The Risk-Aware Enterprise Architecture: Towards a Transparent Inventory of IT Risk Management Artifacts

Manfred Pauli, Michael Schermann, Helmut Krcmar

iteratec GmbH
Inselkammerstraße 4
82008 München
manfred.pauli@iteratec.de

Chair for Information Systems
Technische Universität München
Boltzmannstraße 3
85748 Garching
{michael.schermann|krcmar}in.tum.de

Abstract: A risk inventory provides an integrated view on risk management artifacts, e.g., risks, risk controls, and performance indicators. In this paper, we show how adapting the enterprise architecture management processes (EAM) may provide a foundation for an integrated IT risk inventory. Based on a design research approach, we develop a systematic approach for integrating the disciplines of risk management and enterprise architecture management. We demonstrate the utility of our approach by evaluating an identity management solution in a large bank.

1 Introduction

Although risk management is commonly named as one of the top challenges in information management, risk managers and CISOs struggle with establishing and maintaining transparency over sources for risks, implemented risk controls, and their effectiveness [Pa07, SS08]. In particular, little data is available for forecasting the future impact and probability of an *IT risk* compared to other risks, e.g. in the insurance industry [SS08]. Thus, risk management commonly relies on a very laborious process to extract experts' estimations, which often results in risk assessments of uncertain quality. However, organizations may tap a source of relatively objective data: their enterprise architecture as the formal description of an organizations' IT. [TOG07]. Hence, our research question is: *What are the benefits of integrating risk management and enterprise architecture management?*

The paper follows the design research methodology as suggested by [He04]. Hence, we first argue that risk management lacks of high quality data and that enterprise architecture management (EAM) may provide this foundation. Subsequently, we present a process model that shows how to integrate the disciplines of EAM and IT risk management. We demonstrate the utility of our approach by evaluating an identity management solution in a large bank. The paper closes with a critical appraisal of our approach and points out future avenues of worthwhile research.

2 The Enterprise Architecture as a Foundation for Decision-Making in IT Risk Management

The IT risk management process generally consists of identifying and analyzing risks, plan and implement risk responses and risk monitoring [La06]. There is a plethora of techniques to manage IT risks. When assessing risks, the risk management team has to look at every risk and estimate its probability and its potential impact. The team relies on the experiences of the team member or other expert's estimations. However, experience and estimations can be very erroneous [Sc03]. Furthermore, information on the effectiveness of risk controls is required to justify investments and monitoring risk management efforts.

Risk indicators …

One way to handle this problem is using risk indicators [SS08, He07]. A risk indicator is a variable which has a causal relation to one or more risks [He07]. Usually, a risk indicator exhibits a tolerance levels as well as rules for exception handling [Wi08]. Both, researchers and practitioners, argue that risk indicators will play an important role in risk management, since they provide direct information on the current risk situation as well as on the effectiveness of the risk management process and [Wi04, Ja07].

… and where to find them

Since the objective of enterprise architecture managements (EAM) is to document, plan, control, and monitor the strategic and operational aspects of an organizations' enterprise architecture, we argue that both causes and effects of IT risks manifest in the components of an enterprise architecture.

Commonly, enterprise architectures (EA) follow a hierarchical multi-layer approach [Ha09]. The upmost layer describes the business processes within an organization. The next layer contains the application systems. The following layer specifies the components of the application systems: the technical architecture and infrastructural elements. Projects are cross-cutting concerns across all three layers. Hence, the EA illustrates the relationships between business objectives, business processes, and the components of deployed and planned application systems. Commonly, each element of an EA is called building block and is of a particular building block type.

Furthermore, common EAM methodologies revolve around identifying and maintaining useful indicators to represent the important aspects of enterprise architecture. We argue that these indicators may serve as foundation of developing risk indicators. Hence, EAM provides a high quality data base for risk analysis and justifying decisions in risk management.

3 Towards a Risk-Aware Enterprise Architecture

A typical EAM process begins with the documentation of the existing IT infrastructure, the business processes and their relationships. The next step is to characterize the elements of the IT infrastructure by representing them with different attributes and assigning current and planned values. As soon as a transparent view on the IT infrastructure exists, planning the target shape of the IT infrastructure begins. Finally, the steps of the plan will be addressed by specific projects. Since business requirements will change over time, EAM is an iterative task.

