Enterprise Architecture Risks - An Overview

AISA Project Report

Version: 1.1	Date: 6.3.2008
Author: Eetu Niemi & Tanja Ylimäki	Status: Final

Abstract

Enterprise Architecture (EA) is a modern approach for managing and developing organizations and enabling them to tackle with the challenges induced by constant changes and increased complexity in their environment. However, as an extensive and strategically important program, EA is not without risks. Therefore, this exploratory study aims at 1) providing an overview of generic risks that can potentially be related to EA in organizations, 2) suggesting a classification scheme for the risks to facilitate their management, and 3) discussing the nature of EA risk management. Data is collected by a literature review and a focus group interview of practitioners involved in EA. As a result, a classification scheme for EA risks is suggested, potential risks related to the elements of the scheme presented, and EA risk management discussed.

Contents

1 Introduction

In the modern turbulent business environment, companies are constantly encountering challenges in coping with the changes and complexity in the market. Moreover, the companies have to manage the complexity of their information and communication technology (ICT) environment brought on by the many decades long legacy of ICT, and to assure that ICT supports the business as well as possible. To facilitate companies in responding to these challenges, a recent approach called Enterprise Architecture (EA) has emerged in the last decade (Veasey 2001; Morganwalp and Sage 2004; Goethals et al. 2006; Hjort-Madsen 2006; Kluge et al. 2006). Consequently, the approach has become one of the major concerns of practitioners and academics, and it is being implemented in a multitude of companies and government organizations worldwide.

Basically, EA is a holistic approach for managing and developing an organization, adopting an overall view of its business processes, information systems (IS), information and technological infrastructure (de Boer et al. 2005; Kaisler et al. 2005; Jonkers et al. 2006). EA includes a set of principles, methods and models used to describe the current and future state of an organization, as well as a transition plan top describe the steps needed to transform from the current to the target state (Armour et al. 1999a; Lankhorst 2005). The transformation is usually conceptualized as a continuous, iterative process (Armour et al. 1999b; Kaisler et al. 2005; Pulkkinen and Hirvonen 2005).

EA can be conceptualized from a number of different viewpoints. These include products (and services), processes (Armour et al. 1999a; Jonkers et al. 2006; Rosen et al. 2007), implementations (c.f. Armour et al. 1999b; Kaisler et al. 2005) and impacts (Morganwalp and Sage 2004; Jonkers et al. 2006). EA processes include a collection of planning, development and management processes (Armour et al. 1999b; Pulkkinen and Hirvonen 2005). EA products, in turn, include e.g. EA principles, methods and models (Armour et al. 1999a; Lankhorst 2005), which can be complemented with various services, for instance EA guidance (Armour and Kaisler 2001; The Open Group 2006). Since a typical use for EA is its implementation, it can also be considered a separate viewpoint. Implementations include organizational elements (e.g. organizational structures, processes and information systems) implemented according to or in compliance with EA (Armour et al. 1999b; Kaisler et al. 2005), and other usage of EA in the organization's functions, such as strategy management, investment management, project definition and support, IT governance and system development (Rehkopf and Wybolt 2003; Lankhorst 2005; Bucher et al. 2006; Andersin and Hämäläinen 2007; Emery et al. 2007). EA impacts, on the other hand, may arise from all of these viewpoints.

Because EA is an extensive program, it requires considerable investments and may thus result in many political, project management and organizational challenges (Kaisler et al. 2005). As with any investment, also EA investments (investments related or driven by EA) involve risks which need to be identified and managed (Saha 2006). Organizations investing in EA may face unexpected materialized risks related to business and ICT alike, threatening the success of the EA program. Moreover, since EA is a critical management tool materialized risks can have serious consequences in the organization utilizing EA.

The extensive, continuous and iterative nature of the approach further complicates EA risk identification and management. Unpredictable effects may arise from EA processes (e.g. planning,

development, management, maintenance and use) or may be associated with any of the levels of EA products (e.g. business, information, information systems, technology) (Baldwin et al. 2007). Being such a fuzzy target, research on EA is fragmental (see e.g. Niemi 2007), and on the subject in question extremely scarce. However, risks have been extensively discussed in generic risk literature (see e.g. Crouhy et al. 2001; Lam 2003; Reuvid 2005) and even in specific contexts such as ICT and IS (see e.g. Boehm 1991; Benaroch 2002; Sherer and Alter 2004; Keyes 2005; Benaroch et al. 2006).

In this exploratory study, we aim to provide an overview of generic risks that can potentially be related to EA in companies and to investigate classification schemes for the risks to help tackle with the multitude of potential risks. Moreover, we aim to discuss the nature of EA risk management and its connection to organizational risk management. Consequently, the study contributes to practice and research alike. For practitioners, the results provide a list of risks associated with EA, which can be used as a checklist in risk identification, and initiate discussion on EA risk management. For researchers, the results provide a basis for developing identification and mitigation strategies for the presented risks, and conducting further research on EA risk management.

This report is organized as follows. First, we describe the research process and methods used. Second, we discuss the theoretical background of the study. Third, we present the classification scheme of EA risks selected for this study. Fourth, we give an overview of generic risks related to EA. Fifth, we discuss the nature of EA risk management. The report ends with summary and conclusions.

