Research Center
Finance & Information Management

Fraunhofer FIT
Project Group
Business & Information
Systems Engineering

Discussion Paper

Reducing the Pain of the Inevitable: Assisting IT Project Managers in Performing Risk Management

by

Nicolas Brinz, Christian Regal, Marco Schmidt, Jannick Töppel

To be presented at: 39th International Conference on Information Systems (ICIS),
San Francisco, USA, December 2018

University of Augsburg, D-86135 Augsburg
Visitors: Universitätsstr. 12, 86159 Augsburg
Phone: +49 821 598-4801 (Fax: -4899)

University of Bayreuth, D-95440 Bayreuth
Visitors: Wittelsbacherring 10, 95444 Bayreuth
Phone: +49 921 55-4710 (Fax: -844710)

www.fim-rc.de

WI-785

Reducing the Pain of the Inevitable: Assisting IT Project Managers in Performing Risk Management

Completed Research Paper

Nicolas Brinz
FIM Research Center
University of Augsburg
Universitätsstraße 12
86159 Augsburg, Germany
nicolas.brinz@fim-rc.de

Christian Regal
FIM Research Center
University of Augsburg
Universitätsstraße 12
86159 Augsburg, Germany
christian.regal@fim-rc.de

Marco Schmidt
FIM Research Center
University of Augsburg
Universitätsstraße 12
86159 Augsburg, Germany
marco.schmidt@fim-rc.de

Jannick Töppel
FIM Research Center
University of Augsburg
Universitätsstraße 12
86159 Augsburg, Germany
jannick.toeppel@fim-rc.de

Abstract

An organization's IT landscape is seldom static due to changes in applications, data, or infrastructure. These mostly project-related changes alter the organization's risks. Effective IT risk management requires information on these changes to manage risks. "Traditional" methods for risk management are challenged by a fast-developing IT and the lack of qualified experience. To support project and risk managers in IT risk management, we apply method engineering to develop an integrated method that connects knowledge on threats, actors, vulnerabilities, and mitigation measures with risk-relevant project characteristics to identify, quantify, and mitigate a project's risks. We evaluate our method in a single case study by deploying a software prototype at a globally acting manufacturer of construction and demolition tools with over 25.000 employees. Our evaluation shows that the proposed method has the potential to improve IT risk management regarding standardization and efficiency, while communication and training of end users are crucial.

Keywords: Project Management, Risk Management, Assistance System

Introduction

Today, information technology (IT) plays a central role in almost all businesses. In the digital era, organizations intensify the use of automated IT systems to support business processes and information processing to improve workflow performance considerably. Thus, IT systems and information often become essential parts of an organization's value creation and their outage or insecurity can have detrimental effects on business operations. Enterprise risk management aims at protecting the organization and its ability to pursue its mission by identifying, analyzing, evaluating, treating, and monitoring risk. IT risks have become a major contributor to the overall risk exposure of companies (Grobauer et al. 2011). A survey of 643

computer security practitioners in US corporations, governmental agencies, financial institutions, medical institutions, and universities revealed that already in the year 2000, ninety percent of survey respondents detected cyber-attacks on their company. 273 organizations reported financial losses higher than $265 million due to IT security issues (Gordon et al. 2000). These numbers have risen ever since: Herjavec's 2017 Cybercrime Report (Herjavec Group 2017) predicts that by 2021 cybercrime will cost companies $6 trillion each year. While these are global figures, an organization's IT risks also can take on business-endangering proportions and, thus, need to be managed properly to prevent critical financial losses.

However, a company's IT landscape is subject to constant change. IT projects regularly transform the way things work on the application, data, or infrastructure layers. Each new or modified IT solution can significantly alter IT risks. For example, a new application can open up previously secured attack vectors, the lack of backups in a migrated database can increase the risk of data loss, or hardware components that do not meet quality requirements can cause short-term business interruptions. Thereby, constant change challenges IT risk management (ITRM) in several ways: First, fast-developing IT and the lack of precedents make it difficult to estimate the consequences of change on IT risk. Second, the relationship between the causes and effects of IT risks is very complex due to IT solution interdependencies. A threat can take effect on multiple business processes and, conversely, multiple threats can relate to the same business process.

Considering this complexity, effective ITRM requires the best possible information on the change expected to come. In most companies, an internal change mainly happens within IT projects and with respective IT solutions. Following the divide-and-conquer principle, a better understanding of upcoming IT solutions can help to proactively manage IT risks on a global level (Zissis and Lekkas 2012). But ITRM also requires extensive knowledge of risk management constructs, such as vulnerabilities, threats, impact, or likelihood as well as their interdependencies. Unfortunately, most IT project managers (ITPMs) are not familiar with this knowledge and struggle with the vital but complex task of evaluating and managing the risks that come with their solution. This is a complex task for several reasons: First, ITPMs do not understand ITRM deep enough, while ITRM experts do not know the solution well enough. Thus, if working separately, both sides would face challenges when elaborating on a complete and accurate list of risk scenarios relevant to the solution. Second, people individually do not apply the same scales for assessment. This implies that risk management activities are not comparable between projects or ITPMs. Thus, the aggregation of solution-related risks does not reliably reflect the change in risk going along with a project. Third, performing risk identification and quantification in a joint effort by ITPMs and IT risk managers is very time-consuming and may not be practical for large companies with a high number of simultaneous IT projects. Fourth, information on the risks of comparable projects can prevent a cold start for risk identification and analysis. Its acquisition, however, can require a significant amount of time.

In this paper, we engineer a method designed to overcome the challenges and serve three design objectives:

Design Objective 1: Standardize IT solution risk management (availability, reliability, security, and compliance of solution) locally within IT projects to enhance ITRM quality globally, make results comparable and interpretable, and get a better understanding of a solution's risks (Purdy 2010).

Design Objective 2: Make IT solution risk management (that is, the identification, analysis, evaluation, and mitigation of risks) accessible to non-experts such as ITPMs to facilitate efficient ITRM without the need for every contributor to have specific knowledge on the company's risk profile.

Design Objective 3: Provide a clearly defined process that establishes risk management as a crucial part of the project management process and covers all project phases (initiation, design, implementation or acquisition, and deployment) to ensure the completeness of solution-specific information, prevent the erroneous evaluation of risk and mitigation, and provide all information necessary for the continuous monitoring of risks throughout the solution lifecycle.

The method aims at supporting both, ITPMs, who are responsible for successful project completion, and IT risk managers, who are responsible for the holistic management of IT risks. It integrates risk management activities of both parties and connects ITRM knowledge on threats, actors, vulnerabilities, and mitigation measures with risk-relevant solution characteristics to identify, quantify, and mitigate the solution's risks. A case study confirms the method's utility for both ITPMs and ITRM experts and provides real-world evidence for its efficiency and applicability for daily business. Practitioners can benefit from increased consistency in IT solution risk management, a more efficient evaluation process, and better-informed ITRM.

In a first step, we compile theoretical knowledge on risk and the risk management process. Subsequently, we compare related approaches to integrating risk management into the project management process. In a third step, we conceptualize a method that satisfies the postulated design objectives and develop a software prototype assisting stakeholders in managing IT solution risks. We evaluate our method and prototype in a single case study at a globally acting manufacturer of construction and demolition tools with over 25.000 employees. We conclude our research by pointing out potential limitations and evincing future work.

Theoretical Background

The risk is a central concept for organizations to describe business-endangering events. We follow the definition by Mitchell (1995), who aggregates various definitions and specifies risk as a "combination of the probability of [a] loss [...] and the significance of that loss to the individual or organization". Risk management aims at protecting the performance of an organization and preserve its ability to fulfill its purpose (Stoneburner et al. 2002). Digitalization and increased collaboration across company levels or beyond company borders emphasize the role of IT in organizations. IT risks have become a major driver of corporate risk (Gulati 2007). Thus, the appropriate management of IT risks is indispensable for preserving business success (Bojanc and Jerman-Blažič 2013; Stoneburner et al. 2002).

Literature distinguishes two types of risks in the area of IT, namely project delivery risks (Mahdi and Alreshaid 2005) and service or solution risks (Lainhart 2000). Project delivery risks are risk scenarios resulting in potential loss through done or missed activities during the runtime of the IT project. Typical project risks are a delayed delivery, a budget overrun, or missing functionality and quality – that is, a violation of the in-budget, in-time, and in-scope criteria (Wallace and Keil 2004). Although they might also cause financial loss, they generally do not directly affect business operations, since the project's result – the solution – is not yet fully established. Thus, project delivery risks need to be managed within a project, but play a minor role on an organizational level. In contrast, solution risks are defined as the potential loss resulting from problems when using the solution, service, or process on an ongoing base (Baccarini et al. 2004). These risks typically include occurrence-related risk scenarios and can be distinguished into four risk categories: security, reliability, availability, and compliance (Rot 2008).

