Chapter 14
Information Technology Risks: An Interdisciplinary Challenge

Michael Schermann, Manuel Wiesche, Stefan Hoermann, and Helmut Krcmar

This chapter introduces students to general concepts and theoretical foundations of managing risks induced by developing and using information technology (IT risks). This chapter first provides an overview of the broad nature of IT risks. We introduce categories of IT risks to illustrate its diverse and heterogeneous causes and consequences as well as possible strategies required to balance the risks and benefits of information systems. Second, we illustrate the interdisciplinary challenges that come with managing IT risks on the most researched form of IT risk, namely IT project risks. We discuss the subjectivity of IT risks, various IT risk assessment techniques, outline the process of managing IT project risks, and introduce the dynamics of IT project risks. Third, we present five perspectives on IT risks as a fruitful lens to structure the variety of topics in IT risk research. Using these five perspectives as a framework, we present the most frequently cited IT risk research papers and theories. We conclude with an IT risk research agenda that posits worthwhile avenues for advancing the understanding and control of IT risks.

Keywords Information systems · IT risk · IT risk management · IT projects · Information technology

The Facts

- As information technology (IT) becomes ubiquitous, IT risks become an issue of all stakeholders of an organization. The perspective of the stakeholder determines the impact and magnitude of IT risks. Hence, there is no objective measure for IT risks.
- IT risks come into effect when IT impairs the goals of an organization. For instance, a faulty hard disk is not an IT risk per se until a travel agent is no longer able to book air flights.

M. Schermann (✉) · M. Wiesche · S. Hoermann · H. Krcmar
Chair for Information Systems, Department of Informatics, Technische Universität München, Boltzmannstr. 3, 85748 Garching bei München, Germany
e-mail: Michael.Schermann@in.tum.de

C. Klüppelberg et al. (eds.), *Risk – A Multidisciplinary Introduction*,
DOI 10.1007/978-3-319-04486-6_14,

- The term “IT risk” covers a wide range of issues such as: hacking attacks due to insecure software, loss of revenues due to faulty hardware, legacy systems that make organizations dependent on outdated hardware and software, customers that do not trust electronic commerce websites.
- IT risk research and practice have developed a variety of risk analysis techniques to cover the range of potential IT risks. Checklists help to identify recurring IT risks. Delphi studies support the prioritization of IT risk mitigation measures. Benchmarks illuminate shortcomings in running data processing centers.
- IT risks are bound to a specific situation. A malfunctioning online shop may not have a huge impact at 2 a.m. but consequences may be severe in the weeks before Christmas.
- IT and thus IT risks change at a fast-paced rate. Data leaks due to lost mobile phones or laptops were not an issue several years ago. IT risks are characterized by an arms race between IT risks and mitigation solutions. Again and again, online banking solutions need new security measures.
- The most researched IT risks are IT project risks; that is, risks that occur during the development of new software, hardware, and IT services. Thus, IT project risks serve as an exemplary illustration for the interdisciplinary challenges of handling IT risks.
- IT project risks include technical, social, and organizational aspects. IT projects develop new technology that have unintended side effects. The projects’ progress is impaired by weak customer engagement. Project stakeholders may have conflicting views on the project requirements, which often result in extensive completion delays.
- IT risks propagate through organizations. The strategic goal of reducing expenditures often forces organizations to outsource their IT to IT service providers. The service provider upgrades the outsourced information systems resulting in incompatible interfaces. This lack of control affects the IT enablement of critical business processes and raises new requirements that delay strategic IT projects. Finally, the daily IT operations are impaired by communication barriers and unexpected additional efforts.
- Reflecting the diverse nature of IT risks, IT researchers apply theories from many disciplines. IT investment decisions are grounded in decision-making theory while security risks are resolved by transferring methods from engineering disciplines.

1 Introduction

Information systems are entanglements of information technology (hardware and software), people, and organizations. Our fast-changing and technologically progressing economies, societies, and organizations result in complex risks induced by information technology (IT risks) that we are just beginning to understand [7]. The following examples illustrate the complexity of the nature of IT risks:

- Using the wireless Internet connection, the CEO of an international corporation is finalizing an important email on an upcoming merger in his hotel room. However, being jetlagged, he forgets to establish a secure connection and sends the email over the publicly accessible Internet connection of the hotel. A journalist following the CEO because of rumors about the merger eavesdrops on the Internet traffic of the hotel and intercepts the CEO's email. The content of the email circulates to journalists, analysts, and competitors causing the multi-billion dollar merger to fail.
- The social network Facebook collects information on the private and professional lives of its users to market advertising space on the Facebook platform. However, several privacy issues and concerns have heightened the awareness of potential risks from using Facebook on a private or organizational level. Organizations that prohibit the use of Facebook at the workplace must deal with the efforts their employees use to circumvent technological measures of blocking Facebook.
- The project of constructing a nation-wide billing system in Germany for toll roads that involved satellite-based vehicle tracking was delayed by almost three years and far exceeded the planned budget. Mal-specified and faulty communication and privacy concerns raised by non-governmental agencies caused excessive delays, budget overruns and legal actions. Today, the system is operating very effectively and other countries are interested in adopting it.

Managing risks induced by developing and using information systems has been an on-going challenge for practitioners and researchers alike [8]. The increasing importance of information systems in every aspect of our lives makes IT risk research a highly relevant and fruitful ground for interdisciplinary research. This chapter presents an overview of two important streams of IT risk research. In the first stream, researchers categorize important sources of IT risks, such as IT projects or IT operations [9]. In the second stream, researchers study the important steps of managing IT risks [10]. We illustrate both streams of IT risk research using the example of IT project risk management. Next, we sketch the theoretical foundations of IT risk research. The chapter concludes with a presentation of our thoughts on an agenda for interdisciplinary IT risk research.

2 Sources of IT Risks: Where Do IT Risks Come from?

Figure 1 shows important categories of IT risks as they occur in the various stages of interaction between information systems and business processes. In general, information systems provide the most value if they are aligned with the strategic objectives of the organization.

Strategic IT alignment risks originate from situations and events in which information systems do not align with the strategic objectives of the organization. A prominent example for strategic alignment risk stems from the banking industry.