2 Research Process and Methods

This study employed the qualitative research paradigm and used literature review and focus group interview as methods for gathering information. The study was structured as follows:

1) *Literature review* was carried out systematically. First, generic literature on risks was charted using high-quality academic databases and generic search engines on the internet to provide an overview of risks encountered in organizations. Subsequently, literature on risks related particularly to EA, business and ICT was similarly charted to supplement the overview. Literature by both academia and practitioners was included in the review for a more diverse perception. The sets of risks identified in literature were compared by the authors to assess their completeness and suitability to the EA context. Furthermore, potential classifications for the risks were charted and one feasible classification scheme was adopted to facilitate comprehension of the review results. The classification also included a set of generic risks to be used as a basis for discussion in the next phase of the study. A suggestion of the nature of EA risk management was also made according to literature.
2) *Focus group interview* (see e.g. Krueger and Casey 2000) of 5 practitioners from three Finnish organizations carrying out EA work was organized. The organizations were either independent companies, or parts of domestic enterprises. Moreover, they represented different industries and employed from under 20 to several thousand people. The objectives of the interview were 1) to validate the literature review results in a practical context, and 2) to collect additional, experience-based information. Notes were taken from the interview and it was also audio-recorded.
3) *Consolidation and analysis of the results* was done by combining the results from the literature review and the interview.

3 From General Risks to Enterprise Architecture Risks

This section describes the combined results of both the literature review and the focus group interview.

3.1 Definitions and Conceptualizations of Risk

The Collins English Dictionary defines risk as "the possibility of incurring misfortune or loss". However, in risk literature many authors do not even provide a definition for the term. This may be partly explained by the complex nature of risks. First, they have many characteristics such as *exposure* (maximum amount of damage suffered), *severity* (amount of damage that is likely suffered), *volatility* (variability of potential outcomes), *probability* (how likely a risky event occurs), *time horizon* (the time exposed to the risk), *correlation* (amount of correlation between different risks) and *capital* (how much capital is needed to cover losses) (Lam 2003). Second, all risks are temporal and can thus be materialized in complex chains of risks and mitigations over time (Alter and Sherer 2004). Third, risks are not always negative but may also have positive consequences when they materialize (Alter & Sherer 2004).

As a result, risk seems to have been conceptualized in several ways, each accentuating different risk characteristics. For example, Sherer and Alter (2004) identify various types of conceptualizations of risk from IS literature, such as risks as different types of negative outcomes (risk components), risks as factors leading to a loss (risk factors), risk as probability of negative outcomes, and risk as difficulty in estimating outcome. To broaden the scope of the study and to take into account both causes (risk factors) and effects (risk components), we consider risk both as a factor leading to a negative outcome and as the negative outcome itself (cf. Sherer and Alter 2004). Consequently, in this study, we defined EA risks as

1) any factors that may lead to negative outcomes in the EA program, and
2) any negative outcomes resulting from these factors.

However, the focus group participants commented that in practice the negative outcomes may be considered more important since they represent the actual results. Moreover, it was brought out that the two definitions should be better distinguishable from each other. In practice, it is difficult to disentangle the myriad of risk factors and outcomes as there are more than one level of outcomes.

3.2 Risk Classification Schemes

The amount of different risks identified in literature is extensive. Hence, many authors propose classifications for the risks presented in their papers. Typically, the risk categories depict the more or less abstract function, task, object or entity the risk is related to. For example, generic risk management literature divides risks to various classes such as business, market, operations and credit risks (Crouhy et al. 2001; Lam 2003). In the domain of IS and ICT, the risks identified in literature encompass factors related to the development of systems and software, as well as factors arising outside the scope of development (Benaroch 2002; Saha 2006). To classify these kinds of risks, Keyes (2005) proposes categories such as project, technical and business risks. Similarly, Benaroch (2002) divides ICT investment risk components into three categories: firm-specific,

competition and market risks, each consisting of more specific risk areas such as financial, political, environmental and project.

Risks can also be classified on other grounds. For instance, Bandyopadhyay (1999) addresses ICT risks on three levels, namely application, organizational and interorganizational levels, depicting the level in the ICT environment the risk is related to. Moreover, risks can be classified on the account of how known they are: the risks could be known, predictable or unpredictable (Keyes 2005). However, few authors accommodate the temporal nature of risk to their classification schemes. Yet, Sherer and Alter (2004) present an extensive synthesis of IS risks from literature, classified by generic IS life cycle phases (initiation, development, implementation, and operation and maintenance). Moreover, the authors classify risks by work system (see Alter 2002; Alter 2003) components, namely customers, work practices, participants, information, technologies, environment, infrastructure and strategies, creating a generic model of risks potentially adaptable to any work system. The risks presented are conceptualized as both risk factors and risk components.

3.3 Views of Enterprise Architecture Risk

The reviewed literature included few papers exclusive on EA risks. Drawing from the discussion of ICT investment risks by Benaroch (2002), Saha (2006) discusses EA investment risks and options, presenting EA investment risk factors divided into the categories of organization specific, competitive, market and technical risks. Baldwin (2007), on the other hand, states that EA risks can exist on and between the various levels of EA products (e.g. business, information, information systems, technology).

