Information Infrastructure Risk
Perspectives, Practices & Technologies

Lars Öbrand

To Elsa and Sara, the loves of my life

Table of Contents

Abstract

This dissertation investigates the nature and management of information infrastructure risks in organizations. Specifically, it examines how practitioners identify and manage threats towards their organizational aims, and suggests ways of achieving sustainable risk management, in settings characterized by the integration of information technology (IT) and organizational processes. The dissertation is motivated by the difficulties organizations encounter when attempting to leverage IT as an organizational resource and the observation that IT projects have high rates of failure despite three decades of research on and practice of risk management in Information Systems (IS). The dissertation problematizes extant research on risk in our field and challenges its ontological and epistemological assumptions.

As the role of IT in organizations has changed significantly over the last decades, so has both practice and research concerned with IT related risks. Research on risk in the field of IS has thus come to encompass a large variety of levels of analysis, risk levels and dimensions, organizational processes and research approaches. An analysis of the extant literature shows that despite this richness, it still does not account, or offer support, for situations characterized by a high degree of uncertainty and equivocality. In these kinds of situations, risks are typically emergent and cannot be identified or managed by the prescriptions found within the IS discourse. However, emergence has long been recognized as a characteristic of the organizational consequences of information technology. Paradoxically, while most IS scholars would recognize the socio-technical, or even sociomaterial, nature of IT, it has had little impact on research on risk in our field.

A key argument in this dissertation is that theories of technology and organizational change within IS are equally valid for practice and research on IT related risk and risk management. Information infrastructure theory has been influential in improving our understanding of the changing nature and role of contemporary IT in organizational processes. It highlights the infrastructural character of IT, technological agency, and the entanglement of IT and organizational practices. Grounded in information infrastructure theory, this dissertation examines how practitioners identify, assess, prioritize and resolve risk in their everyday organizational practices. While risk has been used as a concept to characterize the underlying logic of information infrastructure evolution, scant attention has been paid to the particularities of risk emergence and operational risk management practices. As such, existing IS research on risk management explains *why* risk emerges

but not *how*. The notion of practice has recently gained momentum in the IS field for its usefulness as an analytical lens in approaching complex, dynamic and emergent phenomena, and it is reflective of information infrastructure theory in its fundamental ontological and epistemological assumptions. All of the papers included in this dissertation build, to varying degrees, on information infrastructure theory and a practice approach.

The dissertation contributes new knowledge to research on information infrastructure risk and risk management in IS by theorizing information infrastructure risk as emergent, interstitial, and rooted in practice and sociomaterial contexts

Acknowledgements

Most importantly, thank you Sara. You are fantastic. Without your love, support and patience, this work would never be finished. You and Elsa are my alpha and omega. You make everything meaningful.

Finally, thank you dear reader, for making it this far. Just a few pages to go now.

Preface

This dissertation consist of a cover chapter and five research papers. The following research papers are included:

Paper 1: Rönnbäck, L., Holmström, J. & Hanseth, O. (2007) *"IT-adaptation challenges in the process industry: an exploratory case study"* Industrial Management & Data Systems, Vol. 107, No. 9, pp. 1276-1289

Paper 2: Öbrand, L., Holmström, J. & Mathiassen, L. *"Between a rock and a hard place: facing dilemmas in IT risk management"* Currently under review (1st round) at an international journal.

Paper 3: Öbrand, L., Holmström, J. & Newman, M. *"Recalcitrant technologies and unfolding ontologies: exploring epistemic strategies in IT risk management"* Currently under review (1st round) at an international journal.

Paper 4: Öbrand, L., Augustsson, N-P., Holmström, J. & Mathiassen, L. *"Information infrastructure risk: longitudinal study of risk emergence in supplier practices"* Currently under review (2nd round), at an international journal

Paper 5: Öbrand, L. *"Managing information infrastructure risk: problems, causes, cures"* Currently under review (1st round) at an international journal.

Introduction

Background - Information technology, risk & organizational change

Information technology (IT) and risk are closely linked. Perhaps incidentally, the word risk appears to have entered the western vocabulary at approximately the same time as Pascal invented the mechanical calculator in 1642, while the concept of risk management coincides with the advent of supercomputing in the early 1960's. Today, risk is broadly defined as something that poses a threat to the achievement of a specific goal, or, as the international standards organization puts it, "the effect of uncertainty on objectives" (ISO31000, 2009). As such, risk is a particular form of uncertainty – i.e. "*the state, even partial, of deficiency of information related to, understanding or knowledge of an event, its consequences, or likelihood*" (ISO 31000, 2009) – concerning both what we are striving to achieve and our ability to identify or imagine potentially consequential events or developments. Over the course of its history, IT has been used by organizations both as a means of achieving and as a tool for managing complexity and reducing uncertainty by increasing control (Hanseth & Ciborra, 2007). Consequently, it is very closely related to both these aspects of risk. Furthermore, IT is a trigger of risk and new risks have emerged in the wake of various technological developments and applications (Bannerman, 2008; Keil, Tiwana, & Bush, 2002; Lee, 2014; Lyytinen, Mathiassen, & Ropponen, 1996; Smith, McKeen, & Staples, 2001). The increasingly infrastructural and boundary spanning character of IT has been consequential for contemporary organizational life, risk included, and the sources and characteristics of risk have changed (Ciborra, 2004; Hanseth & Ciborra, 2007; Öbrand, Augustsson, Holmstrom, & Mathiassen, 2012). For these reasons the field of Information Systems (IS) offers a good point of departure for understanding risk and risk management related to organizational use and development of IT. For the same reasons, risk and risk management represent a good point of departure for making new contributions to the field of IS.

Risk management can be described as the process by which risks are *identified*, *analyzed* and *handled* in order to improve the chances of achieving objectives. In other words, the practice through which risk is managed. There are numerous more precise definitions (Bannerman, 2008; Boehm, 1989, 1991; Charette, 1989; ISO31000, 2009) but they all reflect this basic concept and vary primarily in the delineation of the specific steps into

which the process is divided. Risk management is a fairly recent function in organizations and has come a long way since its origins in insurance and financial businesses (Dionne, 2013). IT risk management methods first appeared in software development groups but these practices have since spread to and been studied in a wide range of organizational processes and structures. Today, risk management is widely used in IT projects as well as strategic and operational processes related to IT, and there is a plethora of commercial risk management methods and standards on the market and used by organizations.

A review of the literature on risk and risk management in IS reveals a rich and diverse discourse spanning the last three decades. Despite a historical predilection for focusing on software development projects, research now covers a range of areas, phenomena, theories, tactics, and levels of analysis. Although diverse, most previous research efforts can be broadly divided into (1) risk factor, or checklist, approaches; (2) process and non-process approaches; and (3) contingency approaches. Analysis of the underlying assumptions of central concepts within the discourse reveals that these approaches build on an instrumental notion of risk, and while useful in many situations they cannot explain risk or support risk management in situations characterized by high degrees of uncertainty and equivocality. However, such situations are becoming increasingly common due to the organizational use of IT. Indeed, Bannerman (2008) concludes that *"the conceptualization of 'risk' in the research literature may be narrower that the nature of the problem in practice requires"*.

A key assumption in this dissertation is that theories concerning IT and organizational change are equally valid for issues of IT-related risk and risk management in organizational processes. The organizational consequences of IT are a long standing core concern in IS research (Markus & Robey, 1988; Robey & Boudreau, 1999), and many studies have sought to explain and understand the complex relationship between organizations and their IT-based information systems. IT-related risk and risk management constitute particular relationships between organizations and their IT, and as such, the nature, characteristics and role of technology do not differ from other instantiations of this relationship.

Researchers are continually challenged to make sense of the local appropriation of new IT. While some researchers argue that IT creates fairly deterministic pressures on organizations (Kallinikos, 2004; Malhotra, Gosain, & Sawy, 2005), others address the limitations of this determinism and focus on situated actions and reactions (Boudreau & Robey, 2005; Ciborra, Braa, & Cordella, 2000; Orlikowski, 2000). In such cases the

materiality of the technology cannot be ignored (Jonsson, Holmström, & Lyytinen, 2009), but can be appropriated idiosyncratically. Against this backdrop, sociomateriality has recently become an umbrella concept (or arguably, *the* umbrella concept) for theories that assume the emergent imperative and are based on a relational ontology (Cecez-Kecmanovic, Galliers, Henfridsson, Newell, & Vidgen, 2014; Orlikowski & Scott, 2008). There is a growing body of literature highlighting how social and material agencies are entangled, situated, reciprocally constitutive and enacted in practice. While the sociomateriality discourse primarily deals with questions of ontology and epistemology, many IS researchers build on these assumptions when theorizing the organizational consequences of IT (Gaskin, Berente, Lyytinen, & Yoo, 2014; Leonardi, 2011). Reflecting the epistemological stance of sociomateriality, the practice perspective has gained momentum among IS and organizational scholars (Feldman & Orlikowski, 2011). Adopting a practice lens has proven useful for understanding complex, novel, and emergent phenomena (Barley & Kunda, 2001; Ciborra, 1996), and is used as both an empirical lens and theoretical approach (Barley, 2015; Feldman & Orlikowski, 2011). At the core of practice theory are the ideas that situated everyday actions are consequential in the production of social life, that dualisms are rejected as a way of theorizing, and that relationships are mutually constitutive (Feldman & Orlikowski, 2011).

