Business Process Preservation
How to capture, document & evaluate?

Stephan Strodl
Secure Business Austria
Vienna, Austria
sstrodl@sba-research.org

Daniel Draws
SQS
Cologne, Germany
daniel.draws@sqs.com

Goncalo Antunes
INESC-ID
Lisbon, Portugal
goncalo.antunes@ist.utl.pt

Andreas Rauber
Vienna University of Technology
Vienna, Austria
rauber@ifs.tuwien.ac.at

ABSTRACT

Preserved digital data is often of limited use and value, due to the unavailability of the environment where the data has been generated, executed, analysed, and presented. The preservation of complete processes, including the supporting infrastructure, raises a number of new challenges. In highly computerized firms, processes are often based on service oriented architectures with services provided by third parties. Digital preservation of business processes requires keeping the data, software services and infrastructure available for long time spans. The strong intra- and interdependencies of components make modification and adoption for preservation highly complex. Besides the technical challenges, the organisation and legal aspects of a process need to be considered as well. Contracts for external services, licences for software, access rights to business data and national data regulations for sensible data have to be taken into account when preserving complex information systems.

The TIMBUS project targets the research and development of methods and tools for preserving business processes over time. This poster presents a phased phases approach and the processes to capture and identify the relevant context, plan preservation actions and execute and store business process for the future.

1. INTRODUCTION

The TIMBUS research project[1] aims at providing methods, guidelines and tools to preserve processes for the long term. Current business processes are increasingly supported by service oriented architectures using different external services. Services operated by third parties can disappear over time. Internal software services are also not designed for the long term, since they rely on a number of technologies for execution, for example hardware, input file formats, operating systems and software libraries, which face risks such as obsolescence. In the long run, the availability of current technology cannot be guaranteed. The authentic functionality of business processes in the long term can be violated in terms of missing software services and outdated and unavailable technology. To address the preservation of processes, the TIMBUS project extends its research focus beyond the area of data preservation.

Besides the technical aspects, TIMBUS addresses the organisational and legal aspects of preserving business processes. The legal aspects of preserving information system are manifold, e.g. preservation of personal data and software licences. The technical procedure of a business process goes hand in hand with organisational procedures including liabilities, authorities, rights and roles specification. Thus, the relevant context of a business process needs to be identified and preserved for the future.

[1] http://timbusproject.net

2. TIMBUS APPROACH

The TIMBUS approach to digitally preserve business processes can be divided into three phases: Plan, Preserve and Redeploy (as shown in Figure 1). Digital preservation is seen from a risk management perspective. The Plan phase determines the feasibility and the effort of digital preservation for a business process. A risk assessment of the processes is performed and potential preservation solutions are evaluated in the first phase. The second phase executes the preservation strategy resulting on the capturing of the business process and context from live systems and its preparation for archival storage. The last phase retrieves the process from the archive at some time in the future and re-deploys it for re-execution. We now describe each phase in increased detail.

- **Plan**
  In TIMBUS, the preservation of business processes is based on a risk management approach. In the planning

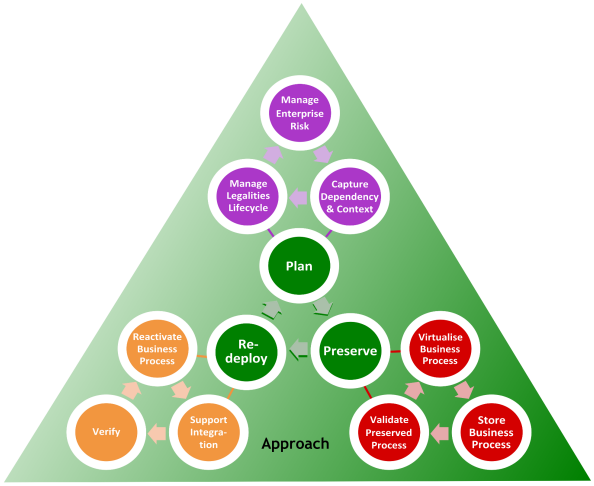

Figure 1: TIMBUS Three Phases

phase a risk analysis of existing business processes is performed. An enterprise risk management process is used based on ISO 31000 [1]. The risks that jeopardize the long term availability of business processes are identified and evaluated. For a detailed analysis of business process, the relevant components and dependencies are captured in a context model. The model describes technical, organisational and legal aspects of a process and their dependencies.

In order to preserve the business process for the long term potential preservation approaches are identified and evaluated against the specific requirements of the settings. The preservation of a business process is a complex task as it requires keeping the data, software services and infrastructure available over the long term, in order to be able to re-run the process in the future, while ensuring that the dependencies between the different components are maintained. One of the research focuses of the project is the preservation of external dependencies, such as web services.

The preservation of the dependencies between the components can be addressed on two levels. On the one hand the detailed dependencies information of software, libraries, services and data can be extracted on the system level. Our approach maintains the connections and identifies compatible alternatives for single components. On the other hand virtualisation is a potential supportive preservation action for complete systems. This approach allows efficient preservation of business processes, including the different components involved and their dependencies. The combination of the two approaches allows efficient preservation of different components and their dependencies of complex business processes. Beside the technical aspects, the organisational and legal aspects of the process also needs to be preserved.

Within the risk management, digital preservation is considered a possible risk mitigation strategy. The risk management is responsible for continuous monitoring of risk factors for active business processes as well as for archived business processes.

- **Preserve**
  In the preservation phase, the business process is captured from the source system. Required preservation actions are performed and the data is prepared for archival storage. Different preservation actions can be applied, for instance, the emulation of external software, the migration of data into other formats or the virtualisation of systems. The dependencies and connection of modified components to other components of the business process need to remain intact over time.

  In order to verify the behaviour and performance of the captured process in the future, validation data is captured. The requirements of the settings specify the significant behaviour and performance measurements that need to be maintained over time. The captured business process is also to be validated for completeness so that it can be redeployed in the future.

- **Redeploy**
  The redeployment phase defines the reactivation of the preserved business process in a new environment at some time in the future. The redeployment procedure needs to be adjusted to the new environment. The required services need to be redeployed on a new infrastructure and the process needs to be installed. The access and usage of the redeployed services and retrieved data need to be adjusted to the new organisational structures and legal conditions. The redeployed business process is then verified against performance measurements of the original process.

3. SUMMARY & OUTLOOK

TIMBUS adopts a risk management approach to consider digital preservation as a risk mitigation strategy for business processes. Digital preservation is used to make a business process, including data, procedures, services and infrastructure, available and useable in the long run. In order to preserve a process the TIMBUS context model allows the capture of the relevant context information of a process. The model captures technical, organisational and legal aspects and their dependencies. Based on the model, risk can be identified and analysed. The model forms also the basis for preservation planning. The assessment of different preservation approaches allows to take decisions considering technical as well as economic aspects. Many business processes build up on service oriented infrastructures, being orchestrations of distributed services. The composition of different services and the technical dependencies of these services expose technical challenges to modify and adopt components for the long term without interfering other services and the process.

Acknowledgments

The research was co-funded by COMET K1, FFG - Austrian Research Promotion Agency and by European Community under the IST Programme of the 7th FP for RTD - Project ICT-269940/TIMBUS.

4. REFERENCES

[1] ISO. 31000: 2009 Risk management-principles and implementation of risk management.