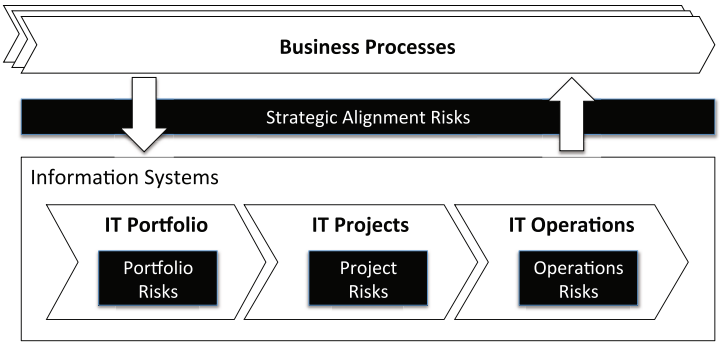

Fig. 1 Sources of IT risks [12]

The advent of mobile banking has drastically changed customers' banking behavior. Most banks struggled with the subsequent business processes because the underlying information systems were inflexible and could not adequately serve these business processes. Typical banking information systems were designed with the highest security standards. This resulted in information systems that were sealed off from the outside world. Customer interaction with these systems was unthinkable. Hence, banks were forced to invest significant sums in the renewal of their information systems. Other strategic alignment risks stem from using (at the time) new technology to support business processes such as IT for e-commerce, financial risk management, support in decision-making, and knowledge management. New information technologies are associated with high uncertainty about the actual capabilities, unintended implications, and their potential business value. For instance, during the rise of e-commerce technologies, risks stemmed from a lack of understanding online consumer behavior [11]. Similar risks are induced by electronic data exchange between organizations and strategic information processing [12].

In contrast to poor strategic decision making, *IT portfolio risks* refer to situations in which the IT department makes bad decisions about what kind of IT should be used and which information systems are necessary to enable business processes. For instance, portfolio risks often arise from outsourcing IT functions [13]. During outsourcing endeavors, organizations usually switch to the information systems of the IT service providers. If future requirements cannot be mapped to these information systems, organizations need to invest in expensive workarounds with poorer performance. For inter-organizational systems, portfolio risks become even more complex and demand cooperation on several levels. This means, organizations need to agree on a shared set of information technologies to establish value chains. More fundamental portfolio risks include IT investment decisions and a missing fit between IT and the corporate culture [14]. For example, while some organizations easily include social networks in their corporate culture, others struggle with deriving value from it.

IT operations risks describe undesired events from a lack of availability, integrity, or confidentiality. Operations risks stem from the failure or misuse of IT [15]. Large-

scale invasions by viruses prevent employees from conducting even the most basic duties such as answering emails or receiving purchase orders. Operations risks can be further divided into two categories: new and unknown risks and known but unsolved risks. In known risks, the degree of uncertainty is relatively low and the number of risks occurring is relatively high. This makes it easier to quantify probability and impact of the considered risks. New and unknown risks usually occur with the emergence of new technologies.

IT project risks describe undesired events during designing, developing, and implementing new information systems [16, 17]. For instance, often stakeholders are not able to define a stable set of requirements. Even after beginning the programming of the information systems, stakeholders change requirements. This results in additional programming efforts that delay project completion. We discuss project risks in detail later in the chapter.

3 Steps of IT Risk Management: How Can One Handle IT Risks?

The goals of IT risk research are to understand what causes IT risks, what are the consequences of IT risks, and how does one deal with IT risks in the most effective manner. Figure 2 illustrates five important steps in handling IT risks based on the 'risk thermostat' by Adams [18] and provides a map for the various research areas on IT risk management. The idea of presenting risk management as a 'thermostat' highlights that the activities of risk management (risk identification, risk assessment, risk mitigation, etc.) are highly intertwined and should not be perceived as an ordered process (though it is being presented that way in most of the literature). Furthermore, the 'thermostat' illustrates that risk mitigation activities do not only affect the original perception and assessment of risks but also the originally stated objectives [18]. Hence, risk management should be seen as a tool to balance objectives and risk with appropriate risk mitigation interventions.

For the first step in the process of risk management, researchers study *IT failures* to understand their specific causes. To do so, they develop explanations of why such failures occur and identify indicators that allow practitioners to identify the associated IT risks as early as possible [17]. For instance, delayed and cost-exceeding software development projects occur from employing immature information technologies. Here, an early indicator would be difficulty in procuring project staffing, i.e., the project manager is not able to find software developers that have experience with the particular technology. Unsecure software often originates in development errors or misuse of information systems [15].

A large body of IT risk research focuses on advancing our understanding of and capabilities for *IT risk assessment*. This literature adopts a general definition of risk from other disciplines [19]. IT risks are events with a probability of occurrence and with either an established or estimated negative impact on the objectives of

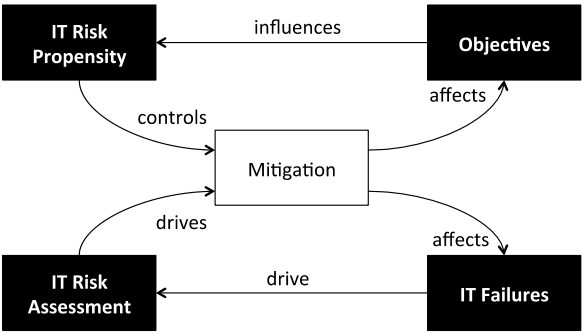

Fig. 2 Steps of IT risk management [18]

stakeholders [20–22]. The challenge with IT risk assessment lies in the subjectivity of IT risks: the stakeholders' perspective determine the impact and the magnitude of IT risks. Hence, it is difficult to establish an objective measure for IT risks.

For the third step in the process of risk management, IT risk research investigates how organizations manage their risk appetite through various levels of *IT risk propensities* that control behavior and decision-making. This stream of research focuses on the integration of risk management in the organization's strategy or strategic decisions on IT through analytical systems or long-term planning and decision support systems. In general, researchers study the decision makers' risk taking behavior [13, 14].

For the fourth step in the process of risk management, IT risk research studies the relationship of risk behavior and the *objectives* of IT endeavors. IT risks come into effect when IT impairs the objectives of an organization. For instance, a faulty hard disk is not an IT risk per se until it hinders a travel agent from booking flights. This literature views IT risks as variations in (often uncertain) outcomes of IT endeavors [11, 23, 24].