Information Infrastructure theory (Blechar & Hanseth, 2007; Hanseth & Lyytinen, 2010; Hanseth, Monteiro, & Hatling, 1996) addresses issues of control and change in relation to the complexity created by increased convergence of digital technologies (Tilson, Lyytinen, and Sørensen (2010). As a result of the digital convergence, single systems are seldom isolated but rather deeply socially and technologically embedded (Tilson et al., 2010) and conditioned by installed bases of socio-technical arrangements (Henfridsson & Bygstad, 2013). The notion of information infrastructure offers two important advantages (Bygstad, 2010): it changes the object of study from a single application within an organization to large socio-technical networks; and it offers a new perspective on how such networks develop. While risks play an important role in the evolution of information infrastructure (Ciborra et al., 2000; Hanseth & Ciborra, 2007; Star & Ruhleder, 1996), there has been little emphasis on understanding risk practices as they play out within information infrastructure evolution. Rather, the concept of risk has been used to explain how side-effects and unintended consequences challenge established notions of control (Hanseth, Ciborra, & Braa, 2001; Hanseth, Jacucci, Grisot, & Aanestad, 2006).

Problem statement and research objective

Over the last decades IT has fundamentally reshaped the conditions for organizing (Orlikowski & Robey, 1991; Tilson et al., 2010) and constitutes a key strategic and operational issue for contemporary organizations. However, despite over 30 years of research and practice, organizations still struggle to leverage IT as an organizational resource (Bharadwaj, El Sawy, Pavlou, & Venkatraman, 2013; Kohli & Grover, 2008; Sambamurthy, Bharadwaj, & Grover, 2003) and IT projects continue to fail with alarming frequency (Bannerman, 2008; Taylor, Artman, & Woelfer, 2012). Ambitious and rigorous attempts have been made in both industry and academia to develop comprehensive risk checklists (Moynihan, 1996; Schmidt, Lyytinen, Keil, & Cule, 2001; Wallace, Keil, & Rai, 2004), process models (Boehm, 1991; Charette, 1996) and analytical frameworks (Barki, Rivard, & Talbot, 2001; Lyytinen et al., 1996; Ropponen & Lyytinen, 2000; Taylor et al., 2012), in order to address this problem. Unfortunately, these efforts have not appreciably reduced the frequency of project failure.

The digital convergence enabled by the integrational character of IT has resulted in increasingly complex amalgams of organizational arrangements that make up organizational life (Hanseth & Ciborra, 2007; Hanseth & Lyytinen, 2010; Tilson et al., 2010). While the use of information systems has traditionally been linked to the ability to control (Beniger, 2009), there is contradictory evidence with regards to its actual outcomes (Ciborra et al., 2000; Drummond, 2011; Orlikowski, 1991). As a consequence, risk will increase (Hanseth & Ciborra, 2007). Risk and risk management therefore constitute a key issue and challenge for organizations.

This does not mean, of course, that the work of practitioners and researchers has been without effect. Many risks are today systematically and efficiently identified and handled in IT projects and within organizations. However, new and salient risks that are outside the scope of existing risk management regimes continue to emerge (Hanseth & Ciborra, 2007). Consequently, there is a need to revisit and reevaluate key assumptions concerning IT risk and risk management (Carlo, Lyytinen, & Boland, 2004; Ciborra, 2004; Hanseth & Ciborra, 2007; Mumford, 1996).

Information infrastructure theory offers an alternative perspective on the character and role of IT in organizations and organizational change processes. Rather than focusing on isolated information systems, it recognizes the heterogeneity of the social and technological components of contemporary organizational life (Ciborra et al., 2000; Star & Ruhleder, 1996) and adopts an emergent and sociomaterial view of agency and

practice, thus building on significantly different ontological and epistemological assumptions than the bulk of IS research on risk. It is also a perspective that has made significant contributions to other areas of IS research as it has proven useful for conceptualizing the collectives of interconnected information systems in organizations (Hanseth & Lyytinen, 2010; Henfridsson & Bygstad, 2013; Tilson et al., 2010). Furthermore, the literature on information infrastructure has introduced an alternative notion of risk to the IS field (Hanseth et al., 2001; Hanseth et al., 2006), adopted from sociology and based on the work of Beck (1992) and Giddens (1999). It differs from the instrumental notion of risk that dominates IS research efforts by assuming risk to be socially constructed and pragmatic, but has to date primarily been used as a rationale for the mechanisms of change within information infrastructures.

As the reach of new IT continues to stretch to different forms of organizations and across ever-more diverse practices, it is imperative that researchers and practitioners alike develop an improved understanding of IT's interactions with the often pluralistic and organic contexts into which it is introduced. On the basis of a practice approach and an information infrastructure perspective, I argue that by identifying the specific practice logics of a given project, it is possible to determine whether these logics are congruent with that of an introduced information system, and thus reliably assess the potential for value creation and the risks associated with the corresponding information systems.

Lyytinen & King (2004) argue that salience and plasticity in the IS discourse are key drivers of legitimacy. Salience refers to the importance of producing research results that matter, for both research and practice. Plasticity is needed because IS research targets a moving target with ongoing developments in technology and practice. This dissertation builds on that idea and suggests that it should include research on risk and risk management. Against this backdrop, the objective of this dissertation is to *analyze how information infrastructure risk emerges and is managed.*

Contribution

This dissertation contributes to extant research by empirically investigating the conditions for and enactment of risk management practices in information infrastructure settings through three qualitative case studies. Two of the case studies were carried out within process industry organizations, in which traditional mechanical technology is increasingly becoming digitized and interconnected. The third study is a longitudinal case study of risk management in information infrastructure provisioning

conducted by an IT consultancy organization. The findings of these studies are presented in the five appended papers, each of which addresses different and relevant aspects of the research objective.

The first paper explores critical IT-adaptation challenges in the process industry by investigating the character, role and consequences of infrastructural technology in a paper and pulp factory. It contributes to information infrastructure theory by highlighting the need for further empirical evidence of, and theorizing on, information infrastructure risk management practices.

The second paper reports findings from a case study at another paper and pulp factory. An analysis of risk management practices in terms of governing variables and action strategies revealed and explained a novel phenomenon – the risk dilemma. It contributes to research on risk and risk management by introducing the notion of risk dilemmas and presenting a practice-based view of risk as an important complement to the instrumental view that dominates both research and practice.

The third paper is based on the same data set as the second, but focuses specifically on how risks are triggered in information infrastructure settings. Conceptualizing risk management as performative, rather than ostensive, it uses concepts from the sociomateriality discourse to explore the internal dynamics of IT risk by investigating the interaction between the character and role of technology in relation to practice. It contributes to IS research on information infrastructures by offering empirical evidence for and theorizing about how risks are triggered in such settings. It contributes to IS research on risk by illustrating and explaining the limitations of traditional risk approaches.

The fourth paper examines how a team of IT professionals managed risk through their practices relating to information infrastructure provisioning over a period of ten years. Adopting a practice lens and analyzing the pragmatics of information infrastructure risk, it shows how risks become increasingly emergent and interstitial as the character of technology changes. It contributes to information infrastructure theory by pinpointing the causes and sources of emergent risk. Moreover, it contributes to IS research on risk by questioning the conventional wisdom of focusing on project-level analyses and by extending our understanding of the limits of risk list approaches.

The fifth paper discusses implications for practice in the management of information infrastructure risk. It reviews the current state of information infrastructure risk research and argues that extant risk management

methods actually constitute a key source of risk for organizations rather than being a viable solution to their problems. It contributes to practice, IS research on risk, and information infrastructure theory by adopting the concept of collective mindfulness from research on high-reliability organizations (HRO), as an alternative way of managing information infrastructure risk.

Beyond the individual contributions to information infrastructure theory and IS research on risk, the dissertation as a whole contributes new knowledge to IS research on risk and information infrastructure theory by *theorizing information infrastructure risk and risk management practice.*

Dissertation structure

This dissertation consists of a cover paper and a collection of five research papers. The remainder of the cover paper is structured into the following sections:

Chapter 2 presents a literature review of related research, specifically IS research on risk, and information infrastructure theory.

Chapter 3 positions the dissertation and outlines its ontological and epistemological assumptions, which are then used to justify a set of methodological choices.

Chapter 4 summarizes the research papers

Chapter 5 discusses the findings in light of the dissertation's research objective.

Chapter 6 presents conclusions

The five research papers are appended after the cover paper.

