon
SQS AG
Stollwerckstraße 11
D-51149 Cologne, Germany
daniel.simon@sqs.com

ABSTRACT
Until now, digital preservation research has been mainly driven by public or publicly funded organisations. The justification of costs for the preservation is based on abstract risks such as the risk of losing cultural heritage information, or the risk of data deficiencies for current and future research in big sets of data. Typically, the benefits from digitally preserving the objects of interest is difficult or impossible to quantify in terms of return-on-invest. In fact, it is common that memory institutions are mandated to preserve specific digital objects, making digital preservation not an option, but a legal obligation. While in the case of cultural heritage and scientific research qualitative reasons for preservation suffice, enterprises have an additional obligation to quantify the expected benefits and expenses in order to determine the scope of information to be managed and take commercial decisions for or against digital preservation. To provide appropriate means for leveraging the benefits of digital preservation in a commercial context, we argue in this paper that enterprise risk managers are the established function to assess and support decisions about preservation in enterprises. We show that enterprise risk management can be linked to digital preservation and how intelligent enterprise risk management can be utilised to identify the need for digital preservation, determine the corresponding actions, and contribute to the overall commercial success of enterprises.

Categories and Subject Descriptors
H.3.7 [**Digital Libraries**]

General Terms
Management, Measurement, Design.

Keywords
Digital Preservation, Intelligent Enterprise Risk Management, Commercial Use of digital preservation

1. OVERVIEW
The ubiquity of information technology in today's economies results in society's dependency on vital business processes supported and enabled by information technology systems. A vast amount of business, scientific and cultural information assets are created, filed and accessed digitally today. This digital information is a fundamental element for business success.

Society's dependency on digital processes conduces to a high exposure to risks affecting the businesses and the underpinning IT infrastructure. Continued access to digital data cannot be taken for granted [1]. Indeed, any business that deals with information can be subject to several risks that should be actively mitigated by digital preservation (DP) means.

DP can be understood as "the ability to sustain the accessibility, understandability and usability of digital objects ..." [2]. It ensures long-term access to digital information. The meaning of long-term has been defined in the OAIS standard (ISO 14721) as "long enough to be concerned with the impacts of changing technologies, including support for new media and data formats, or with a changing user community. Long Term may extend indefinitely". Accounting for this definition and considering the rapid development in information technology, the challenges of preserving digital information in its notion of an intangible asset becomes more and more pressing [3].

In commercial environments, many businesses are primarily focused on short term returns rather than long term sustainability. If DP methods can also be conceived as a means to mitigate business risks then DP can play an integral role in a commercial context. This paper describes how the European funded project TIMBUS [4] is addressing DP as a risk management activity in enterprise contexts.

The rest of the paper is structured as follows. In Section 2 we briefly describe the state of the industry with regards to Risk Management (RM), Enterprise Risk Management (ERM) and Intelligent Enterprise Risk Management (IERM). Section 3 explains how established RM can be extended to integrate DP. Section 4 explains potential benefits of DP for enterprises. In Section 5 we briefly summarise this paper and provide an outlook into future work.

2. RISK MANAGEMENT IN ENTERPRISES
Enterprises apply RM in their various business fields and have developed sophisticated risk assessment and evaluation methods for business domains such as financial, credit and market risks. While the specific risks vary and are heavily subject to expert knowledge, RM processes and methods have undergone standardisation. In the following, we use the generic ISO 31000 RM standard [5]. It formulates RM as an on-going process embedded in an organisational context. This standard has proven its applicability in our research project TIMBUS [4] and serves as the foundation for integrating RM and DP.

2.1 ISO 31000 overview
The ISO 31000 RM standard defines the principles and implementation of RM to control the behaviour 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 Figure 1. The RM process is characterized by the combination of policies and procedures applied to the activities of establishing the context; assessing (identifying, analysing and evaluating); treating; communicating and consulting; and monitoring and reviewing the risks.