Some authors also present results that can be applied to the EA risk context. Especially EA challenges (see e.g. Rehkopf and Wybolt 2003; Kaisler et al. 2005) and EA critical success factors (see e.g. Ylimäki 2006) could indicate potential areas where risks may arise. ICT risk literature, again, refers to architectural risks (see e.g. Avritzer and Weyuker 1998), typically uncovered by architecture reviews or audits, including a great number of technological and project management related factors. However, they seem clearly limited in the EA context, because EA adopts much more extensive view of an organization than traditional software development.

4 Enterprise Architecture Risk Classification Scheme

The work system framework of risks (see Sherer and Alter 2004) was adapted to this study because of its genericity and extensive literature base. The authors also acknowledge that generic work system risks apply to the IS context (Sherer and Alter 2004), suggesting that they may apply to the EA context as well. Furthermore, because a risk classification scheme should consider the conceptualization of risk in question, it is an advantage that the work system framework of risks shares the same conceptualization with this study. The model also provides a meaningful context to classify risks, understandable by not only technically-oriented persons but business personnel as well (Sherer and Alter 2004). Many other classification models utilize insufficiently defined, abstract categories, which may be difficult to comprehend by practitioners. Finally, the model already includes a set of generic risks based on an extensive literature basis, also including factors mentioned in EA risk literature (Saha 2006). However, it should be noted that even though the model takes the temporal nature of risk into account by classifying the risks by IS life cycle phases, this viewpoint was not covered in our study because of time limitations in the focus group interview.

Alter (2003) defines work system as "a system in which human participants and/or machines perform work using information, technology, and other resources to produce products and/or services to internal or external customers". Originally, the author argues that the work system construct should replace the "IT artifact" as the central concept of the IS domain, because the contemporary IS domain is work system-centric rather than ICT-centric (Alter 2003).

However, as EA can be considered from at least the four viewpoints presented in the first section (process, product, implementation and impact), the adaptation of the framework to the EA context may not be straightforward. Therefore, we had to define how the viewpoints are represented by the framework. In our adapted framework, EA processes are represented with the *Work Practices* element, supported by *Participants*, *Information* and *Technologies*. EA products and services are naturally covered by the *Products and Services* viewpoint. EA implementations and impacts, on the other hand, are represented by the *Customer* element since customers implement the EA products and services, and expect the implementations to result in planned impacts. Moreover, implementations (e.g. a new information system developed according to EA) themselves can also be considered to be part of *Environment* and *Infrastructure* elements, and even *Information*, *Technologies* and *Work Practices*, if these elements include EA implementations.

The revised work system framework is depicted in Figure 1. The framework includes nine elements which all contribute to the operation of the system. Conforming to the original definitions (see Alter 2002), we define the elements for our adapted framework as follows.

- *Customers* are the internal and external users of EA products (e.g. principles, methods and models) and services (e.g. EA guidance) (adapted from Alter 2002). A typical use for EA products is their implementation, meaning both the implementation of organizational elements according to or in compliance with EA (see e.g. Armour et al. 1999b; Kaisler et al. 2005), and other use cases (see e.g. Rehkopf and Wybolt 2003; Lankhorst 2005; Bucher et al. 2006; Andersin and Hämäläinen 2007; Emery et al. 2007). Customers might include, for example, organization's management, project managers, ICT developers and partners (see e.g. Niemi 2007).

- *Products and Services* include all EA products and services produced by the work system (adapted from Alter 2002).
- *Work Practices* consist of EA processes (e.g. planning, development and management) and the practices and methods utilized in their operation (adapted from Alter 2002).
- *Participants* include persons who perform any work in the EA work system (adapted from Alter 2002). These include a broad range of roles carrying out work in any of the EA processes, such as enterprise and domain architects, ICT developers and project managers (see e.g. Niemi 2007).
- *Information* consists of any information used or created by the EA work system participants as they produce the EA products and services (adapted from Alter 2002). To produce EA products, information on the entities to be depicted by the products (e.g. organizational structures, processes, systems, applications and services) is required.
- *Technologies* include all kinds of tools and techniques used by the EA work system participants to carry out their work (adapted from Alter 2002). Several tools, such as Rational Rose and UML, are available for modeling EA (see e.g. Kaisler et al. 2005).
- *Environment* encompasses the organizational, cultural, competitive, technical and regulatory factors that have an impact on the operation of the EA work system although it is not directly dependent on them (adapted from Alter 2002). For example, management support and organizational culture have an effect on the architectural performance of an organization (see e.g. Ylimäki 2006).
- *Infrastructure* consists of human, informational and technical resources that are required in the operation of the EA work system although they are situated and managed externally (adapted from Alter 2002). In addition to organizational information systems and training and support staff (see Alter 2002), these resources include sources of information necessary for the production of EA products and services. These sources of information, in turn, may include subject matter experts with knowledge and experience in a specific domain (e.g. business, information, information systems or technology) and various organizational descriptions and plans (see e.g. Babers 2006).
- *Strategies* include both the strategy of the EA work system and the strategy of the organization where the system operates (adapted from Alter 2002).

The focus group participants also agreed that the framework is generic enough to be used to depict an EA work system. Nevertheless, several additional points regarding the framework were brought out. First, it was emphasized that the temporal nature of EA should be taken into account. Specifically, the focus group agreed that each of the elements has its own life cycle (i.e. each element changes in a different rate), and even inside the elements different objects (e.g. technologies and work practices) may have particular life cycles. Therefore, we suggest that the work system elements should be connected to the life cycle phases of EA (c.f. Sherer and Alter 2004).