Information infrastructure risk

This section presents the dissertation's theoretical foundations. It includes a literature review covering two areas of research within the IS discourse to which the dissertation contributes: Risk, and Information Infrastructure. These two areas are initially discussed individually, followed by an outline of their intersection. As stated in the introduction, research on risk within IS has historically struggled to predict or explain new kinds of risks encountered by practitioners. It also struggles to prescribe useful ways and means of managing these risks. Based on these observations, I will problematize the literature on risk and risk management within the IS discourse by analyzing the paradigmatic assumptions it is based on (Alvesson & Sandberg, 2011). I will do so by investigating the ontology and epistemology of the notion of risk within IS research by drawing on concepts from both general risk theory (Renn, 1992) and the discourse on organizational consequences of IT from the IS field, with a particular focus on the notion of emergence (Robey & Boudreau, 1999). I will first present an overview of the literature, starting with a brief overview of general risk theory, followed by a more detailed review of the discourse on risk within the IS field.

Risk

There is no commonly accepted definition of the term risk. It is used and understood in a multitude of ways in research, in practice, and in general, so there is a need to define, categorize and classify it (Renn, 1992), especially as a theoretical construct for use in research (Blumer, 1931) as chances are we otherwise mean different things when referring to the notion (Vlek, 1996). While risk and risk management, as a phenomenon and process, has always been part of human life, the term did not make inroads into research until after World War II (Fischhoff, Watson, & Hope, 1984). In an overview of some 30 years of research on risk, Renn (1998b) defines the only common denominator among the different uses of the term as: *the distinction between reality and possibility*. Risk, thus, will only make sense if one accepts the assumption that human activities are consequential in the production of reality. Risk is often associated with the undesirable consequences of the causal relationship between reality and our activities. It is therefore both a descriptive and a normative concept (Renn, 1992, 1998b) that includes assumptions about cause-effect relationships (of any kind – scientific, religious, superstitious or otherwise) along with an (often implicit) idea of reducing unwanted effects by modifying the things that cause them or mitigating their consequences (Renn, 1992). Importantly for the purposes of

this dissertation, this definition of risk also highlights the need to investigate both reality, i.e. the ontology of information infrastructure risk, and possibility, i.e. the epistemology of risk, as well as their relationship.

Risk and risk management is part of many streams of research and numerous perspectives on risk have been outlined in the literature. The categorization of Renn (1992), divides these perspectives according to their conceptualization of three key elements: undesirable outcomes, possibility of occurrence, and state of reality. He uses this categorization to identify four research perspectives: technical risk analysis, and economic, psychological, or sociological perspectives of risk. Technical risk analyses perspectives attempt to predict the probability of failure related to complex technological systems. Typically, undesirable events include only events that can be objectively observed or measured. Illustrative examples can be found within IS research on software project risk (Boehm, 1989; Charette, 1989), where risk is understood to be the probability-weighted impact of an event on a project. This impact can be approximately estimated using the expression $R = P \times I$ where R is the risk exposure connected to a particular risk factor, P is the probability of realization, and I is the impact on project outcomes (Bannerman, 2008).

Technical risk approaches have been heavily criticized by social scientists for being severely limited in scope (Beck, 1992; Ciborra, 2004; Clarke & Short Jr, 1993; Renn, 1992, 1998b) as they neglect the social processes through which risks are meditated. As noted by Renn (1998b), this approach:

- Neglects that the things actors perceive as undesirable effects depend on the actors' values and preferences.
- Cannot capture the complexities of the interaction between human activities and consequences.
- Might actually increase risk because the organizational structures for managing and controlling risks are prone to failures and deficiencies, which is usually disregarded in risk analyses.
- Assumes equal numerical weight for both magnitude and probability, making it impossible to differentiate between high-consequence/low-probability and low-consequence/high-probability events.
- Implies a clear distinction between experts and laypersons.
- Assumes that risk should be reduced proportionally to the expected harm, thus neglecting that social actions for risk management may have objectives beyond merely minimizing risk.

Renn (1998b) concludes that other, complementary, risk analyses are needed to cover aspects of risk that fall outside the narrow scope of technical risk analyses. However, within these rather severe limitations, technical approaches are efficient at capturing certain kinds of risk.

Economic perspectives on risk build on the idea that risk is mediated through social processes, and focus on subjective utility rather than objectively observable events (Renn, 1992). Consequently, subjective dissatisfaction is measurable (including social effects), and it is possible to quantitatively compare different risk and benefit options. However, the underlying assumption is that individuals are making risk decisions and that the consequences are limited to the decision maker – conditions that are seldom met. Organizational decisions concerning risk are typically collective. Additionally, they often implicate and affect third parties who may not benefit from the decision (MacLean, 1986). Economic perspectives also assume the rational actor paradigm (Renn, 1992), which is contradicted by a significant body of evidence, e.g. (March & Shapira, 1987).

Psychological perspectives on risk take a step further away from technical risk analyses and expand the subjective realm by including psychological aspects of judgment beyond utility preferences, and focusing on risk-related decision making processes as they are shaped by contextual variables (Renn, 1992). This approach highlights the multidimensionality of risk as a concept but is limited by its individual focus.

Sociological perspectives on risk assume that human perception is always filtered through a social context that is both individual and structural, objective and constructivist (Renn, 1992), and links social judgments about risk to individual or social interest and values. A sociological perspective on risk increases its complexity by understanding undesired events as socially defined and, sometimes, socially constructed. Events are mediated through social interpretations and linked to group interests and values (Bradbury, 1989). Risk, thus, does not just have objective, subjective and individual behavioral aspects; it is also pragmatic. As noted by Renn (1998b):

"Possibilities for future events are not confined to the calculation of probabilities but encompass group-specific knowledge and vision. Furthermore, possibilities are shaped by human interventions, social organizations, and technological developments [...] Ignoring the connections between social organizations and technological performance may seriously underestimate the likelihood of failures [...] reality is seen as both a system of physical occurrences (independent of human observations)

10

and constructed meanings with respect to these events and to abstract notions" (Renn, 1998b)

Risk management is also closely related to the notion of uncertainty (Jaeger, Webler, Rosa, & Renn, 2013; Knight, 2012; Miller, 1977; Power, 2008). The International Standards Organization defines risk as *"the effects of uncertainty on objectives"* (ISO31000, 2009), thus highlighting the differences between the two concept and their relationship to one-another. While risk necessarily means uncertainty (because it concerns our perception of what might come to pass), uncertainty is not always a risk – in other words, risk is identified when an uncertainty is perceived as a possible threat to what one wants to achieve. As Ciborra (2004) succinctly put it: *"Risk management is all about uncertainty regarding future events"*. As such, some uncertainties are framed as risks, and treated differently to those which are not.

Risk and risk management within IS research

The discourse on risk and risk management within IS research has evolved over more than four decades. The earliest works in this area were produced by pioneers such as Boehm (1973) and Alter and Ginzberg (1978). Over the years, many researchers have contributed to the field, making the discourse rich in terms of theoretical approaches and diverse in terms of both methodological choices and studied phenomena. Research relating to software and software development projects has consistently formed a stable core of the discourse (Alter & Ginzberg, 1978; Bannerman, 2008; Barki, Rivard, & Talbot, 1993; Boehm, 1989; Charette, 1989; Currie, 1998; Keil et al., 2002; Lyytinen, Mathiassen, & Ropponen, 1998; McFarlan, 1981; Persson, Mathiassen, Boeg, Stenskrog Madsen, & Steinson, 2009; Taylor et al., 2012). A characteristic of the discourse is its close relationship with practice, and as the use and importance of IT has evolved, research has followed. Contemporary research on risk in IS encompasses a great richness of approaches, theories and risk constructs. In keeping with the field's closeness to industry, most of these approaches can be characterized as applied, and cover dimensions ranging from the technical (Boehm, 1991) to the managerial (McFarlan, 1981) and behavioral (March & Shapira, 1987). While many analyses have been conducted at the project level, studies conducted at the organizational (Dhillon, 1996), inter-organizational (Aron, Clemons, & Reddi, 2005), and even societal (Mumford, 1996) levels have also been reported. Complementing the research on software development projects are investigations of risk related to various other phenomena and areas, such as outsourcing (Aubert, 2005; Bahli & Rivard, 2003), enterprise resource planning (ERP) (Aloini, Dulmin, & Mininno, 2007; Sumner, 2000),

security (Nizovtsev & Cremonini, 2009; Straub, 1990), knowledge management (Alhawari, Karadsheh, Talet, & Mansour, 2012; Massingham, 2010), and IT investment (Otim, Dow, Grover, & Wong, 2012). Developments in the field have been summarized in a number of literature reviews (Bannerman, 2008; Ciborra, 2004; Lyytinen et al., 1998; Taylor et al., 2012). However, most of these focus on risk relating to software development projects. This underlines the central role that software development projects have played in the history of risk research within IS.