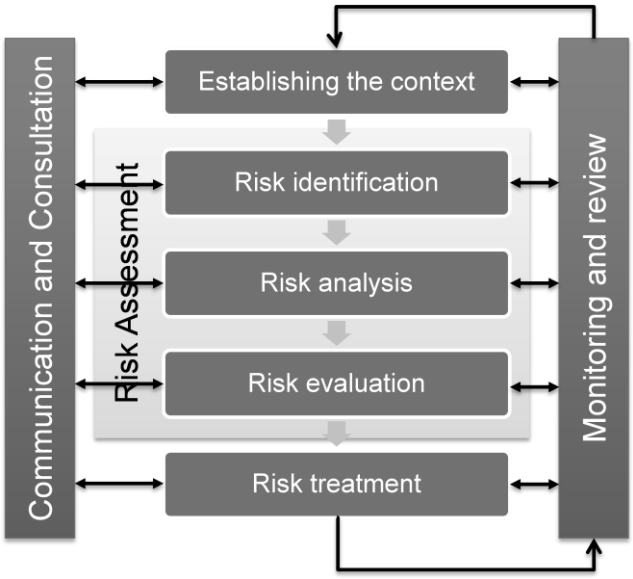

Figure 1. RM process according to ISO 31000

First, establishing the RM context is crucial to identify strategic objectives and define criterions 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 behaviour. 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 RM context phase. Different methods such as brainstorming, questionnaires or inspection support identification of risks. Whatever method used, it is crucial to be as open minded and holistic as possible, because any risk not identified in this step cannot be evaluated in the following steps. For simplifying the understanding and handling, risk managers create taxonomies for risk sources as well as for impact areas. These taxonomies offer the possibility to aggregate the risks to a higher level enabling the required level of abstraction for an effective and efficient RM. To achieve maximum accuracy and completeness, it is best practice to use systematic approaches as offered by Quality Risk Management (QRM) [6] for initialising the identification of risks.

After risk identification, the risk analysis and evaluation estimates the likelihood and impact of risks to the strategic goals as to be able to decide on the appropriate techniques to handle these risks (risk treatment). To determine the likelihood of events and their consequences, probabilities can be estimated and underpinned with indicators. Since the level of risks depends on the effectiveness and efficiency of controls in place existing controls are assessed for their practical relevance to the respective risks. Risk treatment options include:

- avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;
- taking or increasing risk in order to pursue an opportunity;
- removing the risk source;
- changing (for negative impacts reducing) the likelihood;
- changing the consequences;
- sharing the risk with another party or parties (including contracts and risk financing); and
- retaining the risk by informed choice.

The risk treatment step executes per risk the treatment as determined before to reduce the risk and/or to mitigate it. The RM process requires a continuous monitor and review activity to audit the behaviour of the whole environment allowing, 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.

2.2 Application in industry

Many industries implement business changes through projects. Several reference frameworks for project management are established to give guidance when initialising, operating and finalising a project. The most widely-known reference frameworks are PRINCE2 [7], a structured project management framework from the Office of Government Commerce in UK; Project Management Body of Knowledge (PMBoK) [8], a reference to body of knowledge for project management from the Project Management Institute in USA; and IPMA Competence Baseline (ICB) from the International Project Management Association [9].

In project management, a risk is defined as a possible event or circumstance that can have adverse influences on the outcome of a project. RM manages these events, their negative impacts and initiates mitigation actions accordingly. All of the above frameworks cover RM as an integral part. Note that RM does not directly affect or improve project outcomes (e.g., deliverables or work products), but gives additional insights into and transparency about the project outcomes' status and allows for mitigation actions to influence the future course of actions.

While RM is often used in an isolated way (e.g. per business area or per country), ERM breaks the thinking in silos and establishes a holistic enterprise wide management of risks. To address risks at the organisational level and integrating the different views of the stakeholders, ERM provides a framework to manage the uncertainty and the associated threats and opportunities in the context of an enterprise. An example for an integrated model with a strong history in financial auditing is the COSO Enterprise RM framework [10].