A substantial part of IT risks literature focusses on *security risks* as they are the most complex risk class. A widely used conceptual model for IT security threats is the distinction into unauthorized information release (confidentiality), unauthorized information modification (integrity) and unauthorized denial of use (availability), also known as the CIA triad (e.g., Anderson 1972, Saltzer and Schroeder 1975). In line with this, the US Federal Office for Information Security (2016) defines the basic protection goals of IT security to be preventing electronic information from being corrupted, misused, or made unfit on purpose. The class of *reliability risks* includes all events with the potential to cause a short-term outage or bad performance of a product or service, which are not related to an IT security incident (Yacoub and Ammar 2002). Typical sources of reliability risks include maintenance work on infrastructure or software components, programming errors, deficient IT equipment, and human error. If the service fails for a longer period, it is named an *availability risk*. This term is not to be confused with security-related availability risks, which refer to (usually shorter) outages resulting from security attacks. Availability risks typically represent long-lasting breakdowns of data centers and systems, for example, due to fire, terrorism, or the insolvency of a service provider, and are usually associated with high costs due to business interruptions (Loch et al. 1992). *Compliance risks* can arise from potential non-compliance with regulatory requirements or laws. They often lead to significant penalties or reputational damage. For example, the General Data Protection Regulation introduced in May 2018 significantly increases the requirements for the processing of personal data and enforces higher penalties for improper processing of personal data (European Parliament 2016). Thus, it is crucial for business models and services of companies to meet compliance standards.

The management of risks related to availability, reliability, security, and compliance of IT solutions is an important field of action in most organizations to preserve business operations and leverage business opportunities. To achieve consistency in risk management, the ISO 31000:2009 standard defines a general process for managing risks that includes the phases risk identification, risk analysis (what are likelihood and impact of these risk scenarios?), risk evaluation, risk treatment, risk communication, and risk monitoring (Purdy 2010). Risk identification aims at identifying risk scenarios that might be relevant, risk analysis assesses their likelihood and impact, risk evaluation prioritizes them accordingly, risk treatment

establishes targeted mitigation measures, and risk communication and monitoring refer to the continuous controlling and review of risks.

Each risk scenario can be described as a combination of five aspects, namely threat, threat actor, vulnerability, risk effect, and information asset (Simmonds et al. 2004; Undercoffer et al. 2004). A *threat* can be defined as any circumstance with the potential to adversely affect organizational operations (including mission, function, image, or reputation), organizational assets, or individuals through an information system. Examples would be the breakdown of a specific system or malware. An *actor* executes the threat's force. In the system breakdown example, this could be a cybercriminal, an incautious employee, unreliable hardware, or natural disaster. While the threat itself represents only theoretical danger, it can become real, when a vulnerability paves the threat's way and makes them dangerous for the organization (Stoneburner et al. 2002). A *vulnerability* can be defined as the existence of a weakness, design, or implementation flaw that might lead to an unexpected, undesirable event compromising the intended delivery or behavior of the solution or service (Grobauer et al. 2011; Livshits and Lam 2005). For example, an unprotected network port can be the door opener for an actor trying to close down the system. The impact of threat actions may be facilitated through the ineffective design of systems and processes, ineffective execution of processes (e.g., change management procedures, acquisition procedures, project prioritization processes), missed impact of regulation, inappropriate use, or others. In this vein, *mitigation measures* are technical or organizational measures, which try to control the negative effects of a specific vulnerability. Through appropriate controls, vulnerabilities may be completely or partially eliminated. When a threat successfully exploits a vulnerability and passes mitigation, a risk effect might occur. This risk can cause information flows to stop working the way they are designed to, for example, due to a failing service or an inaccessible database. In the modern data-rich economy, information is often the basis for value creation. This is why cybercriminals mainly aim at a company's *information assets* and companies try to protect them from unwanted effects. These effects, which we refer to as *risk effects*, can, for example, be violations of the CIA principle (Anderson 1972), performance failures (Brynjolfsson and Hitt 2000) impeding timely access to information, irreproducible destruction of databases, or legal penalties (Bose 1995). A *risk scenario* comprises details on these categories and describes a specific risk along them.

The quantification of risks typically considers both the likelihood of occurrence and the impact or damage in case of occurrence. The likelihood can be understood as the interrelation between a threat, which brings along certain effectiveness, a vulnerability, which moderates the threat effectiveness, and the mitigation, which reduces the risk's likelihood to occur. The impact is multi-faceted and encompasses categories of damage such as operational, reputational, or financial damage. However, several ITRM frameworks base their impact calculations on the value of data (Musman et al. 2011; Subashini and Kavitha 2011) and business processes assessments (Kratsch et al. 2017; Najjar and Kettinger 2013). The National Institute of Standards and Technology (NIST) recommends a graphical representation of risks in a two-dimensional risk matrix with likelihood and impact values on the horizontal and vertical axes (Stoneburner et al. 2002). Although the interpretation of a NIST risk matrix is strongly company-specific and depends on individual preferences such as the company's risk appetite, this representation helps to identify the most relevant risk scenarios and manage risks according to their relevance for the company.

Related Work

A broad variety of different approaches aims at increasing risk management quality. Particularly in recent years, scientific research increased their effort to establish a common standard for risk management. Guidelines like ISO 31000:2009 or Guide 73:2009 are first starting points to define high-level risk management standards. However, Purdy (2010) emphasizes the need to develop practical guidance on their implementation. Several researchers already responded to this call. We present existing methods and frameworks for risk management in IT projects in the following.

Bandyopadhyay et al. (1999) propose a high-level framework, which establishes a basic structure to enable managers to identify, analyze, and mitigate IT risks associated with the IT environment. The method aims at a better understanding of the "value of their IT assets, IT risks at different levels, and the related vulnerabilities of IT assets to these various risks" (Bandyopadhyay et al. 1999), but needs more specification. Strauss and Stummer (2002) develop a portfolio-based approach, which assesses IT security risks to select appropriate mitigation measures. They capture the decision maker's individual preferences implicitly and iteratively in a series of dialogue steps to align risk evaluation with the decision maker's

preferences. Rot (2008) suggests the application of various quantitative and qualitative methods to assess security, availability, reliability, and compliance risks to acknowledge the fact that different methods have strengths and weaknesses in specific application scenarios.

IT security-related risk scenarios represent a noticeable focus in literature with detailed studies of individual project and solution characteristics. Karabacak and Sogukpinar (2005) propose a method, which evaluates IT security risks based on an end-user survey. Bojanc and Jerman-Blažič (2013) present a model for evaluating security mitigation measures. As a first step, the model starts with an initial data evaluation, followed by an evaluation of vulnerabilities and threats endangering information assets. Based on this information, the model helps IT security experts to identify rewarding investments in IT security by balancing the loss due to an incident and security costs. Saleh and Alfantookh (2011) suggest a framework integrating and enhancing existing information security risk management standards and methods.

Another topic strongly discussed in the literature is the management of project delivery risks. Some of these concepts consider solution risks as a type of functionality or quality risk to consider that the lack of solution risk control can also prevent successful project termination. Schmidt et al. (2001) propose the use of the Delphi method to evaluate software project risks. This method asks ITPMs a pre-defined set of questions to identify software project risks and ranks them according to their relevance. Herzfeldt et al. (2012) recommend six phases followed by gates, where relevant stakeholders decide whether to proceed to the next stage or not to enhance the structure of a risk management process. Scott and Vessey (2002) subdivide project management into four hierarchical levels: external business context, organizational context, information system context, and the project itself. Changes on higher levels need to be broken down to lower levels. Based on this approach, Churliov et al. (2006) propose to apply "value-focused" thinking in the evaluation of enterprise system risks. Therefore, the authors define risk-related objectives and mitigation measures for each risk scenario. Aloini et al. (2007) conduct an extensive literature review of enterprise resource planning introduction projects to identify potential project delivery risks. Thereby, two of the authors define top project risk scenarios, namely expectation failure (low quality) and correspondence failure (unmatched objectives), which are associated with solution risks. Albadarneh et al. (2015) summarize risk management frameworks in agile software development projects. Baccarini et al. (2004) provide an overview of relevant IT project risks and mitigation measures.