More than half of the research efforts reviewed in this chapter (67 of 128) concern risk in relation to software development or implementation projects. These efforts have to a large extent shaped the discourse on risk within our field, especially in the early stages (see chart below). Bannerman (2008) divided research on project risk and risk management within IS into four categories: checklists, analytical frameworks, process models and risk response strategies. Lyytinen et al. (1998) identifies risk management approaches according to the kinds of risk they aim to manage: software risks, implementation risks, project portfolio risks, or requirement risks. In contrast, Taylor (2006) distinguishes between risk factor-based, risk management-based, and contingency-based research. Each different system of categorization produces a slightly different picture but the main contours of the discourse are basically identical no matter which approach is chosen. To provide a more nuanced overview I will combine the categories proposed by Bannerman (2008) and Taylor et al. (2012), which partially overlap but highlight different aspects of the discourse. While the classical approaches identified by Lyytinen et al. (1998) remain valid, they have (as demonstrated above) been complemented by an increasing number of phenomena where risk is an issue.

Checklist and risk-factor approaches build on the idea that most, if not all, relevant risks can be identified *ex ante*, after which appropriate measures can be taken to manage them, typically using heuristics. This approach has contributed significantly to both research and practice in terms of identifying commonly occurring risks related to specific risk levels, e.g. software development and information technology implementation projects (Alter & Ginzberg, 1978; Barki et al., 1993; Boehm, 1989; Gemino, Reich, & Sauer, 2007; Moynihan, 1996; Schmidt et al., 2001; Tesch, Kloppenborg, & Frolick, 2007), including outsourcing projects (Aron et al., 2005; Nakatsu & Iacovou, 2009; Taylor, 2006) and ERP related risks (Huang, Chang, Li, & Lin, 2004; Sumner, 2000). The checklists vary in detail, scope and content, and several attempts have been made to compile aggregate lists. Although substantial and important, some drawbacks of this research have been highlighted (Bannerman, 2008). First, checklists tend to focus the attention of risk

managers only on the included risks, thus increasing the likelihood of overlooking potential risks that are absent from the list (Keil, Li, Mathiassen, & Zheng, 2008; Lyytinen et al., 1998). Second, checklist approaches offer little or no guidance as to which particular lists are suitable for addressing a given situation (Bannerman, 2008). Third, this approach implicitly assumes that sufficient knowledge can be obtained by risk managers at the start of a project (Taylor et al., 2012) and that risk decisions are made based on this knowledge. This assumption is problematic because studies have shown that there are often high levels of uncertainty and complexity in IT projects (Barki et al., 2001; Mathiassen & Stage, 1990), and because the decisions made by risk managers aren't always based on pure rationality and objective knowledge (Lauer, 1996; March & Shapira, 1987).

Both process and non-process approaches to risk management are common in the literature (Bannerman, 2008; Taylor et al., 2012). Analytical non-process frameworks approaches have been proposed as both alternative ways of thinking about risk, e.g. (Lyytinen et al., 1996), and as a way of leveraging risk management efforts by offering an opportunity to treat risk clusters rather than individual risks, e.g. (Addison & Vallabh, 2002). These frameworks typically categorize risk based on its source, see e.g. (Huang et al., 2004; McFarlan, 1981; Persson et al., 2009; Ropponen & Lyytinen, 2000). While frameworks such as this can be complementary to checklist approaches, many of the same limitations apply. Risk management process models are also common within the discourse. They usually focus on the risk management process as a whole or specific parts of it, which include risk identification, analysis, evaluation, treatment, and review (ISO31000, 2009). Risk management models usually prescribe a sequence of action, sometimes including the use of specific techniques or tools, for effective risk management (Bannerman, 2008). Non-process frameworks and risk management process models within IS research cover different risk levels: project (Alter & Sherer, 2004; Boehm, 1989, 1991; Charette, 1989; Heemstra & Kusters, 1996), operational (Ahn & Skudlark, 2002; Rainer, Snyder, & Carr, 1991; Smith et al., 2001), and strategic (Arnold, Benford, Hampton, & Sutton, 2010; Clemons & Weber, 1990; Currie & Willcocks, 1998; Vitale, 1986). Both process and non-process approaches are limited. While process models guide action and sequencing, their application still relies on the judgment and skill of the risk managers. Non-process models support analytical thinking about risk but do not help risk managers identify, prioritize or make decisions about how to respond (Bannerman, 2008).

Contingency approaches are designed to offer decision support for risk managers by providing tools for deciding which management method to choose and when to do it (Taylor et al., 2012). When pioneering the

application of this approach in IS, McFarlan (1981) suggested that rigorous assessment of project size, structure and organizational experience with technology, was key in deciding which risk management model to choose. Similarly, Mathiassen, Tuunanen, Saarinen, and Rossi (2007) present a model for mapping risk profiles to risk resolution techniques, while Barki et al. (2001) develop a model that helps relate the level of risk exposure in high-risk projects with organizational levels of user participation, internal integration and planning. Contingency approaches thus combine non-process frameworks with process models by explicating a relationship between risk type configurations and project dimensions associated with performance such as size, cost, and environmental complexity (Taylor et al., 2012). As such, contingency approaches seek to establish a fit between process characteristics and the degree of uncertainty, in order to provide an overall risk profile that help risk managers to make more detailed decisions about how to proceed (Barki et al., 2001; Mathiassen et al., 2007; Taylor et al., 2012).

While these categorizations capture the bulk of research efforts within the discourse on risk in IS, they are not comprehensive. Before going into more detail about contributions falling outside their scope, I will attempt to illustrate how the discourse has developed over time. In the chart below I have mapped out how the discourse has developed in terms of risk level focus. I have made distinctions between the project, operational, and strategic levels. In addition I have included an "other" category that encompasses contributions which, for various reasons, are not captured by these risk levels.
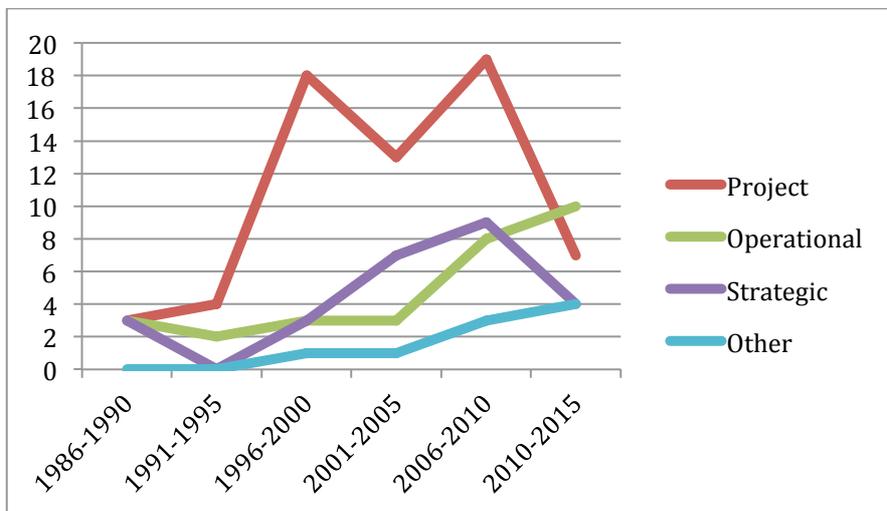
Figure 1. Number of papers published on IS risk research between 1986 and 2015 focusing on four different levels of analysis

The chart roughly illustrates the evolution of the discourse in terms of risk levels. The publications are clustered into five year periods, and clearly show how the project level has dominated research efforts to date. However, there has been a steady increase in risk research at the operational and strategic levels, and in the number of other contributions. While still very much at the heart of the discourse, research on risk related to projects has become significantly less common, both in terms of the actual number of publications, and relative to research focusing on different risk levels. As IT has become an integral part of organizational life, there has been ever more research on risk related to both organizational processes, e.g. business processes (Bai, Krishnan, Padman, & Wang, 2013) or production processes (Rönnbäck, Holmström, & Hanseth, 2007), and strategic issues, e.g. outsourcing decisions (Bahli & Rivard, 2003), IT investment decisions (Benaroch, 2002), and business value (Otim et al., 2012). The "other" category includes research that either ventures beyond organizational use of IT – e.g. by focusing on consumer behavior in e-markets (Verhagen, Meents, & Tan, 2006), or e-services (Featherman, Valacich, & Wells, 2006) –, literature reviews (Bannerman, 2008; Ciborra, 2004; Suriadi et al., 2014), or research that argues for alternative notions and approaches to risk (Carlo et al., 2004; Hanseth & Ciborra, 2007; Hsu, Backhouse, & Silva, 2014; Mumford, 1996).