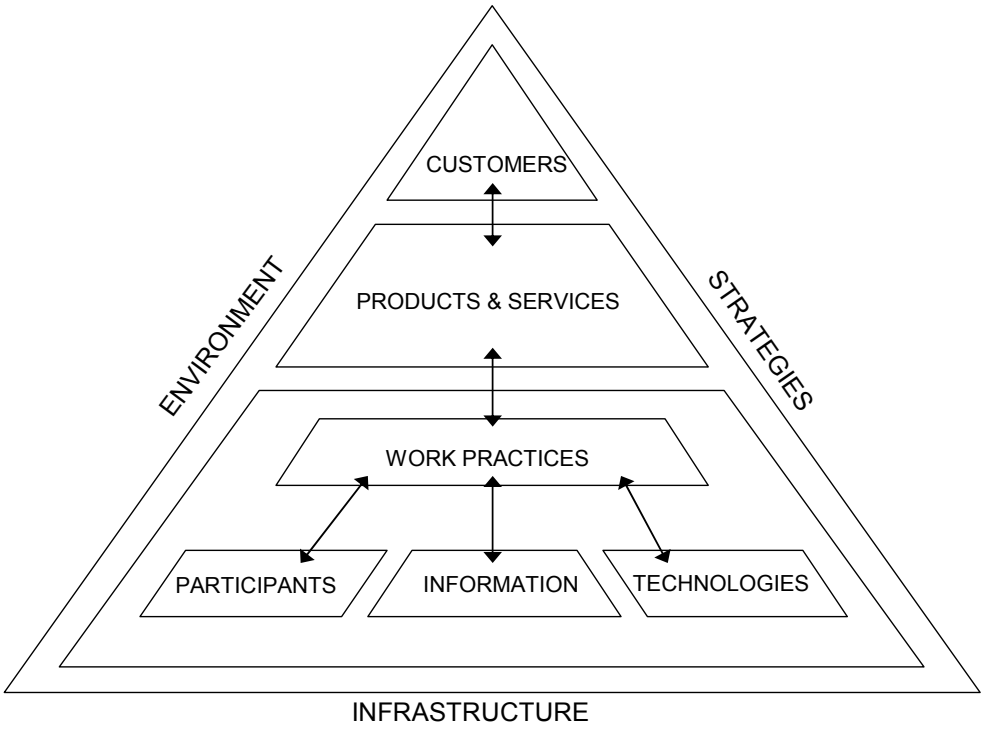

Figure 1. The revised work system framework (Sherer and Alter 2004)

Second, EA products and implemented EA can also be conceptualized from the temporal perspective. Individual EA products, such as architectural models depicting different viewpoints of the organization, have particular life cycles, as well as their implementations such as information systems and processes. The focus group stressed that it is always necessary to consider planned and implemented, as well as outgoing EA implementations. This presents the challenge of depicting the implemented EA in the framework, since it also is a source of risks not to be disregarded. In our adapted framework, the implementation viewpoint is included to the customer element. However, in the future it might be necessary to add an extra element for implementation to signify its importance.

Third, the focus group brought out that as well as all of the elements should implicitly include the temporal dimension, should they similarly include the aspects of security and competence. The focus group stated that competence is at least related to technology, work practices, participants, products and services, and customers. However, we consider that competence should be related to all elements that include stakeholder effort. Therefore, risks relating to the lack of competence may arise in at least the elements of participants, customers, infrastructure and environment; they are not merely related to participants as suggested in the original framework (c.f. Sherer and Alter 2004). Nevertheless, the focus group stated that lack of competence in this context refers more to the lack of common understanding about EA than to the lack of skills. Regarding organizational security, it was suggested that it should be similar, implicit aspect that crosses every element in the framework. Lack of security in the elements of EA work system was considered a risk by the focus group, and should not be included merely to the information element (c.f. Sherer and Alter 2004). According to the group, security influences EA and vice versa.

Fourth, the role of partners in carrying out work on EA was accentuated. However, it was commented that partners cannot be associated with one particular element due to their different roles in the operation of the system. According to the focus group, partners can directly carry out operative tasks in the EA work system, act as suppliers of necessary EA or ICT products and services, or even offer whole outsourced service interfaces for the operation of the EA work system. Moreover, the group accentuated that partners might as well be a source of risks, a point missing in the original framework (c.f. Sherer and Alter 2004). Consequently, we suggest that partners should be considered as participants if they have a role which involves performing operational tasks in the EA work system. If partners act as product or service providers or outsourcing partners, they can be considered as infrastructure. Internally managed ICT products, on the other hand, could be included into technologies.

Fifth, it was stated that the different roles of the management of the organization similarly make it difficult to classify management to any single element. According to the focus group, management is an important stakeholder of EA, providing necessary resources, steering EA by making architecturally significant decisions, observing and measuring the work system, and utilizing EA in organizational decision-making. Management does not directly carry out work in the system, but is a significant facilitator, user and also a developer of EA since its decisions set the general direction for the work in the system. Therefore, we consider management to be part of not only the environment (c.f. Sherer and Alter 2004) but also the participants, customers and infrastructure elements, depending on its role in the organization in question.