The Accenture Global Study [11] reveals a growing importance of ERM. More than 80% of survey respondents have an ERM program in place or plan to have one in the next two years with European companies being the least likely to have an ERM programme (at only 52%). Many companies have started to appoint C-level oversight of the RM function or even establish Chief Risk Officers. The study reveals that 83% of executives expect their investments in RM to increase over the next two years. The bottom line: there is a strongly growing market in RM capabilities and we should aim at triggering DP via RM.

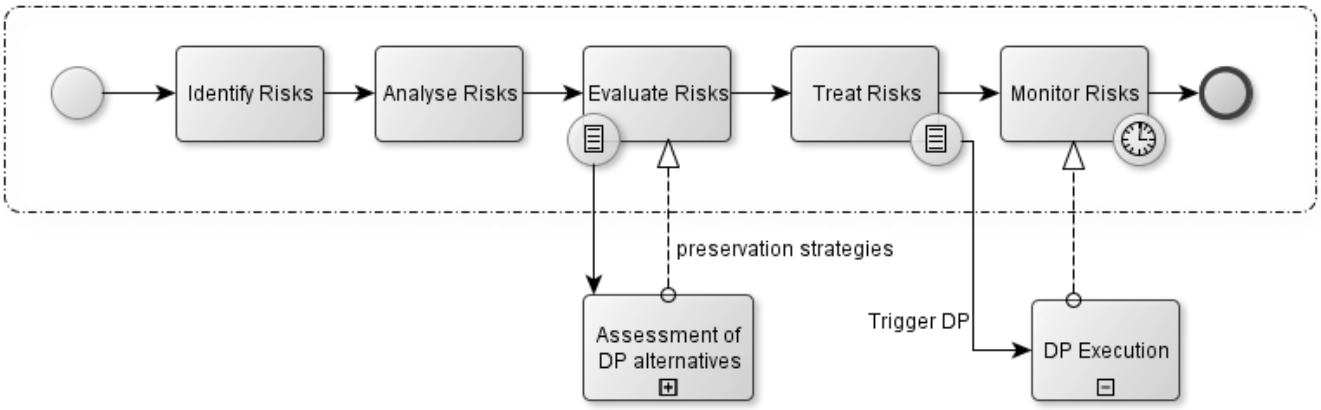

Figure 2. Integration of RM into DP of business processes

2.3 Risk management in digital preservation

The DP community has considered and integrated RM concepts to assess DP repositories. The TRAC Criteria and Checklist [12] is meant to identify potential risks to digital content held in repositories.

The Digital Repository Audit Method Based on Risk Assessment (DRAMBORA, cf. [13]) process focuses on risks, their classification and evaluation according to the activities, assets and contextual constraints of individual repositories. It aims at traditional DP scenarios, providing a catalogue of typical risks in DP environments. In this paper, we take a different point of view with regards to RM and try to elaborate how DP can be beneficial in scenarios where DP is not required *per se*, for example, in enterprises where running business processes are used for commercial purposes [14], [15] or e-Science [16] where the information must be permanently available.

3. DIGITAL PRESERVATION AND RISK MANAGEMENT

DP contributes new aspects to the overall process of ERM in terms of risk identification, risk analysis, and risk evaluation. For certain risks, DP provides effective and efficient means of risk mitigation, i.e., it either eliminates the sources of the risks (e.g., data loss) or at least reduces the likelihood or negative consequences of risks (e.g., availability risks due to failure of disaster recovery).

The goal of DP is the preservation of and within RM, DP provides a toolset for handling and mitigating information related risks. The establishment of interfaces between DP and RM is therefore essential. As shown in Figure 2, the RM process is composed by: *Identify Risks, Analyse Risks, Evaluate Risks, Treat Risks and Monitor Risks*. The *Assessment of DP alternatives* is an external activity used by *Evaluate Risks* to evaluate DP solutions against any other potential RM strategies. Finally, if DP is selected as the treatment action for a particular business risk, the risk treatment process will trigger the archive to start the necessary preservation activities through the *DP execution* process.

3.1 Identify risks

The identification of risks in the organizational context can be extended by identifying risks related to information obsolescence (the original motivation for DP in other areas). In particular, we have identified the following risk areas to be relevant for enterprises:

- Compliance risks;
- Audit risks;
- Business Continuity risks;
- Legal risks, in particular intellectual property (IP) rights;
- Operational risks; and
- Competition risks.