The chart does not, however, show other changes in the discourse. One notable trend is that research at all risk levels (including "other") has begun to search for new ways of understanding, explaining, and relieving risk because despite extensive and rigorous research on risk management over the past few decades, the failure rate of IT projects remains disappointingly high. Hsu et al. (2014) introduce the work of Giddens to analyze operational risk management. (Scott & Perry, 2009) draw on practice theory to investigate how risk management is enacted. Mitev (2011) explores the relationship between risk and regulation through the notion of paradoxes, and the notion of systemic risk is gaining traction (Carlo et al., 2004; Carlo, Lyytinen, & Boland, 2012; Hu, Zhao, Hua, & Wong, 2012). In addition, an alternative notion, and use, of risk has been introduced into the IS discourse through work on information infrastructure theory (Blechar & Hanseth, 2007; Ciborra et al., 2000; Hanseth et al., 2001; Hanseth et al., 1996). This body of work largely builds on a notion of risk developed by Beck (1992, 1994) and Giddens (1999) in their research on reflexive modernization as a way to characterize and explain the dynamics of contemporary society. I will elaborate on this in the section on information infrastructure risk.

Problematizing the discourse

Analyzed through the categorization offered by Renn (1992), most of the approaches mentioned above are based on technical risk analysis and an economic perspective. Checklists and risk factor research are typical examples of technical risk analysis approaches, and as such are subject to the criticisms raised by other social science discourses (see previous section for details). Within their limited scope, however, they can offer significant support for identifying and managing certain kinds of risk. Non-process frameworks that focus on aggregated risk categories, while potentially useful tools for thinking about risk beyond individual risk factors, can also be regarded as forms of technical risk analysis. There are a number of frameworks which recognize the idea that risk is mediated through social processes and that risks are related to other organizational processes such as IT investment strategies (Benaroch, 2002; Kumar, 2002), business processes (Bai et al., 2013), and business value (Otim et al., 2012). As such, they fit the description of what Renn (1992) calls economic perspectives. These approaches are limited by their focus on individuals as the risk decision makers (and the consequences of individuals' decisions), and their reliance on the rational actor paradigm – i.e. that decision makers are inherently rational agents who will base their decisions on sufficient knowledge. Ciborra (2004) notes that there is a surprising lack of behavioral approaches within the discourse, despite the fact that one of the first influential contributions in the field highlighted the problematic aspects of assuming the rational actor paradigm (March & Shapira, 1987).

Risk management can be understood as a specific form of problem solving that focuses on the identification and mitigation of perceived threats to a desired goal. Schön (1983) argues that instrumental approaches to problem solving (such as risk management) fail to take the problem's setting into account. Although the instrumental approach can offer valuable support in focusing the attention of practitioners on well-understood sources of risk, it cannot provide detailed guidance for specific situations. Furthermore it does not help practitioners identify other relevant aspects of situations as they unfold. This is important because the practitioners involved in problem-solving processes are immersed in ambiguous and complex situations (Pich, Loch, & Meyer, 2002; Sommer & Loch, 2004). While this is the case for project risk management in general, it is arguably even more pertinent when it comes to the organizational consequences of IT, whether within or between projects, operational, or strategic. Indeed, this has been at the core of the IS discourse as a whole; significant effort has been made to recognize, understand, and explain the increasingly complex and uncertain conditions that are part of the everyday make-up of contemporary organizational life (Leonardi, 2012; Orlikowski, 1992; Robey & Boudreau, 1999).

Risk is inherently intertwined with the notions of complexity and uncertainty. Both of these are intimately connected to knowledge (or our lack thereof). Hanseth and Ciborra (2007) argue that our increasingly integrated IT solutions have created a situation with such a high degree of complexity that our current ways of understanding and methods of managing them are insufficient. Their main argument is that increased integration leads to increased complexity and thus to increased risk because our understanding of these integrated systems is partial and bounded. As they put it: "*All this means that the more complex a system is, the more unpredictable the outcomes of our interventions – that is the higher risks for negative outcomes of intervention. So: through integration we increase complexity which again leads to increased risks.*" (Hanseth & Ciborra, 2007, p. 5). As previously noted, risk is a particular form of uncertainty. While not all uncertainty is equivalent to risk, risk is always an uncertainty (as it deals with what might, but has yet to, happen). As argued by Hanseth and Ciborra (2007) above, there is a relationship between complexity and uncertainty when it comes to risk. Mathiassen and Stage (1990) proposed a principle based describing this relationship – the principle of limited reduction – which states that attempts to reduce one will necessarily increase the other. For example, reducing complexity by analytical decomposition of the situation will result in a higher degree of uncertainty. Conversely, reducing uncertainty by performing a heuristic search will result in a higher degree of complexity. The processes by which knowledge is generated in order to manage complexity and uncertainty are different: analytical behavior is needed to reduce complexity whereas experimental behavior analysis is key to reducing uncertainty. In their seminal paper on organizational information requirements, Daft and Lengel (1986) make the distinction between uncertainty and equivocality. While uncertainty relates to a lack of information, equivocality means "*ambiguity, the existence of multiple and conflicting interpretations about an organizational situation*" (Daft & Lengel, 1986) (p.556). In this sense, the degree of equivocality relates directly to the degree of complexity. When equivocality is high, the situation is ill-defined, it is unclear which questions to ask and it is unclear what information is needed to reduce the level of equivocality. Below, I will analyze the discourse on risk within IS by adapting the framework proposed by Daft and Lengel (1986).

	Low — UNCERTAINTY — High	
High EQUIVOCALITY	Ambiguity in risk identification, options for risk resolution strategies are gathered. Contingent risk approaches	Ambiguity in risk identification, options and consequences of risk resolution are unclear. Reflexive, adaptive risk approaches
Low	Well-defined risks and established risk resolution methods. Checklist approaches, Process models	Multiple well-defined risk areas, risk resolution consequences are unclear. Non-process frameworks

Checklist and risk factor approaches build on the notion that, and are effective when, the risk management situation is stable, predictable and unambiguous. These approaches are instrumental in the sense that they build on the assumption that all relevant risks can be both identified at the beginning of a process (e.g. a software development project), and once identified, managed by appropriate risk resolution techniques, tools, or strategies. Non-process, analytical, frameworks offer risk managers support in thinking about risk at an aggregate level. While this helps managers look beyond the generic risk factors in a checklist, they offer scant guidance in how to translate the risk framework to the idiosyncrasies of the specific situation. Contingency approaches focus on offering support in situations where the future and context is dynamic or difficult to foresee. The support is twofold: contingency approaches help risk managers to monitor the situation as it unfolds and reduce equivocality by (i) directing attention towards domains (e.g. project size) that could make it possible to derive alternative definitions of the situation, and (ii) mapping pre-determined risk resolution patterns to these definitions. As such, contingency approaches differ from other process models (or checklists) in the sense that they support initial analysis of the situation and allow risk managers to prepare alternative courses of pre-planned actions.

In situations where both uncertainty and equivocality are high, i.e. when risk managers face conflicting, confusing and complex situations where the

consequences of different courses of actions cannot be reliably evaluated or assessed, extant IS risk research cannot support risk managers in their work. In such situations, risks are *emergent*.

Schön (1983) distinguishes between problem solving based on technical rationality and reflective problem solving during which practitioners continuously reflect in, and on, action. Reflection-in-action can be understood as an ongoing conversation with the situation as it unfolds, as opposed to pre-determined sets of action that are conducted instrumentally regardless of the specifics of the situation. While Schön focus primarily on individual practitioners, Haeckel (1995, 2013) develops a model for adaptive organizing in situations characterized by high uncertainty and high equivocality. In their research on organizational theory, Weick et al. (Weick and Roberts (1993); Weick, Sutcliffe, and Obstfeld (2008) have developed principles for creating sustainability in complex and emergent organizational contexts. Ironically, looking at IS research in general, the understanding and management these kinds of situations with regards to unintended consequences of organizational use of IT has arguably been at the very heart of the discipline for quite some time (Cecez-Kecmanovic et al., 2014; King & Lyytinen, 2006; Orlikowski & Baroudi, 1991; Robey & Boudreau, 1999). Beyond the body of work on information infrastructure risk within the IS discourse on risk, though, there are only a few examples of research efforts that specifically focus on these kinds of situations. Carlo et al. (2004) note how risks in distributed complex socio-technical systems "*increasingly originate from multiple sources, affect multiple agent with divergent perspectives and thus become systemic*" (p.57), and argue that the notion of risk within IS research needs to be re-assessed and researchers need to explain "*how risks emerge and are contained in larger socio-technical networks where the information system becomes embedded*" (p.59). In a recent study Hu et al. (2012) similarly use the concept of systemic risk to develop a network approach to risk management for modeling and analyzing systemic risk in banking systems. They argue that due to the interconnected nature of banking systems, where failure of one bank can cause other banks to fail, risk cannot be understood or treated using our conventional notion of the concept.