In sum, the literature suggests several theoretical and practical ITRM approaches as depicted in a non-conclusive overview in Table 1, with a wide variety of considered risk categories and phases within the risk management process. Nevertheless, to the best of our knowledge, there is no practical and holistic approach to IT solution risk management in IT projects that accompanies all phases of the risk management process and captures all solution risk categories.

Paper	**Risk categories**	**Process phases**	**IT project scope**
Saleh and Alfantookh (2011)	Security	All phases	All IT projects
Bandyopadhyay et al. (1999)	Security, Availability, Compliance	All phases	All IT projects
Strauss and Stummer (2002)	Security	Risk treatment	All IT projects
Rot (2008)	Security, Availability, Reliability, Compliance	Risk analysis	All IT projects
Karabacak and Sogukpinar (2005)	Security	Risk analysis	Focus on end users
Bojanc and Jerman-Blažič (2013)	Security	All phases	All
Schmidt et al. (2001)	Delivery	Risk identification	Software development
Herzfeldt et al. (2012)	Delivery, Reliability	All phases	Solution provider
Churliov et al. (2006)	Delivery	All phases	Enterprise systems
Aloini et al. (2007)	Delivery	Risk identification	ERP projects
Albadarneh et al. (2015)	Delivery, Security, Reliability	All phases	Software development
Baccarini et al. (2004)	Delivery, Reliability	All phases	All IT projects
This paper	**Security, Availability, Reliability, Compliance**	**All phases**	**All IT projects**

Table 1. Summary of related work on IT project risk management

Research Design

This works aims at developing a method (Brinkkemper et al. 1996) for IT solution risk management in IT projects, which satisfies the design objectives. We follow standard design science research (DSR) guidelines (Hevner et al. 2004) and employ action design research (Peffers et al. 2012; Sein et al. 2011) to iteratively incorporate evaluation activities into the building process as suggested in the General DSR Evaluation Pattern by Sonnenberg and Vom Brocke (2012). This pattern postulates that each building step in the DSR Methodology (Peffers et al. 2007) should be followed by an individual evaluation activity (Eval 1 to Eval 4). We claim relevance based on the lack of an effective method for (solution) risk management in IT projects in both, theory and practice. The literature review on current risk management approaches in general and for IT projects specifically yields justificatory knowledge. It further substantiates the need for a method that enables ITPMs to provide structured and consistent information about IT solution risks and manage them comprehensively (Eval 1).

We use method engineering (Henderson-Sellers and Ralyté 2010) to design the method and derive its conceptual utility for supporting ITPMs through the management of their solution risks (Eval 2). The method's structure takes inspiration from Stoneburner et al. (2002), who propose nine steps to execute an encompassing risk assessment. Interviews with ITRM experts and ITPMs yield requirements and expectations towards the method and provide interesting insights into the challenges of ITRM in projects. Additionally, method construction builds on a thorough review of six extant risk assessments, which have been performed for diverse completed projects in the IT department of an international manufacturer of construction and demolition tools. This procedure results in a process, which comprises all ITRM activities in projects.

In a subsequent evaluation episode, we implement a functional prototype and perform alpha and beta testing activities to demonstrate the method's operationality and suitability (Eval 3). An alpha version of the prototype is released to the three ITPMs of the six completed projects to collect feedback and refine both method and prototype iteratively. For beta testing, we open the prototype to a wider circle of ITPMs and include eight incomplete projects. To test the method's effectiveness and efficiency in a real-world setting (Eval 4), we conduct a case study with 21 IT projects at the aforementioned international manufacturer of construction and demolition tools and utilize semi-structured interviews and a quantitative questionnaire to collect evidence for the method's perceived utility.

The following section describes the developed method. Its evaluation is presented in the section thereafter.

Method Description

Based on the design objectives and method engineering approach described above, we design and develop a method that aims at integrating risk management into IT project management and supports ITPMs in managing their solution's risks. For this, we identified three different risk management activities: 1) risk scenario identification when initiating the project, 2) risk quantification to report on risks when specifying the solution's design and implementation, and 3) selection of appropriate countermeasures to mitigate unacceptable risks when implementing the solution. The activities can be performed in multiple iterations in the course of a project.

In the following, each of these activities is described in an individual subsection. We describe each activity along a structure similar to the necessary method elements proposed by Denner et al. (2018): we 1) present the *activity* itself, 2) specify the *technique* used therein, 3) introduce the *roles* that project and risk managers can take, 4) refer to the mathematical *engine* which represents the methodological backend, and 5) define the *output* as the activity's results. This structure differs from the original structure by Denner et al. (2018) in two points: *tools* is renamed to the *engine* to prevent confusion with the prototype and *roles* and *engine* swapped places for presentation purposes.

Activity 1: Risk identification

Technique: Activity 1 involves the identification of potential risk scenarios based on project and solution characteristics and is typically performed during project initiation and solution design to explore the need for mitigation. It collects information on the characteristics of the solution to determine potential vulnerabilities and threats and to describe potentially relevant risk scenarios (Aloini et al. 2007). Various

catalogs of vulnerabilities, threats, and risk scenarios (Bandyopadhyay et al. 1999; Bojanc and Jerman-Blažič 2013; Herzfeldt et al. 2012) can be used as a basis to describe availability, reliability, security, and compliance risk scenarios. Each risk scenario entails a particular risk effect out of the following list: data destruction, data modification, data theft, data access, service interruption, low solution performance, and legal violations (in two degrees of severity, minor and major). This list is the aggregation of risk effects suggested in the literature (Aloini et al. 2007; Bojanc and Jerman-Blažič 2013) and General Data Protection Regulation (European Parliament 2016).

We collect input following Schmidt et al. (2001) and Karabacak and Sogukpinar (2005), who recommend the application of a structured questionnaire to assess project and solution characteristics. A first question records the artifact type (e.g., application software, platform, or infrastructure) to filter out vulnerabilities that are not associated with the artifact types, e.g., insecure programming patterns might be an issue with software artifacts but are not relevant for pure infrastructure artifacts. The remainder of the questionnaire captures solution characteristics, which are used to indicate further which of the preselected vulnerabilities are potentially relevant. Table 2 presents the high-level categories that are included in the questionnaire. Each question is linked to one or more vulnerabilities and determines whether they are relevant for the solution or not. Therefore, the particular questionnaire depends on which catalog is used for vulnerabilities. Then, the method maps each vulnerability to risk scenarios (threat and risk effect), which can potentially exploit them. The identification of vulnerabilities and associated threats results in a list of risk scenarios that might be relevant for the solution.

Question Category	**Description**
Information on administrators and end users	Missing knowledge of administrators and end users or careless and malicious behavior causes vulnerabilities (D'Arcy et al. 2009).
Information on system access	Data retained by external partners causes vulnerabilities concerning leakage or unauthorized access due to the shared infrastructure (Takabi et al. 2010). The type and usage of login mechanisms suggest various vulnerabilities (Weigold and Hiltgen 2011).
Information on technological and operational change	Massive technological or operational change causes vulnerabilities due to changes in processes and responsibilities (Clements and Kirkham 2010).

Table 2. Categories of the solution characteristics questionnaire

Roles: The method comprises two central roles, the ITPM and the ITRM expert. The ITPM takes a user role and provides project and solution-specific information, which is the questionnaire in this activity. The ITRM expert is responsible for specifying the contents and calibrating the method. This includes complete lists and descriptions of all potential vulnerabilities, threats, and risk scenarios as well as the modeling of the underlying dependence structure. Furthermore, this requires the development and maintenance of the questionnaire as well as the vulnerability and risk scenario mapping (exemplarily depicted in Figure 1).