Figure 1 shows our process model to tap EAM as a specific information provider for IT risk management. As discussed above, the first step (1) of the IT risk management process is to identify IT risks resulting in a list of IT risks. Then, each risk is represented as a set of risk indicators (2). However, the values of such risk indicators must relate to building blocks of the enterprise architecture (3). For instance, password security metrics apply to systems with access control only. Subsequently, risk managers deduce a meta-model of identified IT risks, risk indicators and associated building blocks. Next, the risk indicators are being associated with values from the EA (4). For instance, the availability of system A is 95 percent whereas system B has 98 percent availability. Subsequently, each building block should be analyzed whether it may provide information on a particular risk indicator. Since there will be a lot of values to a single risk indicator, they have to be extracted (5) and presented to the risk management experts for aggregation and focus (6). Finally, risk controls are being reflected by setting up particular project in the process of EAM (7). Again, it is possible to attach specific indicators that provide information on the performance and goal congruence of the decisions.

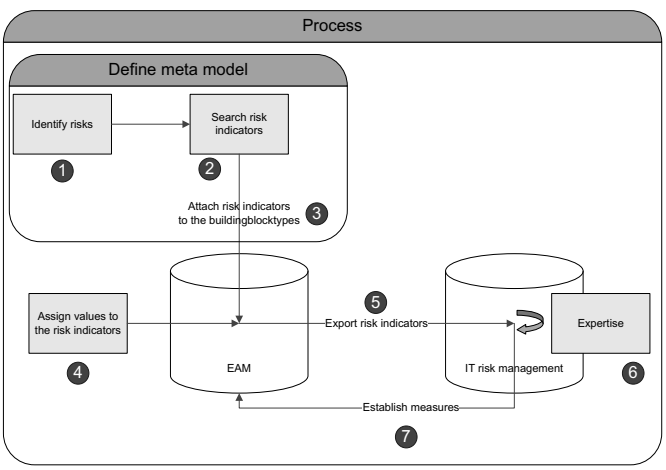

Figure 1: Integrating EAM with IT Risk Management

The presented process provides a generic integration of EAM and IT risk management. In the following, we demonstrate the utility of our approach by evaluating an identity management solution in a large bank.

4 Case Study: Does identity management improve the risk situation?

The following example illustrates the above presented process. We conducted a case study with the IT infrastructure of the bank 'RiskBank[1]' provided by an EAM tool provider. The EA of the RiskBank represents a large IT infrastructure with more than one hundred different application systems. Usually, new risk controls are recommended by specialized application providers or consulting companies. For instance, the fictive company IdentitySolutions offers the CISO of RiskBank a new identity management system called IMS. The system claims to reduce the risk of identity theft resulting from the complex IT landscape [Al08]. IMS consists of training courses for the staff, single-sign-on functionality, password self management, user account management, authorization management and user activity logging.

In the following, we evaluate IMS regarding its effects on the IT infrastructure and the risk situation of RiskBank. As discussed above, the first step is to identify IT risks. The heading of Table 1 shows an extract of the list of considered risks, following the pattern "risk category:risk origin". The categories follow the guidance of Basel II [Ba03]. After having identified the IT risks within the company, the IT risk manager attaches risk indicators to the different risks. One indicator can also be applied to different IT risks. Table 1 shows the assignment of risk indicators to the identified IT risks. The next step is to link the risk indicators to building blocks.

Table 1: Extract of RiskBank's risk indicators [adapted from Wi04, KPI08]

Risk	**Security:Staff**	**Security:Syst**	**Secur Influe**	**Security:F**	
Risk indicators	# Authorized employees	# Password recoveries p employee p	# Criminal intrusions per	# Parti person accour	Logging employe activitie
	# Password loss per employee pe	Password	-	Average tim create an acc	-
	# Security traini	Average tim	-	System h separate	-

Each of the risk indicators listed in Table 1 is attached to building blocks of the type 'application system'. The risk indicators "# Authorized employees" and "# Criminal intrusions per year" are also attached to the infrastructural elements. This step results in a meta-model that contains IT risks, risk indicators, building block types and the relationships among them.

[1] RiskBank is a pseudonym to provide anonymity.

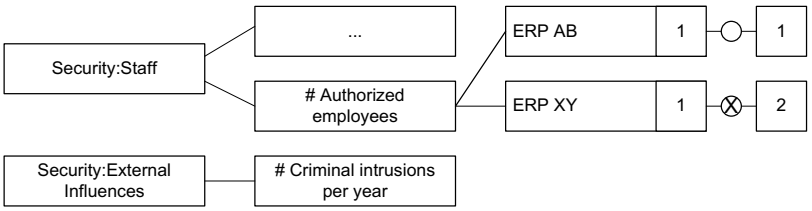

Figure 2: Number of outliers per risk indicator

The next step is to instantiate this meta-model by assigning values to the risk indicators. To do so, the risk management team goes through the enterprise architecture and assigns values from different building blocks (see Figure 2). For example, the indicator '# Authorized employees' for 'ERP XY' has the value '2', i.e. more than system owner that has full access control exist (see Figure 3). The sources of the values can vary. The most confident sources are any results of logging, pinging, and similar actions. The result is a comprehensive and detailed representation of the IT risk situation.