Based on this review, I conclude that earlier IS research on risk aimed to provide a rich body of analysis that could be used to deal with IT related risks. Unfortunately, however, it is based on a notion of risk and risk management that will not support risk managers who find themselves in situations characterized by a high degree of uncertainty and equivocality. Similarly, it cannot help us understand and explain why projects continue to fail, managers continue to struggle with managing IT as an organizational

resource, side-effects, unintended consequences, and paradoxes. While the discourse is evolving in a direction that has focused more efforts, both empirical and theoretical, on investigating alternative notions of risk and risk management, we still do not know how IT risk is implicated and managed. This dissertation aims to develop new knowledge of relevance to the problem via the analysis of underlying assumptions – problematization (Alvesson & Sandberg, 2011; Sandberg & Alvesson, 2011). Through a method of "… identifying and challenging assumptions underlying existing literature …" (Alvesson & Sandberg, 2011, p. 247) new and more interesting research questions are likely to be identified, leading to the development of more influential theories. Thus, rather than conducting studies that develop theories by adding "missing pieces" I seek to challenge the bases and assumptions underlying extant research.

Information Infrastructure & risk

Digitalization is changing the foundations of all aspects of organizational life (Brynjolfsson & Saunders, 2010; Tilson et al., 2010; Yoo, Henfridsson, & Lyytinen, 2010). IT is becoming increasingly infrastructural as it ties together systems, actors and functions within and across organizational boundaries, made possible by increased processing power and higher storage and transmission capacities (Hanseth & Lyytinen, 2010). As a consequence, individual systems are no longer isolated and their performance is conditioned by an installed base of related technological and social arrangements (Henfridsson & Bygstad, 2013). Star and Ruhleder (1996) introduced infrastructure as a way of capturing and analyzing the dynamics and consequences of organizational use of IT beyond a focus on stand-alone information systems. Since their seminal paper researchers have continued to build on that notion, and recently the infrastructure discourse has received increased attention (Monteiro, Pollock, & Williams, 2014; Tilson et al., 2010) as a viable alternative for conceptualizing the phenomena under investigation in a way that makes it possible to address the complexities and paradoxes of contemporary organizing. Studies have shown how information infrastructures have become critical components of organizational operations (Light & Wagner, 2006; Wagner, Scott, & Galliers, 2006) despite evidence that organizations struggle to adapt them through software configuration alone (Hanseth & Braa, 1998; Pollock, Williams, & Procter, 2003; Scott & Wagner, 2003).

Bygstad (2010) argues that the notion of information infrastructure, as opposed to the traditional "information system", offers two distinct

advantages. First, it changes the object of study from a single, stand-alone, application within an organization to large scale socio-technical networks of interrelated technical and social entities. Second, it offers a new perspective on how such networks are developed and evolve. Unlike stand-alone systems, information infrastructures are seldom (never) designed from scratch, but grow organically from an existing base of technology, actors and related processes. There are numerous definitions of information infrastructures that vary slightly, however the definition proposed by Hanseth and Lyytinen (2010) encompasses most variations and gives a fair representation of the concept's core characteristics. They define information infrastructure as *"a shared, open (and unbounded), heterogeneous and evolving socio-technical system (which we call installed base) consisting of a set of IT capabilities and their user, operations and design communities"* (p.4). Information infrastructures are shared across multiple communities in unexpected ways, open in the sense that new components can be freely added and integrated and they have no clear boundaries with regards to who may use or contribute to their design. As a consequence, the heterogeneity of the installed base is likely to increase over time as new components are added and unexpected users, designers and communities are connected and disconnected. This heterogeneity is further increased by the fact that individual components may have quite different natures; they can include new technologies, user communities, standardization schemes, and regulations, among other things. As a result of their openness, they evolve organically rather than being deliberately developed, with no apparent goal or clearly defined purpose. This evolution is constrained and enabled by the installed base since any addition must be, or be made, compatible with what is already in place. Or, as put by Monteiro, Pollock, Hanseth, and Williams (2013):

"IIs are characterized by openness to number and types of users (no fixed notion of "user"), interconnections of numerous modules/systems (i.e. multiplicity of purposes, agendas, strategies), dynamically evolving portfolios of (an ecosystem of) systems and shaped by an installed base of existing systems and practices (thus restricting the scope of design, as traditionally conceived). IIs are also typically stretched across space and time: they are shaped and used across many different locales and endure over long periods (decades rather than years)" (p.576)

Beyond varying conceptualizations of information infrastructure, the existing literature on risk and information infrastructures covers a range of empirical settings (e.g. telecoms, government, manufacturing, and health), technologies (e.g. the internet, standards) and levels of analysis (group, organization, industry, and society). Henfridsson and Bygstad (2013) divides

the research into four streams, each with a distinct focus and views on information infrastructures: complexity models, network models, relational models, and strategic asset models. The first three build on interpretative research efforts, while the last one (strategic asset models) has emerged from positivist assumptions regarding strategic alignment issues. *Complexity models* build on the literature on complexity, and focus specifically on infrastructure evolution as the outcome of a process in which autonomous and heterogeneous actors enact their own goals, seeking to use information technology to adapt to their external environment and each other (J. Braa, Hanseth, Heywood, Mohammed, & Shaw, 2007; Ciborra & Failla, 2000). *Network models* build on actor-network theory and consequently view the process of information infrastructure evolution as being driven by networks of multiple human and non-human actors, with the outcome being determined by their combined and ongoing inscriptions and translations (Aanestad & Blegind Jensen, 2011; Hanseth & Monteiro, 1997). Grounded in theories on work practices and learning (Lave & Wenger, 1991) *relational models* highlight evolution as the process by which socio-technical relationships emerge from the IT-mediated activities of a community-of-practice. (Star & Ruhleder, 1996; Vaast & Walsham, 2009), and argue that infrastructures should be understood through the sensemaking of its users. Finally, *strategic asset models* view evolution as the top-down process by which managers implement changes in order to increase the alignment between digital resources and strategic goals (Broadbent, Weill, & St. Clair, 1999; Weill, Subramani, & Broadbent, 2002).

Although issues of risk and risk management have not been the focal point of any of these four streams, they have had significant impact on the development of information infrastructure theory. Adopting a sociological notion of risk based on the work of Beck (1992, 1994, 2000) and Giddens (1999), Hanseth and others (Hanseth & Ciborra, 2007; Hanseth et al., 2001; Hanseth et al., 2006) describe the logic of information infrastructure evolution processes. At the core of Beck's argument is the assumption that the world is becoming increasingly "risky" through the process of reflexive globalization. Change is understood as a consequence of (unintended) side-effects that propagate through multiple layers of a complex system and ultimately reflect back onto what triggered them in the first place – and they do it in a way that counters the goal of the initial action (Beck, Bonss, & Lau, 2003). In this sense, risk is a defining characteristic of information infrastructures. Several studies have shown how technology intended to increase control has had the opposite results because of side-effects (Blechar & Hanseth, 2007; Ciborra et al., 2000; Hanseth et al., 2001). While risk, in this sense, plays an important role in information infrastructure evolution, there are few studies of the specific risks involved, and little emphasis has

been put on investigating information infrastructure risk management practices. In addition, there have been no detailed investigations into how such risks are managed. The notions of risk currently established in the IS discourse capture and explain emergent risk, i.e. risks that cannot be foreseen, due to the unpredictability of situations. Indeed, risk management situations viewed through an information infrastructure theory lens would almost always be characterized by high degrees of equivocality and uncertainty. But while Beck's notion of reflexivity and risk has been instrumental in explaining *why* unintended consequences tend to increasingly occur, it might be less useful as a tool for obtaining detailed empirical evidence and theorizing about *how* they occur.

In conclusion, while extant research on risk is rich and diverse, it fails to account for an increasing number of new risks related to organizational uses of information technology. Many of these risks emerge from situations that are high in both equivocality and uncertainty. Information infrastructure theory can help explain why these kinds of risks are emerging with increasing frequency, but not *how* they emerge. Without knowing the answer to the "how", we cannot find sustainable ways of managing them.

Methodology

This section aims to position the dissertation in relation to the IS field in general and discourses within the field's evolution. It also presents the underlying assumptions of my research process and some important methodological considerations. It begins with a brief historical overview of IS research with a particular focus on the development of IS research in Scandinavia. Second, it discusses and explicates my position regarding the role of theory in research. Third, it presents qualitative research challenges and how I have navigated them. Fourth, it presents an overview of the data collection and analysis processes used in the papers appended to the dissertation.

Research in context

"If you do not know where you come from, then you don't know where you are, and if you don't know where you are, then you don't know where you're going. And if you don't know where you're going, you're probably going wrong." Terry Pratchett

Information systems research

In the introduction to a special issue on historical interpretations of the IS discipline Hirschheim, Saunders, and Straub (2012) ask why it is so difficult for IS researchers to provide a unified answer to the question "What is IS?". This state of affairs is by no means new to our field. In the very first issue of MIS Quarterly (Benbasat & Schroeder, 1977) start their paper by stating *"During the late 1960´s one of the major points of interest in Management Information Systems (MIS) was trying to define what constituted an MIS. There is still not an agreement on the subject."* Below, I will give a brief overview of how and why the different answers to that question have developed in our field, and why we should take comfort in the fact that the question remains.