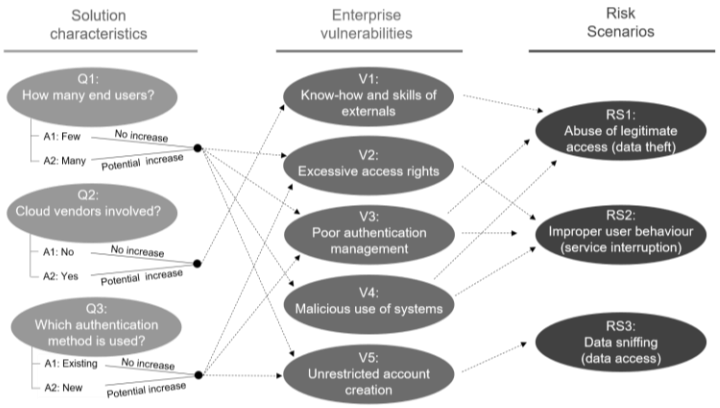


Figure 1. Exemplary characteristic, vulnerability, and risk scenario mapping

Engine: The identification of relevant risk scenarios based on a questionnaire requires a mapping engine. Let $Q_1, \dots Q_n$ be questions with $n \in \mathbb{N}$ individual answer sets $A_i = (a_1^i, \dots, a_{m_i}^i)$, where $m_i \in \mathbb{N}$ denotes the cardinality of the answer set A_i and, thus, the number of possible answer to question Q_i. Each answer set A_i has an ordinal scale. From a risk perspective, a_1^i indicates "no vulnerabilities" and $a_{m_i}^i$ "massive vulnerabilities" with descending interpretable values between. Further, we define for each question Q_i the evaluation metric $\lambda_i: a_j^i \rightarrow [0,1]$ as follows:

$$\lambda_i(a_j^i) = \frac{1}{m_i - 1} \cdot (j - 1).$$

As the vulnerability and risk scenario mapping is interpretable as a graph combining $n \in \mathbb{N}$ questions, $v \in \mathbb{N}$ vulnerabilities, and $r \in \mathbb{N}$ risk scenarios, there exists an adjacency matrix $M \in \{0,1\}^{n \times r}$, which describes the connection between questions and risk scenarios. This matrix contains $m_{ij} = 1$, if there exists a path between question Q_i and risk scenario j, and $m_{ij} = 0$, if there is no such path. Finally, the identification of risk scenario j based on answer vector $a \in A_1 \times A_2 \times \dots \times A_n$ can be conducted by using an identification function f_j. Thereby, the answer vector a represents the selected answer of the questions $Q_1, \dots Q_n$ and, thus, characterizes the project and the IT solution. The identification function $f_j: A_1 \times A_2 \times \dots \times A_n \rightarrow \{0,1\}$ is defined as:

$$f_j(a) = \begin{cases} 1, if \sum_{i=1}^{N} \lambda_i(a_i) \cdot m_{ij} > 0 \\ 0, else \end{cases},$$

where $f_j(a) = 1$ labels the risk scenario j as "identified", which an ITPM has to consider within his project. For this engine, we assume that a risk scenario cannot occur if the potentially exploited vulnerabilities are not given. If required, the same logic can be applied to identify affected vulnerabilities by using the adjacency matrix $M \in \{0,1\}^{n \times v}$.

Output: Activity 1 results in a list of risk scenarios which might be relevant for the solution. These risk scenarios yield a first risk picture of the project-specific solution risk and lay the foundation for risk quantification and mitigation. Furthermore, it creates a list of possible vulnerabilities of the solution.

Activity 2: Risk quantification

Technique: To broaden the scope of our risk analysis, Activity 2 quantifies the likelihood and impact of all identified risk scenario based on information from the project phases solution design and implementation. The multiplication of likelihood and impact equals the expected loss (Sonnenreich et al. 2005). As a new IT solution can change the IT risk landscape (Nocco and Stulz 2006), there exists a pre- and a post-implementation expected a loss for each risk scenario. The delta between both values can be attributed to the solution and, thus, can be used as an indicator for risk relevance.

On the one hand, the likelihood can be calculated by comparing the severity of vulnerabilities without and with the solution. Although there are also some vulnerabilities affecting the impact (e.g., the lack of backups does not make an attack more likely, but increases its impact), the majority of vulnerabilities only affects the likelihood. Our method assumes that attackers most likely choose the most accessible way (Wagener et al. 2011) so that the highest vulnerability for a certain risk scenario determines if an attack is successful or not. Thus, if the severity of the solution vulnerabilities is larger than the severity of the vulnerabilities on an enterprise level, the likelihood of the risk scenario and, thus, the expected loss increases. On the other hand, impact calculation can be based on the value of data used within the solution (Lim et al. 2018; Musman et al. 2011) as well as the value of the solution (Kohli and Grover 2008). This requires an assessment of the organization's data assets, which assigns particular financial damage to each combination of data asset and risk effect. Wang et al. (2011) and Musman et al. (2011) provide a list of critical data assets, which we use in our method. However, the data value does not yet take into account that the value of this data asset can increase with the solution. Therefore, the method should also consider future solution-specific value creation as a determinant for the rising value of data. We use solution life cycle costs as an approximation for the solution's future value (Barth et al. 2001) and distribute these costs evenly over the amortization time to obtain yearly impact values.

Roles: In this activity, the ITPM has to select the data assets that are used by the solution from a pre-defined list and provide the life cycle costs and the expected amortization time of his solution. Additionally, it is the ITPM's responsibility to describe how each risk scenarios can become effective to the solution. On the other hand, the ITRM expert has to provide the company's current risk picture as input for the calibration of the engine. This includes a list with impact and likelihood values for each risk scenario which is usually included in enterprise risk reports, an evaluation of the severity of each vulnerability on an enterprise level, and a completed assessment of data asset values.

Engine: The quantification of risk scenarios requires an engine, which calculates likelihood and impact values based on the solution-specific input of an ITPM. Again, let $Q_1, \dots Q_n$ be questions with $n \in \mathbb{N}$ individual answer sets $A_i = (a_1^i, \dots, a_{m_i}^i)$ and $a \in A_1 \times A_2 \times \dots \times A_n$ denotes the answer vector from Activity 1. Further, we define for each question Q_i the evaluation metric $\rho_i: a_j^i \to \{0, 0.5, 1, 1.5, 2, 2.5, 3\}$ as follows:

$$\rho_i(a_j^i) = \left\lfloor 2 \cdot 3 \cdot \frac{1}{m_i - 1} \cdot (j-1) + 0.5 \right\rfloor \cdot 0.5,$$

where $\lfloor x \rfloor$ denotes the floor function for rounding and $\lfloor 2x + 0.5 \rfloor \cdot 0.5$ rounds values to multiples of 0.5, respectively. This formula maps each answer on a vulnerability severity ranking from zero (no vulnerability) to three (massive vulnerability) under a worst-case scenario assumption without additional mitigation measures. Given the adjacency matrix $M \in \{0,1\}^{n \times v}$ defining the relationship between the modelled questions $A_1, \dots, A_n$ and the vulnerabilities $V_1, \dots, V_v$, we define the solution-specific severity ranking function $s_k: A_1 \times A_2 \times \dots \times A_n \to \{0, 0.5, 1, 1.5, 2, 2.5, 3\}$ of vulnerability V_k as follows:

$$s_k(a) = \left\lfloor 0.5 + 2 \cdot \sum_{i=1}^{n} \rho_i(a_i) \cdot m_{ik} \; / \sum_{i=1}^{n} m_{ik} \right\rfloor \cdot 0.5,$$

where $a_i$denotes the selected answer of question Q_i.Thus, for each risk scenario $R_1, \dots R_r$ with $r \in \mathbb{N}$ exists a solution-specific vulnerability severity ranking vector r_i^s, where each vector element represents the solution-specific severity ranking of an exploitable vulnerability, which is associated with this risk scenario. Thereby, we only consider vulnerabilities with explanatory power regarding the likelihood. In the same way, we define the enterprise vulnerability severity ranking vector r_i^e with the same dimension as r_i^s and the same value set $\{0, 0.5, 1, 1.5, 2, 2.5, 3\}$, where zero denotes "vulnerability has no severity" and three "vulnerability has massive severity" with gradients in between. Severity is based on the current "size" of the vulnerability, considering the current IT landscape and, in particular, existing mitigation measures. For example, if a company does not use any cloud technologies, all cloud-related vulnerabilities would be set to zero. Having this, we define the set of potential likelihood values of a risk scenario R_i as $LL_i \in \{1, 0.5, 0.01, 0.005, 0.001, 0.0005, 0.0001\}$, named "approximately once a year", "more than once every ten years", "once every ten years" and so on. Given the enterprise likelihood LL_i^e of a risk scenario R_i, we assume that the solution-specific $LL_i^s \in \{LL_i^{e++}, LL_i^{e+}, LL_i^e, LL_i^{e-}, LL_i^{e--}\}$, where $LL_i^{e+/-}$ denotes the next higher or lower likelihood value and $LL_i^{e++/--}$ the same with two steps. If the maximum or minimum likelihood value is reached, the likelihood stays the same. Based on the solution-specific and enterprise vulnerability severity ranking vectors r_i^s, r_i^e, we follow Wagener et al. (2011) and quantify likelihood values according to the following case discrimination (their exemplary application is shown in Table 3, grey denotes case-relevant vulnerabilities):

Case 1: We set $LL_i^s = LL_i^{e++}$, if the highest vulnerability severity ranking within r_i^s and r_i^e is originated in r_i^s and difference between the maximum rankings of these vectors is greater than or equal to one.