5 Potential Enterprise Architecture Risks

The generic work system risks presented by Sherer & Alter (2004) were adapted to be utilized as a basis for discussion in the focus group interview. The focus group participants generally agreed with the generic risks presented, but provided a number of additional risks and examples of risks' realization in practice.

The EA work system risks are displayed in Table 1, including both 1) factors that may lead to negative outcomes in the EA program, and 2) potential negative outcomes resulting from these factors. The table includes both the original risks (see Sherer and Alter 2004) and the additional risks mentioned in the focus group interview. Moreover, examples of risks' realization in practice, brought out in the interview, are displayed. The information from the interview is displayed in *italics*.

Table 1. Generic EA work system risks and examples of their realization (adapted from Sherer and Alter 2004; complemented by the focus group)

EA work system element	**Factors leading to negative outcomes**	**Negative outcomes**
Customers	▪ Disagreement regarding the requirements for EA products and services *- Insufficient source information on EA for producing products and services* *- Inconsistent requirements because of different competencies in comprehending products and services* ▪ Difficulty in using EA products or services *- Insufficient competence for using EA products and services correctly* *- Inadequate instructions and training* ▪ *Inadequate implementation of EA products and services* *- Inadequately high or low compliance between EA and its implementations* *- Inadequate temporal planning of implementation* *- Inadequate EA guidance to the implementation project (e.g. incorrect content or timing)* *- Inadequately narrow or wide scope of the implementation project* ▪ *Insufficient organizational security*	▪ Lack of use of EA products and services ▪ Dissatisfaction of customers ▪ *Misuse or misinterpretation of EA products* ▪ *Insufficient realization of EA objectives*

EA work system element	**Factors leading to negative outcomes**	**Negative outcomes**
Work Practices	▪ Poorly designed EA processes *- Burden of obsolete work practices* ▪ Incompatibility between work practices and other EA work system elements *- Lack of approval, authorization or need for work practices* ▪ Insufficient resources ▪ Inadequate planning and control mechanisms *- Insufficient comprehension of objectives* *- Insufficient observation of work practice feasibility* *- Insufficient feedback mechanisms from the customers and participants* ▪ *Insufficient organizational security*	▪ Inadequate EA process performance ▪ *Insufficient predictability of outcomes* ▪ *Insufficient documentation*
Products and Services	▪ Inadequate quality or cost of EA products or services to customer *- Inadequately high EA quality (positive risk)* *- Inadequately high initial costs* ▪ Incompatibility between customer requirements and EA products or services *- Inadequately simple or complex EA* *- Insufficient flexibility of EA* ▪ *Insufficient organizational security*	▪ Lack of use of EA products and services ▪ Dissatisfaction of customers
Participants	▪ Inadequate management of EA processes *- Lack of measurement of participants' work* *- Unclear organization and responsibilities* ▪ Lack of competence *- Incompatibility between participants and technology* *- Inadequate instructions and training* ▪ Lack of motivation and interest *- Lack of measurement of participants' work* *- Inadequate instructions and training* ▪ Poor conflict management ▪ Incompatibility between characteristics of participants and processes ▪ *Insufficient organizational security*	▪ Inadequate EA process performance ▪ Personnel problems

EA work system element	**Factors leading to negative outcomes**	**Negative outcomes**
Information	▪ Insufficient information quality *- Insufficient reliability of information (e.g. documented information vs. tacit knowledge)* *- Insufficient or vast amount of information* *-Insufficient information integrity* ▪ Insufficient information accessibility *- Unobtainable information even when access rights are correct* ▪ Insufficient information presentation ▪ Insufficient information security	▪ Inadequate EA process performance ▪ Participant frustration ▪ Information loss or theft
Technologies	▪ Inadequate usability of technology ▪ Inadequate technology performance for EA processes ▪ Technology errors ▪ Incompatibility between technologies Which all may result from e.g. *- Inappropriate technology (e.g. too old or new technology)* *- Unorthodoxly applied technology* ▪ *Dependence on technology providers* ▪ *Insufficient organizational security*	▪ Inadequate EA process performance ▪ Participant frustration
Environment	▪ Insufficient management support *- Insufficient resources (time, personnel, money) directed to the EA work system* ▪ Inconsistencies with organizational culture ▪ *Inconsistencies with partners or legislation* ▪ Incompatibility between environment and the EA work system *- Incompatibilities between EA and reality* *- Insufficient flexibility of EA* *- Insufficient competence for understanding EA* ▪ High level of turmoil and distractions ▪ *Insufficient organizational security*	▪ Diminished EA work system performance
Infrastructure	▪ Inadequate human infrastructure *- Unclear who to ask for input information for EA* *- Insufficient competence for participating in work on EA* *- Infrastructure consists of separate silos* ▪ Inadequate information system infrastructure *- Infrastructure consists of separate silos* ▪ Inadequate technical infrastructure ▪ *Insufficient organizational security*	▪ Diminished EA work system performance

EA work system element	**Factors leading to negative outcomes**	**Negative outcomes**
Strategies	▪ Poor alignment between organizational strategy and the EA work system *- Unclear or missing "big picture" of EA* *- Inadequate control of the effects of organizational strategy change on EA* ▪ Inadequate EA work system strategy for accomplishing work system goals *- Incorrect comprehension of strategy* ▪ *Insufficient organizational security*	▪ Ineffective EA work system performance