The fifth step in the process of risk management, *IT risk mitigation*, is about the design, implementation, and operation measures that help reduce the probability or the impact of IT risks. Here, the major challenges stem from integrating these measures in the business processes. Usually, risk mitigation measures such as entering passwords or using encryptions are perceived as burdensome. Hence, raising the security awareness and ensuring compliance with risk mitigation measures is pivotal in this step of handling IT risks [15].

In sum, the five steps of IT risk management present important fields for studying risks in IT and highlight the intertwined and complex nature of IT risk. The structure of Fig. 2 highlights the dynamics of IT risks and risk management. Effective risk mitigation activities are highly dependent on contextual factors. The variety and interplay between the four perspectives illustrates the challenges of understanding and establishing effective risk mitigation mechanisms in organizations [25]. In the next chapter, we will illustrate these steps using the example of IT project risk management.

4 The Example of IT Project Risk Management

IT project risk management is the most prominent stream of research in IT risk research. Hence, herewith follows an in-depth presentation on the state of knowledge on this topic.

Identifying Causes and Explanations of Failure: The Subjectivity of IT Project Risk The research to date on project failures is inconclusive. The well-known and widely cited Standish Group [26] report that around 68 % of the sampled IT projects are considered as failures (24 %) or challenged (44 %) in regards to either budget, completion schedule, or scope. Other researchers report different results. Sauer et al. [27], for example, find that about 67 % of the analyzed projects met budget, schedule and scope expectations. Based on the common understanding that risk denotes the probability and the loss associated with an unsatisfactory outcome (e.g., [21]), the question arises, 'What exactly renders an outcome unsatisfactory?'. The answer to this question largely depends on the respective stakeholder's expectation or objectives concerning the project. Stakeholders typically comprise the project manager, the project team members, the customer, the user, and the project sponsors. Depending on which perspective one takes, objectives, unsatisfactory outcomes, and thus risks, can vary. For instance, a software development project manager might strive for schedule, budget and scope objectives whereas the customer considers a high user acceptance rate more important. Similarly, for the project manager, an unsatisfactory outcome might be schedule and budget overrun or scope constraints (e.g. unstable requirements) while for the customer unsatisfactory outcomes refer to anything that impedes user acceptance (e.g. an unintuitive graphical user interface). In sum, the multidimensional nature of project success drives our understanding of risk [28]. The perspective of stakeholders determines the impact and magnitude of IT risks.

Assessing the Technical, Social, and Organizational Domains of IT Project Risks The literature describes project risks by grouping them according to common characteristics [8]. This grouping enables researchers to establish checklists of common risks. Although discussed controversially in literature, such checklists provide an easy and low cost approach to identifying risks in a project and are thus popular in research and practice. Table 1 shows a sample of existing studies on IT project risks.

Risks in IT projects can be grouped into three risk domains: the social subsystem, the technical subsystem, and the organizational subsystem. While the latter domain refers to the project management capabilities of the project team and the planning/control techniques applied by the project manager, the social subsystem domain comprises an unstable or highly political social context and users unable or not willing to contribute to project success. The technical subsystem domain captures risks related to unstable requirements, high project complexity and new or unfamiliar technology.

Figure 3 shows empirical evidence on how IT project risks affect the success of the project in terms of process performance (How well does the project

Table 1 Common risks in IT projects ranked by importance [30]

Rank	Schmidt et al. [9]		Kappelman et al. [29]		Hoermann et al. [30]	
1	Lack of effective project management skills	P	Lack of top management support	S	Inadequate technical infrastructure	T
2	Lack of top management commitment	S	Lack of documented requirements	P	Customer expectations	S
3	Lack of required skills in project personnel	P	Weak project manager	P	Core development dependencies	T
4	Not managing change properly	P	No change control process (change management)	P	Complex system architecture	T
5	No planning or inadequate planning	P	No stakeholder involvement and/or participation	S	Post go live approach not defined	P
6	Misunderstanding the requirements	P	Ineffective schedule planning and/or management	P	Customer financial obligations	S
7	Artificial deadlines	P	Weak commitment of project team	P	Expected performance issues	T
8	Failure to gain user commitment	S	Communication breakdown among stakeholders	S	Customer inability to undertake project	S
9	Lack of frozen requirements	P	Team members lack requisite knowledge and/or skills	P	Non-T&M payment terms	S
10	Lack of people skills in project leadership	P	Subject matter experts are overscheduled	P	Functionality gaps	T

T: Technical subsystem, S: Social subsystem, P: Project management subsystem

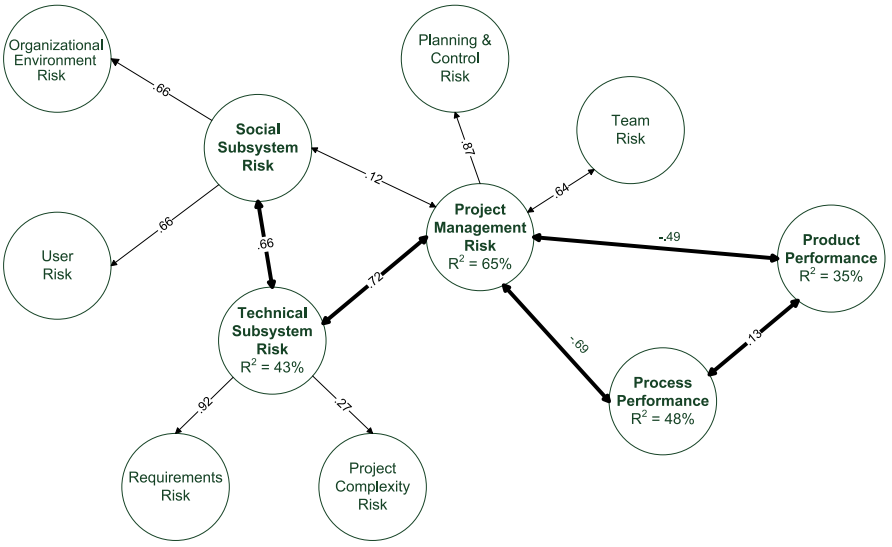

Fig. 3 Effects of IT risk domains on project performance [31]

proceed?) and product performance (How well does the result match the objectives?).