Case 2: We set $LL_i^s = LL_i^{e+}$, if the highest vulnerability severity ranking within r_i^s and r_i^e is originated in r_i^s and difference between the maximum ranking of these vectors is smaller than one.

Case 3: We set $LL_i^s = LL_i^e$, if the highest vulnerability severity ranking within r_i^s and r_i^e are equal and there exists a maximum value in r_i^s, which corresponding enterprise ranking in r_i^e is smaller.

Case 4: We set $LL_i^s = LL_i^{e--}$, else.

Case	Enterprise vulnerability severity ranking vectors	Solution vulnerability severity ranking vectors	Likelihood of risk scenario LL^s
Case 1	$\begin{pmatrix}0\\2\\1\end{pmatrix}$	$\begin{pmatrix}0\\1\\3\end{pmatrix}$	$LL^s = LL^{e++}$
Case 2	$\begin{pmatrix}0\\2\\1\end{pmatrix}$	$\begin{pmatrix}2\\2.5\\0\end{pmatrix}$	$LL^s = LL^{e+}$
Case 3	$\begin{pmatrix}0\\2\\1\end{pmatrix}$	$\begin{pmatrix}2\\1\\1\end{pmatrix}$	$LL^s = LL^e$
Case 4	$\begin{pmatrix}0\\2\\1\end{pmatrix}$	$\begin{pmatrix}1\\1\\1\end{pmatrix}$	$LL^s = LL^{e--}$

Table 3. Exemplary risk scenario likelihood assessment (grey shows pivotal vulnerability)

We define the impact as $I_i = I_i^{VoS} + I_i^{VoD}$ of a risk scenario R_i, where $I_i^{VoS} \in \mathbb{R}^+$ denotes the impact related to the value of the solution and $I_i^{VoD} \in \mathbb{R}^+$ the impact related to the value of the used data. Thereby, we consider damages that realize within one year after occurrence of the risk scenario. Given the life cycle costs $LCC \in \mathbb{R}^+$ and the expected amortization time $T \in \mathbb{N}$ of an IT solution, we define the impact related to the value of the solution I_i^{VoS} as:

$$I_i^{VoS} = \frac{LCC}{T} \cdot \alpha_{R_i},$$

where $\alpha_{R_i} \in (0,1)$ denotes a scaling factors, which is based on the underlying risk effect of risk scenario R_i and characterizes the company-specific severity of a risk effect. The scaling factors are the same for all risk scenarios since they have the same underlying risk effect. Given a solution, which affects or uses $d \in \mathbb{N}$ data assets, of which we know the data values of data $D_1, \dots, D_d \in \mathbb{R}$ according to the risk effect of risk scenario R_i, where $D_i \geq D_{i+1}$ holds. Recall, the used data assessment assigns each combination of data assets and risk effects an impact value. We find that a geometric series is best to model an impact saturation, since the highest impact value is given by the insolvency or a long-term operational outage. Then, the impact related to the value of data I_i^{VoD} is defined as:

$$I_i^{VoD} = \sum_{j=1}^{d} \frac{1}{2^{j-1}} D_j.$$

Output: Activity 2 results in a list of risk scenarios analyzed according to their likelihood, impact and expected loss values. These values and the solution-specific risk landscape can be visualized within a NIST risk matrix. Further, the method provides a list of all affected vulnerabilities with traffic lights denoting their relevance. Red color coding indicates that a vulnerability is responsible for one of the cases 1 to 3 in likelihood assessment of at least one risk scenario and, thus, is assumed to have a high contribution to risk. The ITPM has to analyze these vulnerabilities to ensure the quality of the solution with high priority. Orange color coding indicates that the vulnerability severity ranking of the solution vulnerability is worse than the enterprise solution. This indicates that the solution's quality is potentially below the enterprise standard. A green vulnerability, if the first two cases are not met, should not involve high-risk potential.

Activity 3: Mitigation selection

Technique: Activity 3 particularly considers the solution's vulnerabilities to select adequate mitigation measures to be established in the project's solution implementation phase. It offers a documentation repository, where the ITPM can structurally enter the planned and implemented mitigation measures for each vulnerability. Additionally, we recommend proposing standard mitigation measures per vulnerability as described by Bandyopadhyay et al. (1999). Nevertheless, mitigation measures have to be selected by the ITPM individually, as there are only a few standards that apply to every solution (Pinto et al. 2006). After the implementation of a mitigation measure, we re-evaluate the risk picture of the solution using an enhanced engine of Activity 2. This allows the ITPM to monitor the risk-related progress of the project.

Roles: The ITRM expert provides a set of questions, which can guide mitigation activities, and standard mitigation measures for each vulnerability. They also support the ITPMs in identifying appropriate mitigation measures in a consulting function. ITPMs execute the identified measures, select the suitable degree of mitigation, and provide a short description of each mitigation measure implemented.

Engine: For the evaluation of mitigation effectivity, we again distinguish between vulnerabilities affecting the impact or likelihood of risk scenarios. We assume that the effect of mitigation measures taken by an ITPM is limited to the solution and cannot lower the company's risk on an enterprise level. Given the enterprise vulnerability severity ranking s_k^e and the solution vulnerability severity ranking s_k^s as introduced in Activity 2, we define the mitigated vulnerability severity ranking $s_k^{s\_mit}$ of the solution for likelihood-related vulnerabilities as:

$$s_k^{s\_mit} = s_k^s - q * \max\left((s_k^s - s_k^e), 0\right),$$

where $q \in \{0,0.5,1\}$ denotes the degree of mitigation. We use the coding "not mitigated" (q = 0), "partially mitigated" (q = 0.5), and "fully mitigated" (q = 1). If a vulnerability is not applicable to an identified risk scenario within a project, the user can select "not applicable" (q = 1). The updated vulnerability severity ranking $s_k^{s\_mit}$ provides the basis for the reassessment of the risk scenario's likelihood as presented in Activity 2. Mitigating impact vulnerabilities leads to a reduction of a risk scenario's impact in case of occurrence (e.g. data backup,). Given the impact I_i of a risk scenario R_i with a defined risk effect and related impact vulnerabilities $V_1, \dots V_p$, we define the mitigated impact I_i^{mit} of a risk scenario R_i as:

$$I_i^{mit} = I_i - \beta_{R_i} \cdot I_i \cdot \frac{1}{p} \sum_{j=1}^{p} q_j,$$

where q_j denotes the degree of mitigation of vulnerability V_j as above and $\beta_{R_i} \in (0,1)$ the mitigation scaling factors, which is based on the underlying risk effect of risk scenario R_i and characterizes the maximal mitigation level. The scaling factors are the same for all risk scenarios since they have the same underlying risk effect.

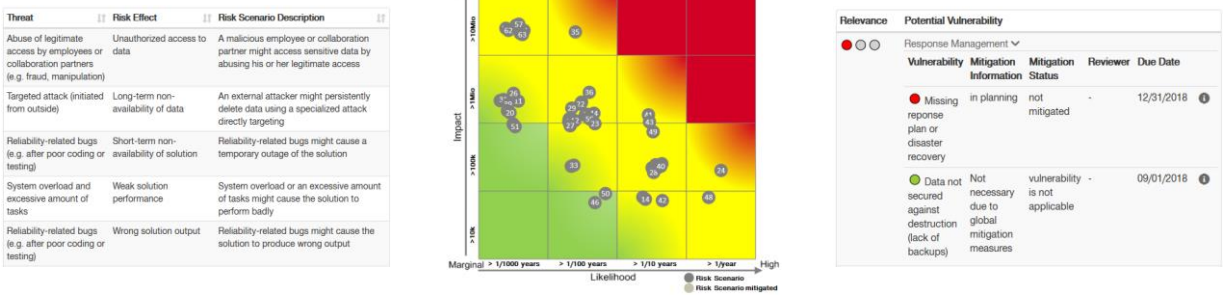
Output: Activity 3 results in an updated list of likelihood, impact and expected loss values for each identified risk scenario, an updated NIST risk matrix, and an updated traffic light visualization. This output is provided multiple times after each mitigation update of the ITPM. Also, the method generates mitigation measure documentation for each vulnerability.