6 Enterprise Architecture Risk Management

In general, risk management can been seen as an activity of balancing 1) risk and reward and 2) processes and people (Lam 2003). Basically, the goal of risk management is to help the organization in achieving its objectives (Lam 2003). A proactive risk strategy enables the organization to plan and prepare for possible risks (Keyes 2005). Preparing for the known, predictable and unpredictable risks (Keyes 2005) requires a feasible risk management process, which usually consists of the following three phases (Bandyopadhyay et al. 1999; Lam 2003):

- Risk awareness and identification: Understanding of the various risk characteristics supports identification of the possible risks involved in any activities carried out in an organization. Furthermore, the actual severity and probability of a potential risk are even more crucial issues to be taken into consideration. A risk-aware organization addresses most risk management issues before they become too big problems.
- Risk measurement and analysis: Measurement is needed to be able to manage risks. Risk measurement seems to be a challenging task in any organization. Tools like scenario analysis (Lam 2003) or risk assessment based on critical success factors (see e.g. Keyes 2005) can be exploited in risk measurement and analysis.
- Risk control basically means the actions taken based on the risk measurement results.

In the EA domain, EA risk management supports the attainment of EA objectives (c.f. Lam 2003). Successful EA, in turn, supports the attainment of organizational objectives, such as organizational flexibility and agility (see e.g. Hoogervorst 2004). Likewise, unsuccessful EA can have serious consequences in the organization. EA is also essentially a tool for facilitating organizational risk management (see e.g. Morganwalp and Sage 2004), a viewpoint also shared by the focus group. In the focus group interview, it was underlined that general risk management practices should be applied in the EA domain as well. Even though EA-related risks are not currently considered in detail in organizations, there seems to be the need of identifying, measuring and controlling EA risks as well. Basically, EA risks can be considered as one category or type of risks the organization's risk management needs to deal with; consequently, EA risk management should not be separate from organizational risk management.

EA risk management can be seen as one of the tasks of the EA management (governance). The EA management team, assisted by everyone carrying out EA work, should identify possible risks. For example, a risk table may be used as a simple tool including each risk's category, probability of occurrence, and assessed impacts (Keyes 2005). These identified EA risks may also provide a feasible basis for EA metrics selection and vice versa. In EA risk measurement, self-assessment of quantitative measures (risk indicators) may be applied (Lam 2003) and risk measurement can bee seen as a responsibility of the EA management team. Finally, the EA management team should take actions based on the EA risk measurement results. However, the risk management responsibilities brought out here may be different in reality, as it was brought out in the interview that they are dependent on the organization of EA management in the specific company.

The focus group stated that EA planning is scenario-based, so it is important to consider the risks related to each scenario. Therefore, EA risks are one criterion for EA-related decision-making which aims at optimizing the risk-benefit ratio. Furthermore, risks still need to be managed and

their outcomes measured in the decision follow-up. The relationship between EA risk management and EA decision-making and follow-up is described in Figure 2. Based on the focus group interview, the arrow from benefits and negative outcomes back to the risk factors was added to describe the cyclic nature of risk process; once in a while it is necessary to review the risk factors again to take into account any changes in the environment. This may also involve a follow-up decision.

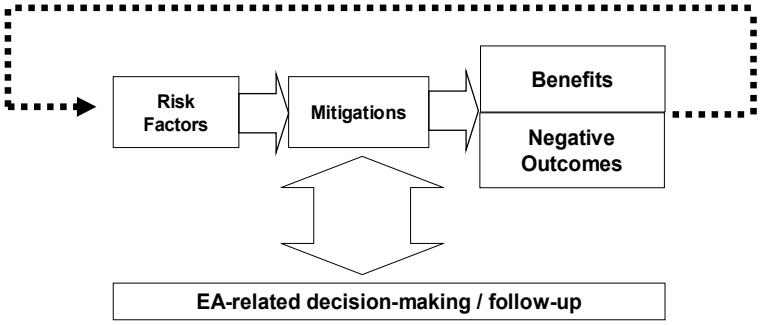

Figure 2. EA risk management vs. EA-related decision-making (adapted from Benaroch et al. 2006; complemented by the focus group)

The interview results also suggest that many of the EA related risks can be avoided – or at least mitigated – with the help of efficient and adequate communication on EA issues using a common language that is understandable by each stakeholder. According to the focus group, poor knowledge on EA in the organization is a risk since it impairs the identification of EA risks. Also a proper documentation of EA products and services supports risk mitigation. The focus group agreed that EA risk management is linked to EA maturity (c.f. Ylimäki 2007): in the lower maturity levels EA risk management does not necessarily need to be a defined process, but in higher levels of maturity risk management needs to be improved as the EA processes, products and implementations becomes more specified. It is also important to define EA risk limits (c.f. Lam 2003): the focus group stated that putting too much resources on EA risk management is a risk as well - the EA does not need to be perfect.

One obstacle to managing EA risks, brought out by the focus group, is the fact that it may be difficult to define the "owner" of the risk: who has the responsibility of dealing with EA risks; business management, EA management or some other stakeholder? Who is responsible of a single risk factor or its outcome? According to the focus group, responsibilities are definable on a project scope, but especially in those cases where a risk extends over two or more departments or lines of business (or any other silos in the enterprise) and is not connectable to any single project, responsibility issues may create challenges.

