A Risk Integration Framework for the Service-Oriented Enterprise

Eric Grandry, IT for Innovative Services (ITIS) Department, Luxembourg Institute of Science and Technology (LIST), Esch-sur-Alzette, Luxembourg
Christophe Feltus, IT for Innovative Services (ITIS) Department, Luxembourg Institute of Science and Technology (LIST), Esch-sur-Alzette, Luxembourg
Eric Dubois, IT for Innovative Services (ITIS) Department, Luxembourg Institute of Science and Technology (LIST), Esch-sur-Alzette, Luxembourg

ABSTRACT

Enterprise architecture management provides the mechanism for governing enterprise transformations required by changes in the environment. In this article, the authors focus on changes that result from the analysis of information system risks and of their impacts on the services delivered by the enterprise. The authors present how the concepts of an information system risks management domain can be integrated into the ArchiMate enterprise architecture modelling language. This article approaches the conceptual integration in two design cycles: first, this article will consider information security risks, and then the authors generalize to information system risks. Additionally, the authors illustrate the application of the proposed approach and demonstrate the benefits of the integrated model through the handling of a case study, first in the domain of information security, and then in the domain of information privacy. The generalized risk-oriented EA model leads to a risk integration framework for the service-oriented enterprise.

KEYWORDS


INTRODUCTION

To remain competitive in the growing services’ economy, enterprises have to transform themselves in business service-oriented enterprises. Business services are delivered by service system defined as “a configuration of people, processes, technology and shared information connected through a value proposition with the aim of a dynamic co-creation of value through the participation in the exchanges with customers and external/internal service systems” (Spohrer, Maglio, Bailey, & Gruhl, 2009). The value proposition of a service system can be refined into a number of requirements qualifying the expected characteristics of the provided business service. Today, many business services are information intensive, and the achievement of those requirements heavily depends on the properties of the supporting Information System (IS). Our research investigates this type of requirements, and more specifically those associated with information security and privacy: the “security goals” and “privacy goals” according to the usual requirements engineering terminology (Elahi & Yu, 2007). The sources for these goals are customers’ needs but also the many regulations and norms the enterprise has to comply with. The occurrence of security and privacy breaches may result in

DOI: 10.4018/IJISSS.2018070101

Copyright © 2018, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
deviations (misalignments) between the goals of the enterprise and the supporting IS. There are many other goals associated with the IS, like accountability, non-repudiation, auditability, trustworthiness (Cherdantseva & Hilton, 2013), which need to be addressed uniformly.

Given the strong dependency of the business service on the supporting IS, the alignment of the deployed IS with the business service system is a key issue, also from a security and privacy perspective. The purpose of Enterprise Architecture Management (EAM) is to align an enterprise to its requirements and business goals, and specifically to the goals associated with the business services. EAM helps to design and guarantee a coherent enterprise’s organizational structure, business processes, and infrastructure (Lankhorst, 2013) through a set of models.

The solutions to overcome the misalignments are more and more complex and it is not either technically feasible or economically sustainable for an enterprise to solve all potential breaches. Risk Management (RM) is a central process managing the effect of uncertainty on the business goals and is largely used to balance the often-conflicting constraints in information security engineering (NIST SP 800-60). It also becomes the response to the increased concern of personal data protection.

The first objective of the paper is to report about our contribution (Grandry, Feltus, & Dubois, 2013) to the design of a security risk-oriented Enterprise Architecture (EA) model. The core of the framework relies on the integration of Information System Security Risk Management (ISSRM – Dubois, Heymans, Mayer, & Matulevičius, 2010) concepts into EAM constructs from a service system perspective. It also addresses the model representation of risk analysis, leveraging the ArchiMate modelling language (The Open Group, 2016), which has been purposely designed for supporting EAM, and inherently supports the service-oriented enterprise.

The second objective of the paper is to generalize the model to manage the risks on any goals of the information system supporting the delivery of business services, not restricted only to the security goals. This generalised model is validated with a specialisation addressing the privacy goals of the business service. The integration of these additional concerns opens the door to the management of the interactions amongst risks: a control mitigating a security risk can indeed cause risks to breach privacy objectives.

The paper is structured as follows. In the next section, the research methodology is exposed, giving insights on the process followed to elaborate the artefacts. Afterwards, we provide background knowledge regarding ISSRM and ArchiMate EA Modelling language. Then, we describe the initial extended EAM, as a mapping between the ISSRM and ArchiMate metamodel, which is illustrated with a case study. The conceptual integration is generalized and illustrated to information system risks, including information privacy in the next two sections, where privacy risks and information security risks are combined, introducing the concern of risk interaction. We finally review related work and conclude with future perspectives.

**RESEARCH METHODOLOGY**

According to Hevner, March, & Park (2004), the design science paradigm seeks to extend the boundaries of human and organisation capability by creating new and innovative artefacts, and the authors further maps their defined artefact to the four artefacts proposed in the research framework from March & Smith (1995), i.e.: construct, model, method and instantiation. This framework prescribes four research activities: build and evaluate, and theorise and justify. The first two refer to design sciences activities, whereas, the latter two concern the natural science activities.

Our development of a metamodel integrating the concepts of both ISSRM and EAM is a research that is in the scope of Design Science Research. We focus on the build activity (i.e., integration of the risk management and the enterprise architecture into an integrated model) and evaluate activity (i.e., validation of the metamodel through case studies).

In practice, we note the build and evaluate design activities are preceded, in most design science research methods, by an activity of problem discovering (e.g., Peffers, Tuunanen, Rothenberger, &
Cyber Crime and Challenges of Securing Nigeria's Cyber-Space Against Criminal Attacks
www.igi-global.com/chapter/cyber-crime-and-challenges-of-securing-nigerias-cyber-space-against-criminal-attacks/210942?camid=4v1a