Prototyping

We implemented the proposed method prototypically by means of action design research (Peffers et al. 2012; Sein et al. 2011) to demonstrate its operationality and suitability. In this process, the instantiation was tested and refined in several iterations. In a first step, testing happened within the research team. In a second step, we worked closely together with alpha testers: two ITRM experts provided the instantiation with relevant ITRM. Three experienced ITPMs tested the configured prototype based on six completed projects. Their feedback on missing functionality, improvable usability, and general bugs helped to refine the method and prototype. Two months before releasing the prototype to the company's whole ITPM community, we opened the method to a wider circle of ITPMs as beta testers and integrated their feedback on the user interface and complementary functionality level based on eight current IT projects.

The developed prototype contains all aspects of our method and provides ITPMs and ITRM experts with relevant output for the three activities (cf. Figure 2). Compared to the method, the prototype features some additional functionality. For example, it is not reasonable to fully automate ITRM due to the complexity of both risk management and underlying project characteristics. Therefore, the prototype provides the possibility for ITPMs to manually correct the estimation based on their experience. Beta testers tried to abuse the overwriting of likelihood and impact values for cheating, which is why we highlight them as modified. Interestingly, both risk experts concluded that they had to correct the values of one of the risk scenarios only very sporadically in beta testing. If a correction was necessary, this has been the likelihood value most of the time. Manual correction then triggers a recalculation process updating the initial indicator. Once a solution is deployed, its risks need to periodically monitored (Stoneburner et al. 2002). Thus, the prototype allows to adapt input parameters at any point in time to continuously recalculate risks.

All data entered can be accessed at any time and illustrative material, such as risk heatmaps before and after mitigation measure execution, is provided.



Threat	Risk Effect	Risk Scenario Description
Abuse of legitimate access by employees or collaboration partners (e.g. fraud, manipulation)	Unauthorized access to data	A malicious employee or collaboration partner might access sensitive data by abusing his or her legitimate access
Targeted attack (initiated from outside)	Long-term non-availability of data	An external attacker might persistently delete data using a specialized attack directly targeting
Reliability-related bugs (e.g. after poor coding or testing)	Short-term non-availability of solution	Reliability-related bugs might cause a temporary outage of the solution
System overload and excessive amount of tasks	Weak solution performance	System overload or an excessive amount of tasks might cause the solution to perform badly
Reliability-related bugs (e.g. after poor coding or testing)	Wrong solution output	Reliability-related bugs might cause the solution to produce wrong output

Relevance	Potential Vulnerability				
	Response Management				
	Vulnerability	Mitigation Information	Mitigation Status	Reviewer	Due Date
	Missing reponse plan or disaster recovery	in planning	not mitigated	-	12/31/2018
	Data not secured against destruction (lack of backups)	Not necessary due to global mitigation measures	vulnerability is not applicable	-	09/01/2018

(a) List of Risk Scenarios (b) Risk Scenarios on Heatmap (c) Mitigated Vulnerabilities

Figure 2. Exemplary results of Activity 1 (a), Activity 2 (b), and Activity 3 (c)

During agile prototyping, we gained valuable insights into critical success factors of the method and its instantiation. First, risk identification and analysis are tiresome but inevitable tasks for ITPMs. Elaborating a list of risk scenarios with estimated values for likelihood and impact does not directly provide them a benefit, but automatically visualizing the risks to enable their easy graphical interpretation does. Second, alpha testers suggested single user interfaces for each project management phase that displays all information relevant in this phase in the form of a "one-pager." Third, feedback in beta testing indicates that trust in the quantification algorithm depends less on how high the risks are in absolute numbers, but rather on how high they are compared to other projects. Fourth, single ITPMs expressed that risk assessments should be shareable so that other stakeholders can directly supply information. Fifth, automatically calculated values need to be reported with the right degree of abstraction. A number looking very precise, i.e., with many non-zero digits, might evoke a wrong feeling of accuracy, whereas too high abstraction, e.g., by reporting only one non-zero digit, might neglect important information. Additionally, feedback from alpha and beta testers indicates that acceptance could be further boosted, when additional features that directly or indirectly address needs related to risk management were provided.

Case Study Evaluation

We introduced the method and its prototypical instantiation within the IT department of an internationally working manufacturer of construction and demolition tools with over 25,000 employees worldwide. Supplementary to the physical products, the company is offering digital services to its customers and currently prepares for the launch of the first Internet of Things solutions for construction sites. A centralized IT department with three, globally distributed locations supplies IT services for regional markets worldwide and faces the typical challenges of digitization: an increasing number of IT services is facing consumers and are reachable over the internet, external IT service providers play a growing role in IT operations, and cyber threat is becoming more and more real.

In this environment, the portfolio of IT services is subject to constant change and progress. To make economically sound decisions, management builds on the evaluation of risk and return. With business success strongly depending on information technology, IT is an important contributor to the corporate risk picture. However, a large number of concurrent transformation projects and the change of risk that comes with each project make it hard to obtain a timely and accurate IT risk picture. To make IT-related change manageable, each introduction, replacement, or shutdown of an IT service or their underlying technology is managed and supervised by an ITPM, whose main job it is to provide all stakeholders with the information they need to complete the project. Therefore, this role comes along with a lot of duties that mainly involve communication and information provision. One of these duties is to provide information on the risk that comes with the solution and to implement appropriate countermeasures. Based on this information, management decides on the solution's go-live. Thereby, too high or unmanaged risk can delay or even inhibit successful project completion.

There is a clear process for risk management within IT projects in place: As a first step, ITPMs have the responsibility to deliver a complete list of solution-specific risk scenarios, which include information on associated vulnerabilities, threats, actors, and effects. This description typically includes information on the most likely attack vector, the threat actor, and the potential damage. ITPMs further estimate the likelihood and impact of each risk scenario. ITRM experts review the list of risk scenarios and their quantification based on their knowledge on similar projects and make a recommendation, which risk scenarios are most relevant for mitigation. During solution implementation, ITPMs establish appropriate mitigation measures to reduce risk. The ITRM team offers to consult support throughout the process. Before introducing the proposed method, ITPMs used a templated Excel spreadsheet, which included lists of potential, vulnerabilities, threats and risk scenarios as input for the risk identification process, but left risk assessment and mitigation to the ITPM. In this context, we introduced the proposed method in March 2018 and utilize the prototype to assist ITPMs in all risk management activities within the IT project management process. The prototype was initially configured by the ITRM team to reflect organization-specific knowledge and preferences. This configuration will be subject to an annual review of all relevant parameters. While the method fully replaces the Excel spreadsheet, the general procedure and responsibilities remain the same.

Introduction and training taught us some valuable lessons on the method's critical success factors. First, the provision of assistance in ITRM might blur responsibility for correct risk assessment and mitigation selection results. Thus, the explicit definition and communication of responsibilities is vital. To maintain ITPMs' commitment, we recommend leaving the responsibility with them. Second, standardization typically implies less room for creativity and action. Some ITPMs might seize this opportunity and try to refrain from the tiresome responsibility. To prevent this and for documentation and communication purposes, our method requires the ITPM to provide a detailed explanation of how each risk scenario might become relevant for the solution and further expects detailed input on planned and performed mitigation activities. Third, the method makes ITRM more accessible but does not eliminate the need for a basic understanding of risk management. As a minimum basis, all users must be familiar with general risk management terms to verify and communicate their solution's risks. Thus, the training of ITPMs in risk management terms should be considered in the method's communication strategy.

To evaluate effectiveness and efficiency, six ITPMs and two ITRM experts filled out a questionnaire asking for a quantitative assessment of the perceived complexity reduction and time savings associated with the method on a 5-point Likert scale from 1="I do not agree at all" to 5="I fully agree". The quantitative evidence (see Figure 3) supports our claim that the method provides benefit to the stakeholders of IT solution risk management. The time-consuming task of risk analysis is rated to be much more accessible regarding both, effectiveness and efficiency, after introducing the method. However, the method has only marginal effects on the efficiency of risk communication activities.

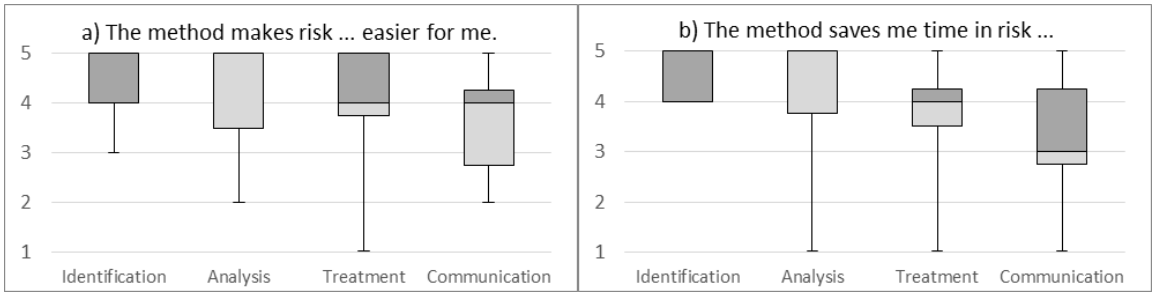


Figure 3. Questionnaire data on effectiveness (a) and efficiency (b), n=8

We additionally conducted semi-structured interviews with the same participants to gain detailed insights into the benefits and weaknesses of the method. We get qualitative feedback on three levels: the result level, the effort level, and the process integration level.