3.2 Analyse risks

After risks have been identified they have to be analysed along the dimensions of their impact and probability of occurrence to obtain an adequate loss estimate representing the financial impact for the organization. We propose a dependency model to systematically investigate interrelations between risks and business processes including their underlying process activities and supportive IT components such as hardware and software.

- Business processes in an organization consist of a defined set of process activities geared towards the efficient execution of a business process.
- The process activities, in turn, are increasingly supported by both internal and external IT components and services.
- The IT components are exposed to different risks, which can result in their unavailability. As a consequence, process activities that are supported or realized by these IT applications cannot be executed. The unavailability or failure an activity has, in turn, an adverse effect on the business process since certain process activities cannot be executed.

To uncover which business processes are affected by which risks, the dependency model can be formalized by the means of three matrices that represent the various layers and their inherent dependencies (cf. [17]):

- Relationship between business processes (BP) and process activities (A) BP×A;
- Relationship between process activities and IT components (ITC) A×ITC; and
- Relationship between ITCs and risks (R): ITC×R.

The first matrix (BP×A) describes the relationships between business processes and its constituting process activities represented by the probabilities of an activity being executed during business process execution. These probabilities can be obtained by means of the business process model. Elements in the matrix can take

values between 0 (activity not part of business process) and 1 (activity part of business process and always executed during business process execution).

The second matrix (A×ITC) reflects which process activities are dependent on particular IT applications. Thirdly, matrix ITC×R represents which IT components are affected by which risks. The relationships are modelled in a binary manner whereby "1" means that a risk affects a specific IT component and "0" means it does not affect it.

To ultimately derive the cause-effect relationships between risks and business processes the three matrices described above have to be multiplied through all layers leading to the matrix

$$BP \times R = (BP \times A) * (A \times ITC) * (ITC \times R).$$

Once the relationships have been identified, it becomes obvious which business processes are affected by which risks and to what degree according to the flow of process activities. Based on those findings risk managers are able to proceed with an adequate determination of quantitative loss values for the organization, reflecting the financial impact for an organization. In an effort to calculate the expected cost of a risk, a widely accepted approach is to build the product of a risks' likelihood and impact level [18]. Determining a risks' likelihood is one of the most challenging parts of qualitative risk analysis since often little historical data are available. In that case, external risk databases can be used to support the determination of the likelihood.

Besides the financial dimension of a risk extant research provides suggestions on additional components of impact attributes that help to better determine the overall risk level [19] as quantitative methods lack the ability to provide a holistic analysis of secondary impacts [20]. Secondary risk impact values are not measured in numeric terms but rather as verbal, discrete statements [21]. Towards the end of a holistic approach that not only considers the direct financial impact caused by a risk but also considering secondary impacts we draw from [22] and suggest a framework of secondary impact attributes to include the dimensions of strategic, reputational, customer and legal impact.

3.3 Evaluate risks

The next step in the process is the assignment of risk classes and the comparison of different risks. For each of the risks identified before, the risk manager determines mitigation actions for risks, i.e., for risks where DP can be used as a mitigation action, he considers DP as risk treatment. As to decide whether DP is a suitable treatment, the following criteria are taken into account:

- cost of DP in different service levels;
- value at risk in business process,
- underlying activities, and supporting IT; and
- residual risk with digitally preserved business process.

3.4 Treat risks with digital preservation

In the area of information related risks, DP can assist at the following three aspects of risk treatment:

- Changing the likelihood of specific risks. Establishing DP is expected to lead to more transparency about business processes in organizations. Many of the risks addressed by DP are caused by informational lack of transparency.
- Change the (negative) consequences of adverse events, e.g., facilitating disaster recovery, enabling business continuity
- Sharing the risk with another party or parties: DP assures availability of information. In this respect, DP will move the information related risk to archive providers who will have to deal with archive related risks.