Mitigating IT Projects Risks: Towards Standards of IT Project Risk Management Most authors acknowledge risk management as an integral part of IT projects, especially when it comes to managing large and complex projects. Boehm [21] introduces the concept of risk exposure (defined as probability and impact of an unsatisfactory outcome) to software development projects and characterizes risk management as a process comprising the six steps: risk identification, risk analysis, risk prioritization, risk management planning, risk resolution, and risk monitoring (see Fig. 4).

Instead of describing the risk management process in detail, Lyytinen, Mathiassen, and Ropponen [16] provide a framework to evaluate project risk management approaches as a distinct form of organizational behavior. The framework comprises three distinct environments (the management environment, the project environment, and the system environment), which are linked by the (risk) management process and the development process and help to organize risk management activities in a systematic and comprehensive way.

Understanding the Risk Propensity: The Dynamics of IT Project Risks In addition to the question which risks appear in IT projects and how can these risks be organized, the question of when they appear and how they evolve is also of substantial interest to IT project managers and researchers. Alter et al. [20] discuss several potential limitations of extant research on IT project risk, one of them being the 'frequent omission of the temporal nature of risk'. As the authors state, risks are likely to have different temporal patterns; not only their importance but also the points of time at which they occur can vary over the project life cycle.

In an earlier study, Alter et al. [8] studied the temporal aspect of IT project risks and suggested that linking them to project phases and consequently adapting project risk management increases the likelihood of successful IT projects. The authors identify eight risks and allocate them to seven project phases depending on when their effects become apparent. The identified risks include: non-existent or unwilling users; multiple users and designers; disappearing users, designers or maintainers; inability to specify the purpose or usage pattern in advance; lack or loss of support; lack of prior experience with similar systems; inability to predict and cushion the impact on all parties; and technical problems or cost-effectiveness issues. Alter et al. [8] map these risks to particular project phases and propose several risk-reducing strategies.

In a more recent study, Gemino et al. [32] introduce a temporal model of IT project performance that classifies IT project risks into a priori risks and emergent risks. While the a priori risks are associated with structural elements of the project and with knowledge resources available to the project team, emergent risks denote deficiencies in organizational support or result from the volatility of projects. A project manager might estimate a priori risks before the start of the project; emergent risks only become apparent during particular project phases. Using structural

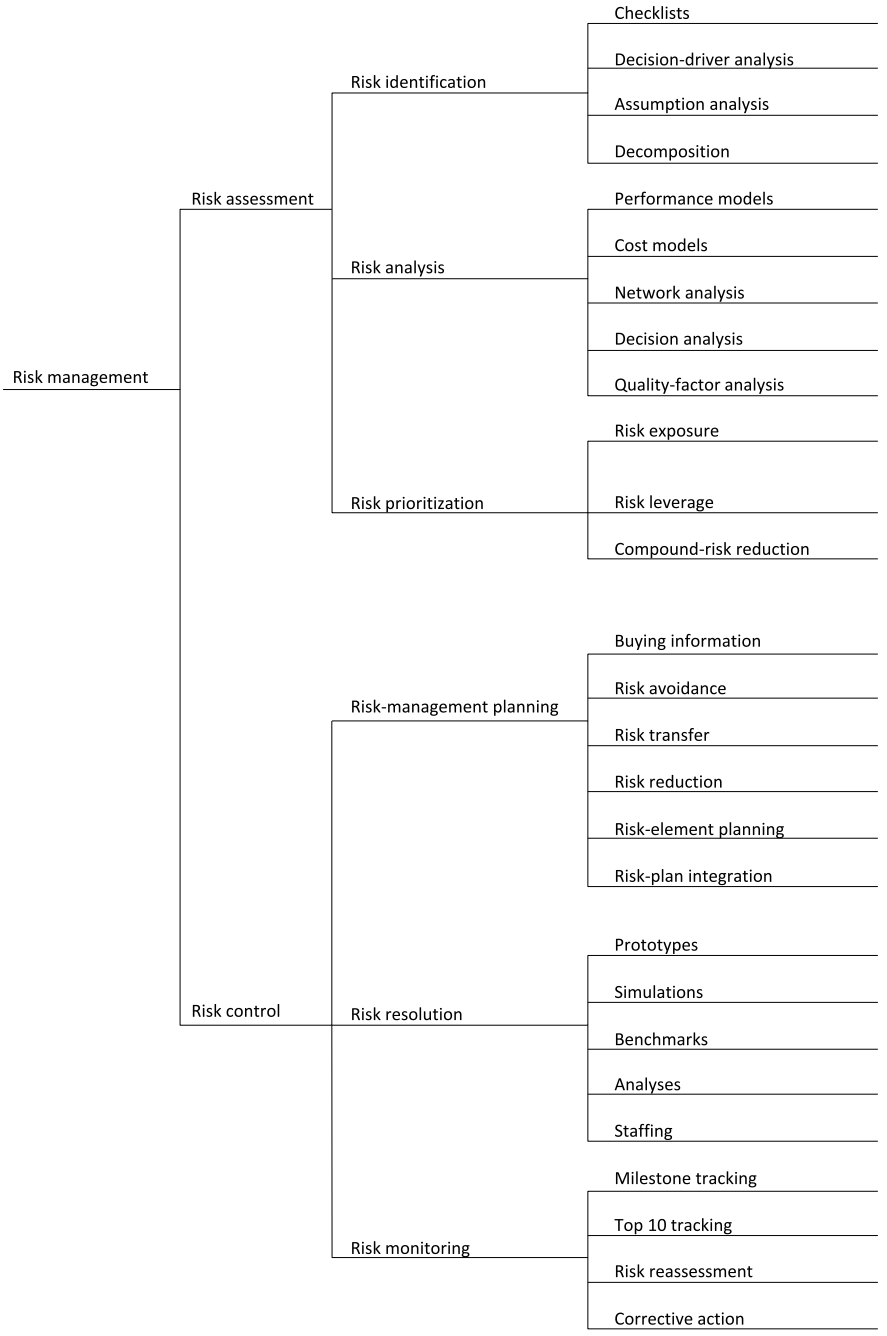

Fig. 4 Project risk management [21]