A number of attempts have been made to capture and describe both the core and the evolution of the IS field (Cooper, 1988; Davis, 2000; Dickson, 1981; Hirschheim et al., 2012; King & Lyytinen, 2006), each with slightly different focus and analyses. As a whole, they paint a picture of IS research as a continuously evolving field rich in institutions, theoretical perspectives, methodological approaches, and diverse philosophical underpinnings. For the purposes of this dissertation, compressing some 50 years of history into a few pages makes it necessary to be very selective. For a more detailed account, see (Hirschheim et al., 2012).

An increased interest in Management Information Systems (MIS) in the 1960's by both practitioners and researchers saw the beginning of what was to become the IS field (Davis, 2000; Hirschheim et al., 2012). In the early years IS research was largely developed by scholars and practitioners in North America and Europe, particularly in Scandinavia and the U.K. During this time many perspectives and schools of thought emerged that have had enduring influence on the field. An overview of IS would not be complete without recognizing the impact of C. West Churman's conceptualization of "inquiring systems" (Churchman, 1971), which focuses on the relationships between methods of investigation and the different kinds of information they produce. Building on Churchman's pioneering work, Checkland developed Soft Systems Methodology (SSM) as a way of addressing failures in systems development by analyzing the relationship between technical and social systems (Checkland, 2000). At around the same time, other scholars such as Mumford (1974) helped to establish the socio-technical systems perspective through which the idea of participative design emerged (Hirschheim et al., 2012). An alternative approach was proposed by Börje Langefors and his distinction between datalogical and infological problems (Langefors, 1966). The notion of infology highlights how information is more than data, and that the recipient's knowledge and experience partly determines how

information is interpreted. Although the notion of infology is all but forgotten today, the ideas put forward by Langefors were instrumental in the development of Scandinavian IS research and its impact on the field.

While European research efforts, e.g. socio-technical systems and Langefors' infological approach, put practitioners front and center, so did the research efforts in North America, which focused primarily on the relationship between decisions, decision makers and the information technology supporting the decisions (Dickson, Senn, & Chervany, 1977). It is also within the North-American tradition that much of the early work on the validity of IS research was done. Put bluntly, this work traces the origins of several ongoing debates concerning issues such as rigor and relevance, quantitative and qualitative research, and positivism and interpretivism. In addition, as noted by Hirschheim et al. (2012), while the different conceptualizations of IS put forward during this time were driving forces of the field's inception, no agreement was ever reached and each conceptualization has subsequently served as the foundation for a multitude of theoretical developments.

Apart from the theoretical streams that shaped the early IS field, it has since the beginning been closely tied to practice and practitioners. As a case in point, contributions to MIS Quarterly were initially (in 1977) separated into two different sections: Applications, and Theory and Research. While these were merged some years later, the split highlights a characteristic of the field that has endured over the 50-odd years of its existence. A majority of the early research contributions focused on either information systems development projects or the organizational use of IT, and ever since it has been common for IS researchers to work closely with industry. The character of this relationship between research and practice has however been shaped by the different schools of thought within IS research. Broadly, the North American tradition has focused on applying scientific (here meaning quantitatively generated) knowledge to the organizational appropriation of information technology, perhaps best exemplified by the extensive discourse on user acceptance (Venkatesh, Morris, Davis, & Davis, 2003). The European tradition, rooted in the work of Langefors and STS, has arguably been even closer to practice in the sense that much attention has been paid to investigating practice (rather than prescribing) in order to create a deep understanding of how things work. In this sense, the European tradition can be characterized as an effort of engaged scholarship (Mathiassen & Nielsen, 2008; Van de Ven, 2007; Van de Ven & Johnson, 2006) enacted through approaches such as action research (Iversen, Mathiassen, & Nielsen, 2004; Lindgren, Henfridsson, & Schultze, 2004) and participatory design (Bødker, Kensing, & Simonsen, 2009; Ehn, 1993). In concert with the field's close relationship with practice and its focus on applying knowledge to

phenomena of importance to practitioners, IS research has been concerned with design, both as an output of research (e.g. design principles for systems development) and as a theoretical or methodological foundation of research efforts, as exemplified by design science (von Alan, March, Park, & Ram, 2004)).

Throughout its history, the IS field has focused much of its efforts around questions regarding the nature of the relationship between IT and organizations - more specifically, the potential of IT to transform organizations (see e.g. Markus & Robey, 1988; Symons & Walsham, 1991). In their review of the IS literature Robey and Boudreau (1999) show how theories built on deterministic logic lead to the paradoxes and contradictory evidence found both within and across studies of the organizational consequences of IT. Instead, they propose the use of theories built on the logic of opposition, i.e. theories that explain organizational change by recognizing forces that simultaneously promote and oppose social change. The use of such theories in IS research has increased appreciably since the publication of their paper. For example, recent publications have employed structuration theory (Orlikowski, 1992; Orlikowski & Robey, 1991; Rose, Jones, & Truex, 2005) actor-network theory (Hanseth, Aanestad, & Berg, 2004; Holmström & Stalder, 2001; Sarker, Sarker, & Sidorova, 2006) theories of organizational learning (Mathiassen & Purao, 2002; Pentland, 1995) and institutional theory (Berente & Yoo, 2012; Kallinikos, 2007). In addition, there has been an expansion in the range of views on casual agency, i.e. the nature and direction of causality, in research on the organizational consequences of IT. Markus and Robey (1988) classify the views of causal agency into three distinct categories; the technological imperative, the organizational imperative, and the emergent perspective. While all three views are represented in contemporary research, the emergent perspective has gained significant ground over the last few decades. The most significant theoretical recent developments within IS research concerning the organizational consequences of IT have built on the emergent perspective, including the adoption of structuration theory (Orlikowski, 1992), ANT (Walsham, 1997), sociomateriality (Leonardi, Nardi, & Kallinikos, 2012), and practice theory (Feldman & Orlikowski, 2011) to name but a few. The rivalry between different theoretical approaches has indeed been an important driving force in the evolution of the IS discipline. In this context I agree with Walsham (2005), who wrote:

"I believe that there are many theories, of which I have mentioned only a few, which are relevant to the study of human and machine agency in the context of research on GIS projects in India. I don't think they can, or should, be 'integrated,' if what is meant by this is bringing them together in

one grand theory of agency. I think, however, that we can use different theories, including structuration theory and actor network theory, to illuminate different issues, and to theorize different elements of the overall research topic. So, I am more in the 'thousand flowers' camp. However, in case this is taken to mean that I think 'anything goes' in the way of theory, I do not. Researchers must show how and why they think their theory is relevant, and they must convince readers and reviewers that their theory adds something new." (Walsham, 2005, p. 156)

Put more simply, there is no "best theory", and every researcher must show how and why a given theory is relevant to a particular research project. Since its inception, the IS field has established itself as a diverse and pluralistic academic field (Hirschheim et al., 2012; King & Lyytinen, 2006) with multiple specialties and communities, journals and conferences, theories and methodologies, assumptions and perspectives. Today, IS research encompasses a wide variety of areas, including (but not limited to) the analysis and development of information systems (Avison, Dwivedi, Fitzgerald, & Powell, 2008; Hirschheim, Klein, & Lyytinen, 1996; Rockart, 1978; Wand & Weber, 2002); the adoption and use of information systems (Benbasat & Barki, 2007; Burton-Jones & Gallivan, 2007; Markus & Silver, 2008; Yoo, 2010); management of the organizational use of IS and technical capabilities (Galliers & Sutherland, 1991; Markus, 1983; Melville, Kraemer, & Gurbaxani, 2004; Sambamurthy et al., 2003; Wagner et al., 2006); communication, decision-making, knowledge management, and innovation (Alavi & Leidner, 2001; Shim et al., 2002; Wasko & Faraj, 2005; Yoo et al., 2010); and IS in society and a global context (Hsieh, Rai, & Keil, 2008; Kling, 2000; Lacity, Khan, & Willcocks, 2009; Walsham, 2002). Beyond these established areas, there are a number of emerging topics and ongoing controversies, the most pervasive of which is perhaps that concerning the field's legitimacy.