A full and detailed catalogue of enterprise risks where DP affects has to be developed in the specific context of an enterprise. In general, DP does not focus on domain specific business risks such as credit risk, counterparty risks, currency exchange, etc. but mainly treats information related risks. Since information is derived from data relative to specific contexts, risk identification and DP need to be tailored to the environment as required. Amongst others, DP affects

- Compliance risks;
- Audit risks;
- Business Continuity Management (BCM) risks;
- Legal risks;
- Operational risks; and
- Competition risks

as will be discussed in Section 4.

3.5 Monitor risks

For risks where DP is a feasible treatment, often actions needs to be taken due to changes of technology or the context. In general all changes of a processes context may lead to information related risks. Examples for changing contexts are

- Organisational changes (service providers go out of business or are acquired by a different company); or
- Legal changes (regulation, taxation, IP rights).

From the RM perspective, the Risk monitoring provides the DP governance and management layer in terms of the business. DP planning is triggered when the Risk Manager identifies the need for DP as a mitigation action (or, more general, as a risk treatment). The Risk Manager is responsible for providing a rough business case. After DP planning, the rough cost estimate is validated against the business case and DP design and DP execution are completed.

In case the risk events occur and have the anticipated (negative) impact, the monitoring and control process triggers the DP access step. To this end, any of the risk events as identified in risk analysis can trigger the DP access according to the risk mitigation plan. Additionally, the DP internal monitoring and control process needs to be established to maintain the structure of the digitally preserved business process vitality.

3.6 Roles and responsibilities in RM

To perform the RM process steps described above in an accurate manner that is aligned with an organizational objectives, specific roles and responsibilities need to be defined and assigned within the organization. Therefore, RACI charts have proven to be useful means in the project management arena. A RACI matrix describes the participation by various roles in completing specific activities. Extrapolating to the context of this study, RACI matrices can support the clarification of roles and responsibilities required to perform the RM processes and related DP activities. Extant research indicates that the organizational configuration of DP activities in a corporate context is contingent on internal and external factors. Thus, we propose to employ RACI matrices in support of RM and DP to appropriately assign responsibilities as illustrated in Table 1.

R: Responsible A: Accountable C: Consulted I: Informed	Organizations Management	IERM Manager	DP Manager	Indicator Manager
Risk Evaluation				
Calculate and assess risks	C	RA	C	
Determine risk treatments	C	A	R	
Generate reports		A	R	C

Table 1. Illustration of a RACI matrix

4. DIGITAL PRESERVATION PROCESS BENEFITS

A traditional cost/benefit analysis is an approach to measure benefits and costs. Although, costs for a DP program often do not directly map to costs in other programs, making it extremely difficult for decision makers to create an accurate budget for preservation. In the following, several use cases are elaborated and the respective benefits for the stakeholders of the use case are qualified. The success and acceptance of DP in industry can be fostered if ERM identifies benefits and the specific risks to be mitigated by DP. These benefits can be pinpointed at least to the following use-cases.

4.1 Compliance and Regulatory Requirements

In almost all industries and markets, authorities define rules and regulations for the market players either because the markets are of highest importance for European Society as a whole or the markets are dominated by a small number of big players and the European Monopoly Commission monitors the market behaviour to assure fair pricing for end consumer. Examples for regulated industries and markets are amongst others telecommunications, energy, and banking sectors and the respective markets. To demonstrate market behaviour according to the rules and regulations becomes more and more complex but is ever more closely monitored by authorities and auditors. According to [11], one of the biggest challenges in RM is the implementation of regulatory demands and the compliance with the rules and regulations is the most business critical driver for future activities.

4.2 Transparency on Intellectual Property Rights

In today's commercial environments, business processes and the supporting IT environment demands for proper management of IP rights. Numerous artefacts of different types are utilized and made use of to achieve the overall business objectives. With DP, all relevant artefacts and artefact types are identified during the archiving process, e.g.,

- Services (subscription licenses);
- Software (license keys for applications);
- Databases (licenses for DBMS); and
- Content (videos, pictures, music, text, …).