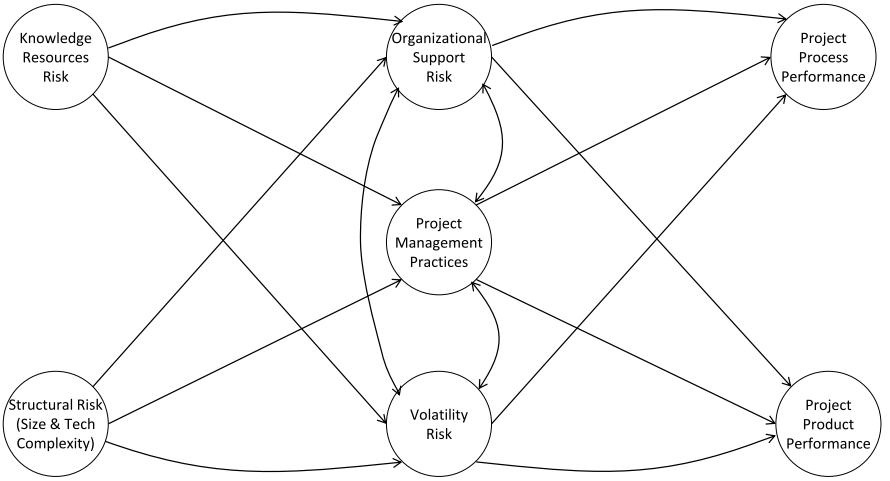

Fig. 5 The temporal model of IT project performance [32]

equation modeling, the authors show that their model offers an improved explanatory power over traditional models of performance, partly resulting from the temporal perspective on IT project risks (see Fig. 5).

Safeguarding the Organizations' Objectives: The Benefit of IT Project Risk Management The benefits of project risk management are difficult to express in financial or other quantitative terms [33]. This means that practitioners of project risk management usually need to justify any effort associated with risk management. Other stakeholders often perceive risk management as an effort that comes on top of an already heavy operational workload. Subsequently, they try to resist or even avoid risk management. A considerable amount of research attempts to provide an empirical verification of the benefits of project risk management (e.g. [17, 24, 31]). Barki et al. [34], derive a contingency model, and hypothesize that project success is affected by the fit between the project's risk profile and its risk management profile. These authors conducted a survey of IT project managers to assess 75 Canadian IT projects in terms of system quality and cost gap (constructs for project success), as well as internal integration, user participation, and formal planning (constructs for the risk management practices). A project's risk exposure can be assessed using Barki et al.'s [23] instrument which comprises 23 risk variables. Analysis of a correlation between the degree of fit between a project's risk profile and its risk management profile and the performance measures indicates that projects that better adapt to their degree of risk exposure usually perform better. In a methodologically quite different action research approach, Baskerville and Stage [35] apply risk analysis to improve the managerial control over prototyping projects. By defining risks, specifying their consequences, assigning priorities, and selecting resolution strategies, the authors suggest that risk management can help improve the communication among users and developers, point out difficulties in maintaining the original project

Table 2 The 10 most-cited publications on IT risk

Citation	Discipline	Domain	Focus
Boehm, 1991 [21]	CS	IT projects	Risk management
Jarvenpaa et al., 2000 [38]	IT	E-commerce	Consumer trust
McFarlan, 1981 [36]	IT	IT projects	Risk management
Alter and Ginzberg, 1978 [8]	IT	IT projects	Risk models
Pavlou, 2003 [39]	IT	E-commerce	Consumer trust
Charette, 1989 [22]	CS	IT projects	Risk management
Barki et al., 1993 [23]	IT	IT projects	Risk factors
Nidumolu, 1995 [24]	IT	IT projects	Risk models
Keil et al., 1998 [37]	IT	IT projects	Risk factors
McKnight et al., 2003 [40]	IT	E-commerce	Consumer trust

CS = Computer science; IT = Information systems research

plan, and get a clearer picture on the status of the project. Using this approach, the authors reported few if any disruptions from the identified risks during the course of the project.

5 Theoretical Foundations of IT Risk

In this section, we discuss the most-cited publications as of April 2011 as a starting point for students who wish to explore IT risk research. On the one hand, reflecting the diverse nature of IT risks, IT researchers apply theories from many disciplines. On the other hand, the field of IT risk research is still very young and thus lacks original theories. This makes IT risk research a very promising ground for interdisciplinary research. The following sections serve as starting points to IT risk research.

Starting Point: The 10 Most-Cited Publications on IT Risk One of the most prominent publications on IT risks originates from the discipline of Computer Science (CS) (see Table 2). Boehm's [21] publication on risks in software development practices provides risk examples, recommendations for best practice, and principles for effective risk management to prevent software project disasters. Other pieces of research address the separate and aggregated assessment of project risks to ensure proper decision-making [36] and strategies for coping with uncertainty in management information systems development projects [8, 22]. Extensive research exists on the effects of coordination mechanisms and risk drivers on project performance [24], the detailed elements, which influence failure in developing systems (tasks, structure, technology, and actors), and lists of software risk factors and mitigation strategies for specific risks [23]. In the field of risk factors, IT project research concentrates on the effects of risk management and environmental factors on risk components, determination and prioritization of risk lists in IT projects [37].

Table 3 Most-cited theories in IT risk research

Citation	Domain	Topic
Williamson, 1979 [41]	Transaction cost economics	Transaction costs vary for firms, markets, and contractors depending on situational setting
Mayer et al., 1995 [44]	Trust	Propose a model of antecedents and outcomes of trust, incorporating trustor, trustee, and the role of uncertainty
Boehm, 1988 [45]	Software development	Proposes a spiral model for software development which consists of four phases of activities and incorporates elements of specification- and prototype-driven processes
Davis, 1982 [46]	Technology acceptance	Develops strategies for determining requirements for IT development on both an organizational and individual level
Grover et al., 1996 [43]	Outsourcing	Determine the importance of service quality and partnership within outsourcing relationships
DeLone and McLean, 1992 [42]	IT Success	Propose an integrated model of information systems success, including the impact of system quality and information quality on organizations
Ang and Straub, 1998 [47]	Outsourcing	Identify the economic determinants of IT outsourcing to incorporate outsourcing decisions in the strategy of an organization
Ganesan, 1994 [48]	Buyer-seller relationships	Finds mutual dependence and trust as determining factors for marketing endeavors under a given timely horizon
Zucker, 1986 [49]	Trust	Discusses processes, contingencies, and institutions as central elements of trust production
Zmud, 1986 [50]	Software development	Develops an approach for staffing, planning, and controlling software development
Akerlof, 1970 [51]	Buyer-seller relationships	Discusses the role of information uncertainty regarding quality heterogeneity in buyer-seller relationships
March and Simon, 1958 [52]	Organization theory	Discuss the motivational and affective aspects of human behavior, and cognition processes in organizations