7 Summary and Conclusions

This study aimed at providing an overview of generic risks that can potentially be related to EA in companies by a literature review and a focus group interview of practitioners. Furthermore, potential classification schemes for the risks were charted from literature, and one of the schemes – the work system framework – was selected and discussed in the focus group interview. The framework also included a set of generic work system risks, which were also discussed in the interview. In addition, EA risk management was discussed. In this study, EA risks were conceptualized both as 1) factors that may lead to negative outcomes in the EA program, and 2) negative outcomes resulting from these factors. The latter was considered more important aspect in practice by the focus group interviewees.

Although the focus group participants agreed that the work system framework is generic enough to be used to depict an EA work system, they brought out several comments regarding to the framework:

- The life-cycle aspect of all of the EA work system elements should be more explicit in the framework. Particularly, both EA products and implementations have distinct life cycles, which should be considered.
- Implemented EA is an important source of risk in the EA work system so it should potentially be regarded.
- All of the EA work system elements are affected by the level of organizational security.
- Every EA work system element that involves human effort is prone to risks related to lack of competence. However, lack of competence in this context should be more conceptualized as the lack of common understanding about EA than the lack of skills.
- Both partners and management may have diverse roles in the operation of the EA work system so they cannot be associated with only one specific element.

The focus group also generally agreed with the generic EA work system risks presented, but provided a number of additional risks and examples of risks' realization in practice, which were added to the initial list of EA work system risks. Practitioners can use these results to identify typical risks related to each element in the EA work system, and to assure that risk management practices have been planned for all relevant risks. Moreover, the EA work system framework may be used to structure the EA approach in organizations, regarding other aspects than risks as well.

Regarding to EA risk management, the focus group interview results suggest that

- Even though EA-related risks are not currently considered in detail in organizations, there seems to be the need of managing them.
- EA risk management should be in a close connection or a part of organizational risk management. In turn, EA facilitates organizational risk management.
- The risk-gain ratio in EA-related decision-making should be optimized and decision follow-up implemented as a continuous activity.

- Communication, common language and sufficient EA documentation are important EA risk mitigation strategies.
- Clear risk management responsibilities are important in the EA context. In addition to the level of EA risks related to a single development project, more extensive responsibilities for risks should be defined.

As the validation of the results was rather limited in the course of this study, more empirical research is still needed. Especially, the EA risks presented should be further analyzed for their significance in practice and more concrete examples of their realization uncovered. Moreover, as the temporal nature of EA risks was not thoroughly investigated in this study, the risks should be studied with regard to time; for example, which risks are especially related to which steps in the EA program, levels of EA maturity, or phases of the EA life cycle. Uncovering the actual causal chains of risks is also an important area of further research, as well as the different levels of risks; in this study, only two levels were included. Following lines of research could also focus on quantifying the effects of the realization of EA risks on the organizational level. Also, implementing EA risk management as an organized, continuous activity that is linked to the organization's generic risk management is a challenge which requires further investigation.

References

Alter, S. (2002). "The Work System Method for Understanding Information Systems and Information System Research." Communications of the Association for Information Systems **9**(1): 90-104.

Alter, S. (2003). "18 Reasons Why IT-Reliant Work Systems Should Replace "the IT Artifact" as the Core Subject Matter of the IS Field." Communications of the Association for Information Systems **12**(1): 366-395.

Alter, S. and S. A. Sherer (2004). "A General, but Readily Adaptable Model of Information System Risk." Communications of the Association for Information Systems **14**(1): 1-28.

Andersin, A. and N. Hämäläinen (2007). Enterprise Architecture Process of a Telecommunication Company – A Case Study on Initialization. Proceedings of the 11th International Conference on Human Aspects of Advanced Manufacturing: Agility and Hybrid Automation (HAAMAHA 2007). Poznan, Poland, IEA Press.

Armour, F. J. and S. H. Kaisler (2001). "Enterprise Architecture: Agile Transition and Implementation." IT Professional **3**(6): 30-37.

Armour, F. J., S. H. Kaisler and S. Y. Liu (1999a). "A Big-Picture Look at Enterprise Architectures." IT Professional **1**(1): 35-42.

Armour, F. J., S. H. Kaisler and S. Y. Liu (1999b). "Building an Enterprise Architecture Step by Step." IT Professional **1**(4): 31-39.

Avritzer, A. and E. J. Weyuker (1998). Investigating Metrics for Architectural Assessment. Proceedings of the Fifth International Software Metrics Symposium, Metrics 1998. Bethesda, MD, USA, IEEE Computer Society: 4-10.

Babers, C. (2006). The Enterprise Architecture Sourcebook Volume One: Process and Products. El Paso, Texas, USA, Charles Babers.

Baldwin, A., Y. Beres and S. Shiu (2007). "Using assurance models to aid the risk and governance life cycle." BT Technology Journal **25**(1).

Bandyopadhyay, K., P. P. Mykytyn and K. Mykytyn (1999). "A framework for integrated risk management in information technology." Management Decision **37**(5): 437-444.

Benaroch, M. (2002). "Managing Information Technology Investment Risks: A Real Options Perspective." Journal of Management Information Systems **19**(2): 43-84.

Benaroch, M., Y. Lichtenstein and K. Robinson (2006). "Real Options in Information Technology Risk Management: An Empirical Validation of Risk-Option Relationships." MIS Quarterly **30**(4): 827-864.