The different types of artefacts usually come with different types of IP rights. In everyday use, to make use of an artefact protected by IP rights a license from the owner of the respective right needs to be acquired by the user of the artefacts. Even though license management is a standard task in IT Service Management, many companies have room for improvement in the day to day implementation. As different countries have different regulations concerning the treatment of intellectual property right, there is a significant risk that IP rights are violated in daily business and business processes depend on proper licensing. In some cases, companies have been sentenced to pay enormous amounts of license fees to the IP owners. Additional complexity comes from diversification of the IP rights depending on the artefact type.

As part of DP, IP rights for the various artefacts are identified during expediency and tested during exhumation. If exhumation is tested properly (e.g. into an environment sufficiently different from the origin environment), IP gaps such as missing licenses can be detected and fed back to the license management functions.

A second aspect comes into play when the originator of business process, software, or other work wants to prove authorship of certain artefacts. In this case, DP can be used to provide evidence of the state of the art at the time of DP execution. (If a 3rd party intends to open a case for patent rights about a process, software etc. the evidence of 'prior art' can be made by disclosing the DP archive and make use of the archive provider as a 'neutral' witness).

4.3 Long-term Customer Support

Certain industries (like airplane or pharmacy industries) sell products with long lifecycles or the products are based on a rapidly changing technical platform. If a company wants to provide long-term support to their customers either for the products it is worth considering DP as an enabler for long-term preservation of business and product related side products, processes and knowledge.

In IT focussed organisations, often IT service management frameworks (ITSM), in particular, IT infrastructure library (ITIL) [23] as best practise approach is applied to ensure the quality of support. The service operation processes of ITIL as well as a similar process structure in non-IT organisations can be regarded as the set of business processes delivering support for the customer. If an organisation applies the concepts and methods of TIMBUS DP to this set of business processes, long term support for customers can be achieved. In an ITIL based organisation environment, a number of concepts from ITIL (e.g., the Definitive Media Library (DML) where all configuration items including associated items like documentation and licenses) can be re-used in the DP context. DP assures availability and accessibility of significant and relevant information to that even after a long period of time all knowledge required to support a product or a service is retained and preserved even after the service itself has been decommissioned and can be recovered easily.

4.4 Competitive Advantage

Competitive advantage is achieved when an organisation adopts or develops a capability or combination of capabilities that allows it to outperform its competitors. With DP in place, commercial organisations have a number of competitive advantages over other market players with DP.

Firstly, an enterprise that is DP ready has achieved a maturity level that can be actively advertised to its clients. The enterprise has proven capabilities of pro-active and sustainable business process management and can demonstrate to clients its modularisation and standardisation of business processes. In other words, DP ready organisations are well advanced on their path to an industrialised IT and have repeatable and predictable processes. As a consequence of the process oriented work, the enterprise can leverage the benefits of division of labour and make use of out-

sourcing methods to lower costs on one hand. On the other hand, due to internal resources focussing on their competencies the services and products can be evolved and enhanced much faster than in an everyone-does-all working style.

Secondly, in specific environments, DP readiness can be a distinctive feature – e.g., in the public sector, avionics, or defence industry as it shows the long term strategic approach of an organisation to the market.

4.5 Side effects of digital preservation

Establishing DP in organizations is expected to have positive side effects as well as negative ones. The first positive side effect is expected to be an increasing maturity of the organisation. Oriented on the different levels of the Capability Maturity Model Integration the improvement of organisations is correlated with the increasing degree of transparency. As DP needs a holistic transparent view on an organisation, the introduction of DP will automatically increase the maturity.

As DP is about the instantiation of the preserved environment in a new context, it is expected that DP will reduce the dependence of the artefacts to preserve from different persons. In this case DP will advance the enterprise on their way to an industrialised IT.

The increasing awareness for risks laid in information and business processes is expected to improve the awareness for the information and the business processes itself. If both are more present and exposed they can support the role of the business process management. The information about the objects to preserve and the contexts they are embedded will also lead to higher degree of transparency in the business process and the underlying (IT) artefacts.

On the other hand, DP may also lead to negative impacts. At least the instantiation of the archive will cause different efforts like every other entity in organizational processes. As DP is not directly affecting the core business it will lead to higher management efforts and increase administration overheads for the first time. Like every other monitoring activity, the maintenance of the digital archive (analyse the designated community) may slow down the daily business a bit.