The second area of research concentrates on the role of IT for on-line transactions. Existing research provides various perspectives on the role of consumer trust in e-commerce transactions. Research provides four high-level constructs: disposition to trust, institution-based trust, trusting beliefs, and trusting intentions for developing and empirically validating measures for a multidisciplinary and multidimensional model of trust in e-commerce [40]. Research also exists on the role of organizational size and popularity on trustworthiness and risk perception [38], and intention to transact and on-line transaction behavior as key drivers for engaging consumers in on-line transactions [39].

Starting Point: The Core Theories of IT Risk IT risk research is grounded in an interdisciplinary set of theories from organizational behavior, management, and

IT. Examples of such theories are thoughts on transaction cost economics which propose: transaction costs vary for firms, markets, and contractors depending on the situational setting [41], IT success is a multi-dimensional construct including influencing factors such as system quality and information quality [42], and the importance of service quality and partnership within outsourcing relationships [43]. Such theories represent the historical development of IT as a socio-economical discipline. Table 3 provides an overview of the most-cited theories.

6 Towards Interdisciplinary IT Risk Research

We return to the examples given in the introduction to illustrate the multi-dimensional character of IT risks. The impact of IT and the associated risk are continuously produced and reinterpreted on all levels of society. In the first example, the CEO chose convenience over security by sending confidential emails over an unsecured network. Through deliberately ignoring security advice, the CEO renders as useless the risk mitigation strategies of his company. In his work setting at a hotel, the risk of eavesdropping conflicted with achieving his objective, which was to communicate a message intended to be received by a specific, targeted group.

Facebook accumulates mass data through continuously adding new functionality, such as geo-coding of messages, and people begin using it in unanticipated ways, such as organizing political uprisings. Hence, governments and institutions have begun to criticize Facebook because of either privacy concerns or a sense of loss of control. Despite any real or perceived issues of privacy, people and organizations increasingly use Facebook to communicate. Similarly, appropriate mitigation strategies are the temporary result of agreement among many stakeholders within and across an organization. In the case of the billing systems for road tolls, the project should be considered a total failure according to typical project success measures. However, the steady governmental income and the ease of use of the system on an organizational level have led to reinterpretations of the project. In light of the system's success, even the privacy concerns on a societal level took a back seat in the public discussion.

To cover these aspects of IT risks, a multi-disciplinary body of theory is necessary. Therefore, we identified and reviewed publications on risk outside of the IT discipline. We analyzed these publications using qualitative data analysis and present these central publications on risk and discuss their potential for advancing IT risk research.

What Are Elements of IT Risks? Other disciplines discuss the fundamental elements of risk in great detail. For instance, Kahneman and Tversky ([53], cited 572 times per year) theorize about biases and the role of heuristics in individual risk perception. On a societal level, Beck ([54], cited 592 times per year) analyzes the structures and social systems of communicating risks as well as reaching societal

consensus on risks. Still, research on the elements of risks in information systems provides promising ground for advancing a commonly shared understanding of IT risk. This issue is highlighted by the fact that no established and commonly shared definitions of "IT risk" exist [20].

What Are Measures of IT Risks? Measures of risks are an enduring topic in other disciplines. Artzner et al. ([55], cited 226 times per year) develop risk measures for financial markets. Similarly, Sharpe et al. ([56], cited 169 times per year) measure the effect of adding assets to a financial portfolio. By contrast, Slovic ([57], cited 142 times per year) explores contortions in measuring risk perception in groups. Kahneman and Tversky ([53], cited 572 times per year) show that utility is an inappropriate measure for risks. Although many authors question the applicability of financial risk measures to IT risks [58], some IT authors show their applicability in the domains of contract portfolios of IT services [59]. The research of Slovic [57] and Kahneman and Tversky [53] provides valuable insights into measuring qualitative risk as it is often suggested in the IT project management literature.

What Are Acceptable IT Risks? Given limited resources for risk mitigation, an important challenge in risk management is determining acceptable levels of risk. Here again, other disciplines provide promising trains of thought. Jorion ([60], cited 206 times per year) introduces the value at risk measure to determine acceptable levels of risk in the financial domain. Criticism against transferability to other domains has been expressed [58]. However, IT researchers have begun to explore the use of value of risk to determine acceptable levels of project risks [61]. Research on the social acceptability of risks offers valuable insight on risk. Douglas ([62], cited 148 times per year) explores the collaborative interpretation of acceptable risks by diverging stakeholders. IT researchers increasingly argue that strategic IT decisions under risk, successful IT projects, and collaboration risks in IT need to evolve from a single dimensional (shareholder) perspective to a multi-dimensional (stakeholder) perspective. Using the body of knowledge on risk research in sociology and thoughts on acceptable risk could provide a fresh perspective and help to develop theories with potential to bring about significant progress in risk research in IT.

What Are the Benefits of Risky Behavior with IT? Knight ([19], first edition from 1921), has been cited 732 times per year across disciplines, which makes the publication one of the fundamental and most-influential publications on risk. Knight's [19] main argument is that coping with unknown risks determines the success of economic organizations. Thus, organizations that mitigate risks effectively are able to allocate more resources to dealing with uncertain issues. Zuckerman ([63], cited 483 times per year) explores the psychological mechanisms for taking risks. His view provides a fresh perspective on risk for the IT discipline where risk is commonly associated with negative effects, failures, and loss (e.g. [23]). Beck ([64], cited 170 times per year) analyzes the potentials of transparent and open societal processes that construct shared understanding of risk and uncertainty. Research

in IT could fundamentally benefit by incorporating the notion of uncertainty in risk research. This would shift the focus from risk exposure as a basis of decision making to situations where the probability distribution of a random outcome is unknown. Measures could be developed to cope with new and unknown risks effectively, such as through early warning systems. Unfortunately, many risk incidents incorporate a high degree of uncertainty and often lack the necessary number of empirical incidents to soundly predict the underlying distribution.