On the result level, one of the ITRM experts reported that the number of risk scenarios per project has increased since the method's introduction and he has the feeling that they are also more complete. However, one ITPM criticizes the missing opportunity to dig deeper into a class of risk scenarios that are particularly relevant for their project. For quantification, four ITPMs expressed that they are confident about the majority of values, although they are not able to verify the results of the quantification. One of them praised

the increased transparency of risk values and mentioned that "the tool makes it easier for me to explain my risk scenarios' likelihood and impact values to my boss and the ITRM team." This statement, however, also hints at the danger that values might be taken for grant and are not consciously used. Although the automatic calculation cannot eliminate errors, one ITPM sees the biggest benefit in the standardized assessment building on consistent scales (cf. Design Objective 1). To substantiate his point, he explains that "the tool replaces unsystematic error through systematic error, which is good because the results remain comparable and the reason for the systematic error can be fixed globally".

On the effort level, five of the six ITPMs emphasized that they experience much higher productivity related to risk management since their effort for risk identification and quantification has substantially reduced compared to the manual approach. The sixth ITPM mentioned this, but mainly saw the downside of this effort reduction and expressed his fear that other ITPMs might not take the task seriously enough when things are getting too easy. All ITPMs agreed that the prototype and visualization of risks make it easier for them to understand the basic risk management concepts and that the automatic calculation acts as a warm start for the discussion of all risk scenarios with the ITRM experts (cf. Design Objective 2). The latter has also been emphasized by the ITRM experts, who, today, experience much better prepared and structured meetings, where ITPMs ask for advice or review of the evaluation of solutions' risk and the selection of appropriate mitigation measures.

On the process integration level, both ITPMs and ITRM experts see a clear improvement in assessment quality, which is the result of the method starting early in the development process to collect risk-relevant information and accompanying all project phases (cf. Design Objective 3). While the ITPMs' motivation to perform IT solution risk management typically only originates in their responsibility to document solution risks, they actively manage project delivery risks to prevent the project from failing. Three ITPMs explicitly wished an extension of the prototype to include project delivery risks because managing them bears similar challenges. Although the method and its engine would be extendible to include delivery risks, it has not yet been part of the research because time restrictions did not permit to develop a second evaluation of characteristics targeting project delivery risks. Both risk experts praised that there is now a central source, where all risk-related information is stored, and expressed their desire to make the reporting of IT risks to the enterprise risk management team easier by aggregating the information on all solutions' risks.

In sum, our evaluation shows that the proposed method has the potential to improve ITRM in terms of effectiveness and efficiency. It also shows that communication and training of end users are crucial. Therefore, we are convinced that the method proposed is worth exploring and could build the foundation for a dynamic approach to ITRM.

Conclusion

With companies increasingly relying on automated IT systems for information process and business process support, the IT landscape is subject to constant change. New or modified IT solutions emerge as the result of IT projects and can significantly change companies' IT risk in terms of likelihood and impact. While an effective and efficient ITRM requires extensive knowledge on single aspects of risk management (e.g., knowledge on vulnerability, threat, actor, impact, or likelihood), it also requires an understanding of the dependencies and interrelations between these facets. Due to the best solution-specific knowledge, ITPMs are usually the ones responsible for managing the risks of the IT solutions they develop, but struggle with the complex task of risk management. We developed a method which integrates knowledge of ITRM experts to standardize and semi-automate the risk management process in a reasonable manner. The method aims to achieve three design objectives: 1) enhance risk management quality by standardizing identification and quantification, 2) make ITRM accessible to non-experst, and 3) assist ITPMs throughout the project management process. A software prototype instantiates this method and is used to evaluate the method in a single case study at a globally acting tool manufacturer with over 25.000 employees. We evaluated effectiveness and efficiency based on a quantitative questionnaire filled out by six ITPMs and two ITRM experts and found that the method provides significant benefit regarding effectiveness and efficiency for risk identification, analysis, and mitigation, but not in the same extent for risk communication. With the same participants, we conducted semi-structured interviews, which indicate that the guided risk assessment can significantly boost ITRM. A major advantage is the interindividual consistency of risk-related information, however, communication and training of the method's end users are crucial.

In total, we are convinced that the method is practically useful for most organizations. Due to the nature of a single case study, the generality of the method has not yet been evaluated for other companies than the one examined in the case study. Therefore, it is not clear, whether the method provides value for other companies that do not base decision-making on the evaluation of risk and return or have not incorporated risk management into their IT project management process. This will be subject to further research. Further, risk management approaches often strive for a holistic view on risks. We suggest an opposing view following the divide-and-conquer principle and propose a method that aims at managing risks locally in projects. Although our method does not yet support the automatic aggregation of information due to the missing consideration of project interdependencies, it generally yields the potential to automate risk management in parts. We aim at further improving our method by performing similar case studies in other companies to scrutinize the generality of our method. To examine the long-term effects with respect to our design objectives, we plan to repeat the quantiative and qualiative evaluation when the method is fully adopted.

Acknowledgments

This research was (in part) carried out in the context of the Project Group Business and Information Systems Engineering of the Fraunhofer Institute for Applied Information Technology FIT.

References

Albadarneh, A., Albadarneh, I., and Qusef, A. 2015. "Risk management in Agile software development: A comparative study," in *Applied Electrical Engineering and Computing Technologies (AEECT), 2015 IEEE Jordan Conference on*, pp. 1–6.

Aloini, D., Dulmin, R., and Mininno, V. 2007. "Risk management in ERP project introduction: Review of the literature," *Information & Management* (44:6), pp. 547–567.

Anderson, J. P. 1972. "Information Security in a Multi-User Computer Environment," in *Advances in computers*, M. C. Yovits (ed.), Boston [etc.]: Academic Press, pp. 1–36.

Baccarini, D., Salm, G., and Love, P. E. D. 2004. "Management of risks in information technology projects," *Industrial Management & Data Systems* (104:4), pp. 286–295.

Bandyopadhyay, K., Mykytyn, P. P., and Mykytyn, K. 1999. "A framework for integrated risk management in information technology," *Management Decision* (37:5), pp. 437–445.

Barth, M. E., Beaver, W. H., and Landsman, W. R. 2001. "The relevance of the value relevance literature for financial accounting standard setting: another view," *Journal of accounting and economics* (31:1-3), pp. 77–104.

Bojanc, R., and Jerman-Blažič, B. 2013. "A quantitative model for information-security risk management," *Engineering Management Journal* (25:2), pp. 25–37.

Bose, P. 1995. "Regulatory errors, optimal fines and the level of compliance," *Journal of Public Economics* (56:3), pp. 475–484.

Brinkkemper, S., Lyytinen, K., and Welke, R. J. 1996. *Method Engineering*, Boston, MA: Springer US.

Brynjolfsson, E., and Hitt, L. M. 2000. "Beyond Computation: Information Technology, Organizational Transformation and Business Performance," *Journal of Economic Perspectives* (14:4), pp. 23–48.

Churliov, L., Neiger, D., Rosemann, M., and Zur Muehlen, M. 2006. "Integrating risks in business process models with value focused process engineering," .

Clements, S., and Kirkham, H. 2010. "Cyber-security considerations for the smart grid," in *IEEE Power and Energy Society general meeting, 2010*: *IEEE PES-GM 2010 ; 25 - 29 July 2010, Minneapolis, Minnesota, USA,* Minneapolis, MN. 7/25/2010 - 7/29/2010, Piscataway, NJ: IEEE, pp. 1–5.

D'Arcy, J., Hovav, A., and Galletta, D. 2009. "User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach," *Information Systems Research* (20:1), pp. 79–98.

Denner, M.-S., Püschel, L. C., and Röglinger, M. 2018. "How to Exploit the Digitalization Potential of Business Processes," *Business & Information Systems Engineering* (60:4), pp. 331–349.

European Parliament 2016. "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)," *Official Journal of the European Union* (119), pp. 1–88.