An additional negative side effect could be the increased effort needed to address privacy policies within an archive. This will affect different administrative departments in an organization and increase the communication overhead.

5. SUMMARY AND OUTLOOK

In this paper we laid out the enterprise view on DP and how RM can be extended to be an advocate function for DP in commercial contexts. To this end, we propose to argue for DP as a risk treatment for certain business risks and show how DP processes can interact with established RM processes.

As a next step, the processes and concepts described above will be applied and evaluated in several use cases in the course of the TIMBUS project.

6. ACKNOWLEDGMENTS

Parts of this work have been supported by the European Union in the TIMBUS project [4]: “Digital Preservation for Timeless Business Processes and Services”, Grant Agreement Number 269940.

7. REFERENCES

[1] F. Berman, "Got Data? A Guide to Data Preservation in the Information Age," Communications of the ACM, vol. 51, no. 12, pp. 50-56, 2008.

[2] S Rabinovici-Cohen, M G Baker, R Cummings, S Fineberg, and J Marberg, "Towards SIRF: Self-Contained Information Retention Format," in *Proc. of the SYSTOR '11*, Haifa, 2011.

[3] CCSDS. (2011, Oct.) Reference Model for an Open Archival Information System (OAIS).

[4] TIMBUS. (2011-2014). http://timbusproject.net/about

[5] ISO, ISO 31000 Risk management — Principles and Guidelines, 2009.

[6] Frank Simon and Daniel Simon, *Qualitätsrisikomangement*. Berlin: Logos Verlag, 2010.

[7] Office of Government Commerce, *Managing Successful Projects with PRINCE2*., 2009.

[8] William R. Duncan, *A guide to the project management body of knowledge (PMBOK guide)*.: Project Management Institute, 2004..

[9] International Project Management Association, *IPMA Competence Baseline 3.0*., 2006.

[10] COSO. (2012, March) Committee of Sponsoring Organizations of the Treadway Commission. http://www.coso.org/erm-integratedframework.htm

[11] Accenture, "Report on the Accenture 2011 Global Risk Management Study," 2011.

[12] CRL/OCLC, "Trustworthy Repositories Audit & Certification: Criteria and Checklist (TRAC)," The Center for Research Libraries and Online Computer Library Center, 2007.

[13] A. McHugh, R. Ruusalepp, S. Ross, and H. Hofman, "The digital repository audit method based on risk assessment (DRAMBORA)," in *Digital Curation Center and Digital Preservation Europe*, 2007.

[14] J. Barateiro, G. Antunes, M. Cabral, J. Borbinha, and R. Rodrigues, "Digital preservation of scientific data," in *European Conference on Digital Libraries*, Aarhus, Denmark, 2008.

[15] J. Barateiro, "Digital preservation of heterogeneous data," Bulletin on IEEE Technical Committee on Digital Libraries 2009.

[16] D. Marcum and G. George, "The Data Deluge - Can Libraries Cope with e-Science," Libraries Unlimited, 2010.

[17] S. Sackmann, "A reference model for process-oriented it risk management," in *ECIS 2008 Proceedings*, 2008.

[18] B. Suh and I. Han, "The IS risk analysis based on a business model," *Information & Management* , vol. 41, no. 2, pp. 149-158, 2003.

[19] H. Beeck and T. Kaiser, "Quantifizierung von Operational Risk," in *Handbuch Risikomanagement*, L. Johannig and B. Rudolph, Eds., 2000, pp. 633-654.

[20] J. Hargreaves, "Quantitative Risk Assessment," in *Enterprise Risk Management*, J. Fraser and B. J. Simkins, Eds., 2010, pp. 219-236.

[21] H. P. Königs, *IT-Risiko-Management mit System*.: Vieweg + Teubner, 2005.

[22] J. Fraser and B. J. Simkins, *Enterprise Risk Management*.: John Wiley & Sons, 2010.

[23] Office of Government Commerce , *IT Infrastructure Library (ITIL)*.: The Stationery Office, 2007.