In sum, this chapter provides an overview of IT risk research, outlines the existing body of knowledge on IT risk research, and identifies promising areas for future research. With information systems becoming ubiquitous, IT risks permeate every aspect of life and effective risk mitigation increasingly requires an interdisciplinary approach.

7 Food for Thought

- Collect IT risks from newspapers and press releases. Identify what caused the IT risk, what mitigation activities where taken, and what was the damage or loss of the project.
- Consider the case of a faulty airline check-in system that was not online for a day and a half. The faulty system caused quite a stir among customers and the press but an analysis two months after the incident showed that the actual damage was way below €250,000. Discuss and develop an explanation.
- Discuss the statement of a CIO of a major corporation: "IT risks are a daily issue but without IT risks I would be afraid we would be behind our competition".
- Discuss the case of the billing systems for road tolls. First, stakeholders, press, and public opinion considered the project to be a total failure. Two years after the project was completed, the steady incomes on the governmental level as well as the system's ease of use have led to reinterpretations of the project. Today the system is being exported to other countries.
- Develop an IT risk assessment for the risk of hackers entering the billing system of a large online shopping system and stealing 100,000 sets of credit card information. Develop the risk assessment from the perspective of a person affected by this incident and from the perspective of the provider of the online shopping systems.

8 Summary

To operationalize the advancement of IT risk research, we first conceptualize three levels of research inquiry as one dimension of a research agenda. On the individual level, risk research focuses on the mechanisms of risk perception and the subjective assessment of risks. On the organizational level, risk research focuses on

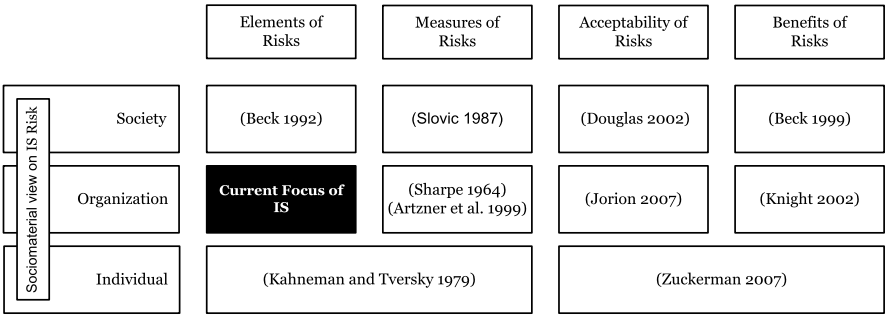

Fig. 6 Starting points for interdisciplinary IT risk research

managing risks as a function to achieve organizational goals. On a societal level, risk research focuses on the social construction processes that lead to either consensual or conflicting norms and practices for coping with risks. The other dimension of the research agenda consists of the four bodies of theoretical foundations of risk research, which we discussed above. Figure 6 shows the research agenda along with seminal publications as starting points toward interdisciplinary IT risk research.

References

Selected Bibliography

1. S. Alter, S. Sherer, A general, but readily adaptable model of information system risk. Commun. AIS **2004**(14), 1–28 (2004)
2. H. Barki, S. Rivard, J. Talbot, Toward an assessment of software development risk. J. Manag. Inf. Syst. **10**(2), 203–225 (1993)
3. R. Charette, *Software Engineering Risk Analysis and Management* (Multiscience Press, New York, 1989)
4. R.K. Rainer Jr., C.A. Snyder, H.H. Carr, Risk analysis for information technology. J. Manag. Inf. Syst. **8**(1), 129–147 (1991)
5. D.W. Straub, R.J. Welke, Coping with systems risk: security planning models for management decision making. MIS Q. **22**(4), 441–469 (1998)
6. L. Wallace, M. Keil, A. Rai, How software project risk affects project performance: an investigation of the dimensions of risk and an exploratory model. Decis. Sci. **35**(2), 289–321 (2004)

Additional Literature

7. M. Wiesche et al., Classifying information systems risks: what have we learned so far? in *46th Hawaii International Conference on Systems Science (HICSS 2013)*, Maui, HI, USA (2013)