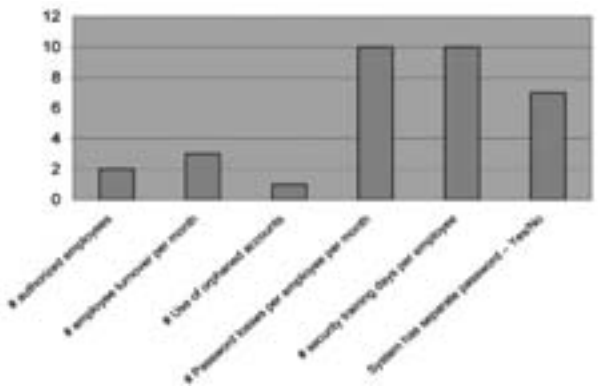

Figure 3: Number of outliers per risk indicator

However, preparing decision making requires aggregating the indicators. At 'RiskBank', we summed up the number of outliers per risk indicator. For instance, we found that the indicator "# Password losses per employee per month" was beyond its tolerance level. In particular, the underlying building blocks were crucial systems at 'RiskBank'. However, these systems were used for particular accounting purposes only and were commonly with separated access control ("System has separate password"). Hence, employees tended to forget the passwords. Thus, the functionality of 'single-sign-on' of the IMS proposal would provide appropriate means to control the associated risks. Although this example is of simplified nature, it shows the benefits of integrating IT risk management with enterprise architecture management. For instance, the IMS could be instantiated as a project in the enterprise architecture and the risk indicators would serve as key performance indicators of the project. Hence, risk managers are able to actually show the benefits of risk controls.

5 Conclusion & Outlook

This paper argues for the enterprise architecture as a solid and reliable source of information for IT risk management. We suggest risk indicators as an approach to establish an integrated information source. The results of the case study show that quantitatively grounded decision-making in risk managements does not require estimating probabilities and potential impacts. The demonstration shows that our approach focuses on the potential effects of risk controls and thus enable risk managers and decision makers critically appraising new trends, products, and services from the IT security industry. In sum, this paper presents an effective approach for grounding decision-making in IT risk management in available data [SS08]. Future research focuses on enhancing the visual representation of risk indicators [Te99].

References

[Pa07] Parker, D.B., Risks of risk-based security. Communications of the ACM, 2007. 50(3): p. 120.

[SS08] Shostack, A. and A. Stewart, The New School of Information Security. 2008, Upper Saddle River, NJ, USA: Addision-Wesley.

[TOG07] The Open Group, The Open Group Architecture Framework (TOGAF). 2007, The Open Group,: San Francisco, CA, USA.

[He04] Hevner, A.R., et al., Design Science in Information Systems Research. MIS Quarterly, 2004. 28(1): p. 77-105.

[La06] Landoll, D.J., The security risk assessment handbook: a complete guide for performing security risk assessments. 2006, Boca Raton, FL, USA: Auerbach Publications.

[Sc03] Schneier, B., Beyond Fear: Thinking Sensibly About Security in an Uncertain World. 2003, Berlin: Springer.

[He07] Herrmann, D.S., Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience, and ROI. 2007, Boca Raton, FL, USA: Auerbach Publications.

[Wi04] Witty, R.J., K. Brittain, and A. Allan, Justify Identity Management Investment With Metrics. 2004, Gartner, Inc.: Stamford, CT, USA.

[Ja07] Jaquith, A., Security Metrics: Replacing Fear, Uncertainty, and Doubt. 2007, Upper Saddle River, NJ, USA: Addison-Wesley.

[Ha09] Hanschke, I., Strategisches Management der IT-Landschaft: Ein praktischer Leitfaden für das Enterprise Architecture Management. 2009, München: Hanser.

[Al08] Allan, A., Identity and Access Management Technologies Defined. 2008, Gartner, Inc.: Stamford, CT, USA.

[Ba03] Basel Committee on Banking Supervision, Sound Practices for the Management and Supervision of Operational Risk. 2003, Bank for International Settlements: Basel, Switzerland.

[KPI08]. KPI Library. Information Technology. 2008 [cited October 06, 2008]; Available from: http://kpilibrary.com/category/itman/.

[Te99] Tegarden, D.P., Business information visualization. Communications of the AIS, 1999. 1(1): p. 1-38.