Boehm, B. W. (1991). "Software Risk Management: Principles and Practices." IEEE Software **8**(1): 32-41.

Bucher, T., R. Fischer, S. Kurpjuweit and R. Winter (2006). Enterprise Architecture Analysis and Application - An Exploratory Study. Proceedings of the EDOC Workshop on Trends in Enterprise Architecture Research (TEAR 2006). Hong Kong, China.

Crouhy, M., D. Galai and R. Mark (2001). Risk Management. New York, USA, McGraw-Hill.

de Boer, F. S., M. M. Bosanque, L. P. J. Groenewegen, A. W. Stam, S. Stevens and L. van der Torre (2005). Change Impact Analysis of Enterprise Architectures. Proceedings of the 2005 IEEE International Conference on Information Reuse and Integration (IRI-2005). Las Vegas, USA, IEEE Computer Society: 177-181.

Emery, C., S. M. Faison, J. Houk and J. S. Kirk (2007). The Integrated Enterprise: Enterprise Architecture, Investment Process and System Development. Proceedings of the 40th Annual

Hawaii International Conference on System Sciences (HICSS'07). Hawaii, USA, IEEE Computer Society.

Goethals, F., M. Snoeck, W. Lemahieu and J. Vandenbulcke (2006). "Managements and enterprise architecture click: The FAD(E)E framework." Information Systems Frontiers **8**(2): 67-79.

Hjort-Madsen, K. (2006). Enterprise Architecture Implementation and Management: A Case Study on Interoperability. Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS '06). J. Ralph H. Sprague. Kauai, Hawaii, IEEE Computer Society.

Hoogervorst, J. (2004). "Enterprise Architecture: Enabling Integration, Agility and Change." International Journal of Cooperative Information Systems **13**(3): 213-233.

Jonkers, H., M. Lankhorst, H. ter Doest, F. Arbab, H. Bosma and R. Wieringa (2006). "Enterprise architecture: Management tool and blueprint for the organization." Information Systems Frontiers **8**(2): 63-66.

Kaisler, S. H., F. Armour and M. Valivullah (2005). Enterprise Architecting: Critical Problems. Proceedings of the 38th Hawaii International Conference on System Sciences (HICSS'05). Hawaii, USA, IEEE Computer Society.

Keyes, J. (2005). Implementing the IT Balanced Scorecard - Aligning IT with Corporate Strategy. Boca Raton, USA, Ayerbach Publications.

Kluge, C., A. Dietzsch and M. Rosemann (2006). How to Realise Corporate Value from Enterprise Architecture. Proceedings of the 14th European Conference on Information Systems (ECIS 2006). Göteborg, Sweden, Association for Information Systems.

Krueger, R. A. and M. A. Casey (2000). Focus Groups. A Practical Guide for Applied Research. Thousand Oaks, USA, Sage Publications.

Lam, J. (2003). Enterprise Risk Management: From Incentives to Controls. Hoboken, New Jersey, USA, John Wiley & Sons.

Lankhorst, M. (2005). Enterprise Architecture at Work. Modelling, Communication, and Analysis. Berlin, Germany, Springer-Verlag.

Morganwalp, J. M. and A. P. Sage (2004). "Enterprise Architecture Measures of Effectiveness." International Journal of Technology, Policy and Management **4**(1): 81-94.

Niemi, E. (2007). Enterprise Architecture Stakeholders - A Holistic View. Proceedings of the 13th Americas Conference on Information Systems (AMCIS 2007). Keystone, Colorado, USA, Association for Information Systems (AIS).

Pulkkinen, M. and A. Hirvonen (2005). EA Planning, Development and Management Process for Agile Enterprise Development. Proceedings of the 38th Annual Hawaii International Conference on System Sciences (HICSS '05). Hawaii, USA, IEEE Computer Society.

Rehkopf, T. W. and N. Wybolt (2003). "Top 10 Architecture Land Mines." IT Professional **5**(6): 36-43.

Reuvid, J., Ed. (2005). Managing business risk: a practical guide to protecting your business. London, England, Kogan Page.

Rosen, M., S. W. Ambler, T. K. Hazra, W. Ulrich and J. Watson (2007). Enterprise Architecture Trends. Enterprise Architecture, Vol. 10, No. 1. Arlington, Massachusetts, USA, Cutter Consortium.

Saha, P. (2006). "A Real Options Perspective to Enterprise Architecture as an Investment Activity." Journal of Enterprise Architecture **2**(3): 32-52.

Sherer, S. A. and S. Alter (2004). "Information System Risks and Risk Factors: Are They Mostly About Information Systems?" Communications of the Association for Information Systems **14**(2): 29-64.

The Open Group. (2006). "The Open Group Architecture Framework version 8.1.1, Enterprise Edition (TOGAF 8.1.1)." Retrieved 10 September 2007, 2006, from http://www.opengroup.org/architecture/togaf/.

Veasey, P. W. (2001). "Use of enterprise architectures in managing strategic change." Business Process Management Journal **7**(5): 420-436.

Ylimäki, T. (2006). "Potential Critical Success Factors for Enterprise Architecture." Journal of Enterprise Architecture **2**(4): 29-40.

Ylimäki, T. (2007). "Towards a Generic Evaluation Model for Enterprise Architecture." Journal of Enterprise Architecture **3**(3).