8. S. Alter, M. Ginzberg, Managing uncertainty in MIS implementation. Sloan Manag. Rev. **20**(1), 23–31 (1978)
9. R. Schmidt et al., Identifying software project risks: an international Delphi study. J. Manag. Inf. Syst. **17**, 5–36 (2001)
10. J.R.K. Rainer, C.A. Snyder, H.H. Carr, Risk analysis for information technology. J. Manag. Inf. Syst. **8**(1), 129–147 (1991)
11. P.A. Pavlou, D. Gefen, Psychological contract violation in online marketplaces: antecedents, consequences, and moderating role. Inf. Syst. Res. **16**(4), 372–399 (2005)
12. M. Junginger, *Wertorientierte Steuerung von Risiken im Informationsmanagement* (Universität Hohenheim, Stuttgart, 2004)
13. C.L. Iacovou, R. Nakatsu, A risk profile of offshore-outsourced development projects. Commun. ACM **51**(6), 89–94 (2008)
14. M. Benaroch, Y. Lichtenstein, K. Robinson, Real options in information technology risk management: an empirical validation of risk-option relationships. MIS Q. **30**(4), 827–864 (2006)
15. D.W. Straub, R.J. Welke, Coping with systems risk: security planning models for management decision making. MIS Q. **22**(4), 441–469 (1998)
16. K. Lyytinen, L. Mathiassen, J. Ropponen, A framework for software risk management. J. Inf. Technol. **11**(4), 275–285 (1996)
17. J. Ropponen, K. Lyytinen, Can software risk management improve system development: an exploratory study. Eur. J. Inf. Syst. **6**(1), 41 (1997)
18. J. Adams, *Risk* (Routledge, Oxford, 1995)
19. F.H. Knight, *Risk, Uncertainty and Profit* (BeardBooks, Washington, 2002)
20. S. Alter, S. Sherer, A general, but readily adaptable model of information system risk. Commun. AIS **2004**(14), 1–28 (2004)
21. B. Boehm, Software risk management: principles and practices. IEEE Softw. **8**(1), 32–41 (1991)
22. R. Charette, *Software Engineering Risk Analysis and Management* (Multiscience Press, New York, 1989)
23. H. Barki, S. Rivard, J. Talbot, Toward an assessment of software development risk. J. Manag. Inf. Syst. **10**(2), 203–225 (1993)
24. S. Nidumolu, The effect of coordination and uncertainty on software project performance: residual performance risk as an intervening variable. Inf. Syst. Res. **6**(3), 191 (1995)
25. M. Schermann, *Risk Service Engineering: Informationsmodelle für das Risikomanagement* (Gabler, Wiesbaden, 2011)
26. The Standish Group, *CHAOS Summary for 2010* (The Standish Group, Boston, 2010)
27. C. Sauer, A. Gemino, B. Reich, The impact of size and volatility on IT project performance. Commun. ACM **50**(11), 79–84 (2007)
28. A. Shenhar et al., Project success: a multidimensional strategic concept. Long Range Plan. **34**(6), 699–725 (2001)
29. L. Kappelman, R. McKeeman, L. Zhang, Early warning signs of IT project failure: the dominant dozen. Int. J. Proj. Manag. **23**, 31–37 (2006)
30. S. Hoermann, M. Schermann, H. Krcmar, Towards understanding the relative importance of risk factors in IS projects. A quantitative perspective, in *18th European Conference on Information Systems*, Pretoria, South Africa (2010)
31. L. Wallace, M. Keil, A. Rai, How software project risk affects project performance: an investigation of the dimensions of risk and an exploratory model. Decis. Sci. **35**(2), 289–321 (2004)
32. A. Gemino, B. Reich, C. Sauer, A temporal model of information technology project performance. J. Manag. Inf. Syst. **24**(3), 9–44 (2007)
33. K. de Bakker, A. Boonstra, H. Wortmann, Does risk management contribute to IT project success? A meta-analysis of empirical evidence. Int. J. Proj. Manag. **28**(5), 493–503 (2010)
34. H. Barki, S. Rivard, J. Talbot, An integrative contingency model of software project risk management. J. Manag. Inf. Syst. **17**(4), 37–69 (2001)

35. R. Baskerville, J. Stage, Controlling prototype development through risk analysis. MIS Q. **20**(4), 481–504 (1996)
36. F.W. McFarlan, Portfolio approach to information systems. Harv. Bus. Rev. **59**(5), 142–151 (1981)
37. M. Keil et al., A framework for identifying software project risks. Commun. ACM **41**(11), 76–83 (1998)
38. S.L. Jarvenpaa, N. Tractinsky, M. Vitale, Consumer trust in an Internet store. Inf. Technol. Manag. **1**(1–2), 45–71 (2000)
39. P.A. Pavlou, Consumer acceptance of electronic commerce: integrating trust and risk with the technology acceptance model. Int. J. Electron. Commer. **7**(3), 101–134 (2003)
40. D.H. McKnight, V. Choudhury, C. Kacmar, Developing and validating trust measures for e-commerce: an integrative typology. Inf. Syst. Res. **13**(3), 334–359 (2003)
41. O.E. Williamson, Transaction-cost economics: the governance of contractual relations. J. Law Econ. **22**(2), 1–30 (1979)
42. W.H. DeLone, E.R. McLean, Information systems success: the quest for the dependent variable. Inf. Syst. Res. **3**(1), 60–95 (1992)
43. V. Grover, M.J. Cheon, J.T.C. Teng, The effect of service quality and partnership on the outsourcing of information systems functions. J. Manag. Inf. Syst. **12**(4), 89–116 (1996)
44. R.C. Mayer, J.H. Davis, F.D. Schoorman, An integrative model of organizational trust. Acad. Manag. Rev. **20**(3), 709–734 (1995)
45. B.W. Boehm, A spiral model of software development and enhancement. IEEE Comput. **21**(5), 61–72 (1988)
46. G.B. Davis, Strategies for information requirements determination. IBM Syst. J. **21**(1), 4–30 (1982)
47. S. Ang, D. Straub, Production and transaction economies and IS outsourcing: a study of the US banking industry. MIS Q. **22**(4), 535–552 (1998)
48. S. Ganesan, Determinants of long-term orientation in buyer-seller relationships. J. Mark. **58**(2), 1–19 (1994)
49. L.G. Zucker, Production of trust: institutional sources of economic structure, 1840–1920. Res. Organ. Behav. **8**, 53–111 (1986)
50. R. Zmud, Management of large software development efforts. MIS Q. **4**(2), 45–55 (1980)
51. G.A. Akerlof, The market for "lemons": quality uncertainty and the market mechanism. Q. J. Econ. **84**(3), 488–500 (1970)
52. J. March, H. Simon, *Organizations* (Wiley, New York, 1958)
53. D. Kahneman, A. Tversky, Prospect theory: an analysis of decision under risk. Econom., J. Econom. Soc. **47**(2), 263–291 (1979)
54. U. Beck, *Risk Society: Towards a New Modernity* (Sage, Frankfurt am Main, 1992)
55. P. Artzner et al., Coherent measures of risk. Math. Finance **9**(3), 203–228 (1999)
56. W.F. Sharpe, Capital asset prices: a theory of market equilibrium under conditions of risk. J. Finance **19**(3), 425–442 (1964)
57. P. Slovic, Perception of risk. Science **236**(4799), 280 (1987)
58. D.B. Parker, Risks of risk-based security. Commun. ACM **50**(3), 120 (2007)
59. R.J. Kauffman, R. Sougstad, Risk management of contract portfolios in IT services: the profit-at-risk approach. J. Manag. Inf. Syst. **25**(1), 17–48 (2008)
60. P. Jorion, *Value at Risk: The New Benchmark for Managing Financial Risk*, vol. 2 (McGraw-Hill, New York, 2007)
61. M. Sutter et al., Calculating the conditional value at risk in IS projects: towards a single measure of project risk, in *19th European Conference on Information Systems (ECIS)*, Helsinki, Finland (2011)
62. M. Douglas, *Risk and Blame: Essays in Cultural Theory* (Routledge, New York, 2002)
63. M. Zuckerman, *Sensation Seeking and Risk* (American Psychological Association, Washington, 2007)
64. U. Beck, *World Risk Society* (Polity Press, Cambridge, 1999)