Federal Office for Information Security 2016. "The State of IT Security in Germany 2016," .
Gordon, L. A., Loeb, M. P., Lucyshyn, W., and Richardson, R. 2000. *CSI/FBI Computer Crime and Security Survey*. https://www.researchgate.net/publication/243784811_CSIFBI_Computer_Crime_and_Security_Survey. Accessed 2 May 2018.
Grobauer, B., Walloschek, T., and Stocker, E. 2011. "Understanding Cloud Computing Vulnerabilities," *IEEE Security & Privacy Magazine* (9:2), pp. 50–57.
Gulati, R. 2007. "Silo busting: how to execute on the promise of customer focus," *Harvard Business Review* (85:5), 98-108, 145.
Henderson-Sellers, B., and Ralyté, J. 2010. "Situational method engineering: state-of-the-art review," *Journal of Universal Computer Science* .
Herjavec Group 2017. "Cybercrime Report," .
Herzfeldt, A. B., Hausen, M., Briggs, R. O., and Krcmar, H. 2012. "Developing a Risk Management Process and Risk Taxonomy for Medium-Sized IT Solution Providers," in *ECIS*, p. 165.
Hevner, A. R., March, S. T., Park, J., and Ram, S. 2004. "Design science in information systems research," *MIS Quarterly* (28:1), pp. 75–105.
Karabacak, B., and Sogukpinar, I. 2005. "ISRAM: information security risk analysis method," *Computers & Security* (24:2), pp. 147–159.
Kohli, R., and Grover, V. 2008. "Business Value of IT: An Essay on Expanding Research Directions to Keep up with the Times," *Journal of the Association for Information Systems* (9:1).
Kratsch, W., Manderscheid, J., Reißner, D., and Röglinger, M. 2017. "Data-driven Process Prioritization in Process Networks," *Decision Support Systems* (100), pp. 27–40.
Lainhart, J. W. 2000. "COBIT™: A Methodology for Managing and Controlling Information and Information Technology Risks and Vulnerabilities," *Journal of Information Systems* (14:s-1), pp. 21–25.
Lim, C., Kim, K.-H., Kim, M.-J., Heo, J.-Y., Kim, K.-J., and Maglio, P. P. 2018. "From data to value: A nine-factor framework for data-based value creation in information-intensive services," *International Journal of Information Management* (39), pp. 121–135.
Livshits, V. B., and Lam, M. S. (eds.) 2005. *Finding Security Vulnerabilities in Java Applications with Static Analysis*.
Loch, K. D., Carr, H. H., and Warkentin, M. E. 1992. "Threats to Information Systems: Today's Reality, Yesterday's Understanding," *MIS Quarterly* (16:2), p. 173.
Mahdi, I. M., and Alreshaid, K. 2005. "Decision support system for selecting the proper project delivery method using analytical hierarchy process (AHP)," *International Journal of Project Management* (23:7), pp. 564–572.
Mitchell, V.-W. 1995. "Organizational Risk Perception and Reduction: A Literature Review," *British Journal of Management* (6:2), pp. 115–133.
Musman, S., Tanner, M., Temin, A., Elsaesser, E., and Loren, L. 2011. "A systems engineering approach for crown jewels estimation and mission assurance decision making," in *2011 IEEE Symposium on Computational Intelligence in Cyber Security (CICS)*: *11 - 15 April 2011, Paris, France ; [part of] IEEE SSCI 2011, Symposium Series on Computational Intelligence,* Paris, France. 4/11/2011 - 4/15/2011, Piscataway, NJ: IEEE, pp. 210–216.
Najjar, M. S., and Kettinger, W. J. 2013. "Data Monetization: Lessons from a Retailer's Journey," *MIS Quarterly Executive* (12:4), pp. 213–225.
Nocco, B. W., and Stulz, R. M. 2006. "Enterprise risk management: Theory and practice," *Journal of applied corporate finance* (18:4), pp. 8–20.
Peffers, K., Rothenberger, M., and Kuechler, B. 2012. "Design science research in information systems. Advances in theory and practice," in *7th International Conference, DESRIST*.
Peffers, K., Tuunanen, T., Rothenberger, M. A., and Chatterjee, S. 2007. "A design science research methodology for information systems research," *Journal of Management Information Systems* (24:3), pp. 45–77.
Pinto, C. A., Arora, A., Hall, D., and Schmitz, E. 2006. "Challenges to sustainable risk management: case example in information network security," *Engineering Management Journal* (18:1), pp. 17–23.
Purdy, G. 2010. "ISO 31000: 2009—setting a new standard for risk management," *Risk analysis* (30:6), pp. 881–886.
Rot, A. 2008. "IT risk assessment: Quantitative and qualitative approach," *Resource* (283), p. 284.

Saleh, M. S., and Alfantookh, A. 2011. "A new comprehensive framework for enterprise information security risk management," *Applied computing and informatics* (9:2), pp. 107–118.
Saltzer, J. H., and Schroeder, M. D. 1975. "The protection of information in computer systems," *Proceedings of the IEEE* (63:9), pp. 1278–1308.
Schmidt, R., Lyytinen, K., Keil, M., and Cule, P. 2001. "Identifying software project risks: An international Delphi study," *Journal of Management Information Systems* (17:4), pp. 5–36.
Scott, J. E., and Vessey, I. 2002. "Managing risks in enterprise systems implementations," *Communications of the ACM* (45:4), pp. 74–81.
Sein, M. K., Henfridsson, O., Purao, S., Rossi, M., and Lindgren, R. 2011. "Action design research," *MIS Quarterly* , pp. 37–56.
Simmonds, A., Sandilands, P., and van Ekert, L. 2004. "An Ontology for Network Security Attacks," in *Applied Computing*: *Second Asian Applied Computing Conference, AACC 2004, Kathmandu, Nepal, October 29-31, 2004. Proceedings*, S. Manandhar, J. Austin, U. Desai, Y. Oyanagi and A. K. Talukder (eds.), Berlin, Heidelberg: Springer, pp. 317–323.
Sonnenberg, C., and Vom Brocke, J. 2012. "Evaluations in the science of the artificial-reconsidering the build-evaluate pattern in design science research," in *International Conference on Design Science Research in Information Systems*, pp. 381–397.
Stoneburner, G., Goguen, A. Y., and Feringa, A. 2002. "Risk Management Guide for Information Technology Systems," *Special Publication (NIST SP) - 800-30* .
Strauss, C., and Stummer, C. 2002. "Multiobjective decision support in IT-risk management," *International Journal of Information Technology & Decision Making* (1:02), pp. 251–268.
Subashini, S., and Kavitha, V. 2011. "A survey on security issues in service delivery models of cloud computing," *Journal of Network and Computer Applications* (34:1), pp. 1–11.
Takabi, H., Joshi, J. B. D., and Ahn, G.-J. 2010. "Security and privacy challenges in cloud computing environments," *IEEE Security & Privacy* (6), pp. 24–31.
Undercoffer, J., Pinkston, J., Joshi, A., and Finin, T. (eds.) 2004. *A target-centric ontology for intrusion detection*.
Wagener, G., State, R., Engel, T., and Dulaunoy, A. 2011. "Adaptive and self-configurable honeypots," in *IFIP/IEEE International Symposium on Integrated Network Management (IM), 2011*: *23 - 27 May 2011, Dublin, Ireland ; [including workshop papers]*, N. Agoulmine (ed.), Dublin, Ireland. 5/23/2011 - 5/27/2011, Piscataway, NJ: IEEE, pp. 345–352.
Wallace, L., and Keil, M. 2004. "Software project risks and their effect on outcomes," *Communications of the ACM* (47:4), pp. 68–73.
Wang, J., Praeg, C.-P., and Spath, D. 2011. *Quality Management for IT Services:* IGI Global.
Weigold, T., and Hiltgen, A. 2011. "Secure confirmation of sensitive transaction data in modern Internet banking services," in *Internet Security (WorldCIS), 2011 World Congress on*, pp. 125–132.
Wes Sonnenreich, Jason Albanese, and Bruce Stout 2005. "Return On Security Investment (ROSI) - A Practical Quantitative Modell," in *Journal of Research and Practice in Information Technology*.
Yacoub, S. M., and Ammar, H. H. 2002. "A methodology for architecture-level reliability risk analysis," *IEEE Transactions on Software Engineering* (28:6), pp. 529–547.
Zissis, D., and Lekkas, D. 2012. "Addressing cloud computing security issues," *Future Generation computer systems* (28:3), pp. 583–592.