Legitimacy is a core issue for any field as it is directly related to whether the discipline serves any justifiable purpose or not. As such, questions of legitimacy should not be taken lightly. These kinds of questions are common in disciplines as they become established, and so are not unique to IS research; similar discourses have played out within fields including sociology (Mazlish, 1989) and management research (Engwall, 1995). There are different kinds of legitimacy, and at an early stage in the evolution of IS research, serious questions were raised about whether the field could generate computer-based systems of sufficiently high quality to be used by managers (Ackoff, 1967). In general, however, questions of legitimacy have concerned the relationships between IS research and other fields, i.e. academic legitimacy. Much of the discourse is centered on the issue of a

(perceived need for a) theoretical core in IS research (Baskerville & Myers, 2002; Benbasat & Zmud, 2003) and ways of establishing and theorizing a core object of study (Orlikowski & Iacono, 2001; Weber, 2003). While there is widespread agreement that diversity and plurality are defining characteristics of the IS field (Alavi, Carlson, & Brooke, 1989; Banville & Landry, 1989; Benbasat & Zmud, 2003; Iivari & Lyytinen, 1999; King & Lyytinen, 2006; Klein & Hirschheim, 2008; Orlikowski & Baroudi, 1991; Weber, 2003), there are many widely divergent opinions on what this implies. There are two main positions within the discourse: (1) diversity and plurality are destructive and should be overcome by reaching agreement on a unified theoretical core (see e.g. Benbasat & Weber, 1996); and (2) diversity and plurality are unavoidable and promising (Robey, 1996). Lyytinen and King (2004b) argue that the question of legitimacy cannot be resolved by adopting a consensual theoretical core and that legitimacy must instead be achieved by ensuring that (1) our research efforts are salient; (2) the results of IS research are robust; and (3) the field retains its plasticity, i.e. its ability to adapt to changing circumstances.

Against the backdrop of this broad, albeit brief, overview of IS research history it seems clear to me that although diverse and pluralistic, the discourse is not fragmented. There are distinct clusters of assumptions that have developed over time and manifest themselves in the different perspectives, theories and methodological choices that have been put forward and adopted at different times in the discourse. I also believe that the analysis and arguments put forward by Lyytinen and King (2004b) are convincing, essentially correct, and fit very well with IS research as an applied and pragmatic field. We absolutely do not need a unified theoretical core or a fixed object of study. What we do need, though (perhaps contrary to Lyytinen and King (2004)), are these kinds of discourses. They are necessary in research fields because they allow us to be reflexive about where we are and where we are (potentially) going. In a sense, research fields without these kinds of meta-discussions are either stagnant or without purpose. These discourses, then, can be understood as instrumental in the ongoing sensemaking (Weick, Sutcliffe, & Obstfeld, 2005) of our field.

IS in Scandinavia: local enactment and global ties

Much like the IS field in general, IS research in Scandinavia is characterized by diversity and pluralism in terms of theory, methodologies and perspectives (Dahlbom, 1995; Iivari & Lyytinen, 1999). The impact of Börje Langefors (see Dahlbom and Langefors (1995) for more detail) has, of course, been immense – especially in the early years. Together with Kristen Nygaard he shaped the contours of IS research in Scandinavia for years to come (Iivari & Lyytinen, 1999). Langefors' pioneering work on systems

development, influence in the establishment of IS as a field, and the creation of initial research infrastructures (e.g. IFIP TC8) helped to establish IS research communities in all of the Scandinavian countries, and was also one of the reasons for the disproportionate significance of Scandinavian research on the evolution of IS as a whole (Iivari & Lyytinen, 1999). Nygaard brought a socio-political dimension to research in general, and systems development in particular, by initiating a close collaboration with relevant trade unions (Nygaard & Terje Bergo, 1975). Since Langefors and Nygaard, Scandinavian research has been characterized by a preoccupation with the area of systems development, a close relationship with practitioners, and a particular sensitivity towards related socio-political issues. Following Langefors, there has also been a strong orientation towards conceptualization and philosophy in terms of considerations of fundamental aspects of IS, both in terms of practice and research (Croon Fors, 2006; Dahlbom & Mathiassen, 1993; Ehn, 1988; Ivanov, 2001; Janlert & Stolterman, 1997; Lyytinen & Hirschheim, 1988; Mathiassen & Stage, 1990) throughout Scandinavian IS research.

Several overviews and analyses of Scandinavian IS research have been presented (Bansler, 1989; Bjerknes & Bratteteig, 1995; Iivari & Lyytinen, 1999; Mathiassen & Nielsen, 2008), showing how systems development issues have, historically, been at the forefront of research efforts. Within this area, several themes have emerged and developed. Rooted in the trade union research projects, there has been a strong focus on users of information systems – in particular on user participation (See Bjerknes & Bratteteig for an extensive overview). This body of work introduced a notion of design that has had lasting impact on the trajectory of research (e.g. Ehn, 1998; Stolterman, 1991). Another discourse developed from the focus on systems development has highlighted the political aspects of information technology usage, both within the workplace and on a societal level (see e.g. Klang, 2006).

Reflective of the idea of usefulness and salience, there is also a strong orientation towards pragmatism within Scandinavian IS research. IS researchers in Denmark introduced action research as a way of generating usefulness for both researchers and practitioners (Avison, Lau, Myers, & Nielsen, 1999). Göran Goldkuhl and the Linköping-based VITS network is another example of efforts made to generate useful research results (Goldkuhl, 2004). Similarly, IS research in Göteborg, heavily influenced by Bo Dahlbom (Dahlbom, 1995), has developed close relationships with regional industry through e.g. the Viktoria Institute (K. Braa, Sørensen, & Dahlbom, 2000; Ciborra, 2000; Ljungberg) and IS research in Umeå has been developed through close relationships with regional industry, in

particular the process industry (Arvidsson, Holmström, & Lyytinen, 2014; Jonsson et al., 2009; Levén, Holmström, & Mathiassen, 2014; Westergren & Holmström, 2012)

During the last decade, research has focused less on users and systems development projects and more on the challenges presented by the increased digitalization of "everything". Recent dissertations have highlighted the need to reconsider old truths (Nylén, 2015; Westergren, 2011) and illustrate how Scandinavian IS research has adapted to changing circumstances. However, challenging established notions and theories is nothing new, but rather a continuation of a long and successful Scandinavian IS research tradition. It is only through our close relationship with practice we can detect, trace and explore changes, and it is through our firm philosophical roots that we are able to recognize and understand them. Scandinavian IS research is arguably stronger than ever. Although no single individual can rival the individual impact of Langefors on IS research, a quick look at the editorial boards of all major IS journals reveal that Scandinavia is well represented on today's global IS scene.

The role of theory in IS research

Tightly connected to the issue of research contribution is the question of theory. In a recent debate paper, Avison and Malaurent (2014) question the emphasis on theory in IS research and present six inter-related concerns regarding the consequences of a focus on theory as the way to contribute to research. In short, they argue that the current norms with regards to the role of theory hinder the acceptance of novel and exciting research, and instead tempt researchers to tell the story of the theory rather than the phenomenon, distort understanding of the research setting, make un-ethical decisions with regards to data selection, directly apply theories from other disciplines without adapting them to the specifics of IS, miss out on opportunities to make novel contributions, and make research trivial rather than interesting. They propose, instead, that IS research should open itself up to "theory-light" papers in which "theory plays no significant part in the paper and the contribution lies elsewhere". A set of guidelines for writing such papers has been drawn up.

In her response, Gregor (2014) shows how their concerns have little to do with the role of theory and instead relate to our journal norms and their failure to recognize the practical aspects of theorizing– i.e. how theory is developed. In addition, she points out that theory plays different roles in research and that there are different views of what it is, and argues that *"Developing theory is what we are meant to do as academic researchers*

and [what] sets us apart from practitioners and consultants". Henfridsson (2014) points out the importance of theory in creating compelling stories to inform, explain and inspire action. He also observes that research is cumulative by nature, and that qualitative research become generalizable through the ties between a particular narrative or phenomenon and the cumulative tradition (i.e. theory). Lee (2014), in his response, notes that it is impossible to separate the question of what theory is from the question of what science is. Indeed, both Gregor (2014) and Henfridsson (2014) refer to the work of Weick (1995) to elaborate on the process of theorizing as a key research activity and a driving force of new knowledge.

This is, of course, not a new topic of debate within research communities. In a similar debate in the field of Organizational studies 20 years ago, Weick (1995) observed that theories are almost always approximations, and that we should not confuse the process with the product.

"The process of theorizing consists of activities like abstracting, generalizing, relating, selecting, explaining, synthesizing, and idealizing. These ongoing activities intermittently spin out reference lists, data, lists of variables, diagrams, and lists of hypotheses. Those emergent products summarize progress, give direction, and serve as placemarkers. They have vestiges of theory but are not themselves theory. Then again, few things are full-fledged theories. The key lies in the context – what came before, what comes next?"

Another way of putting it would be to say that theories are enacted through the process of theorizing, and the products of our theorizing efforts are snapshots of the process and not theory in itself. They must, however, be grounded in an ongoing theorizing discourse to be useful. This view of theorizing and theory is reflected in the arguments made by Gregor (2014); Henfridsson (2014) and Lee (2014) in response to Avison and Malaurent (2014).

My position reflects that of Weick (1995), Gregor (2014), Henfridsson (2014) and Lee (2014). Research is cumulative and, to be research, must be grounded in a specific research discourse. I regard these discourses as collective theorizing processes, where we collectively move the field forwards through our contributions or "interim struggles" (Weick, 1995), whereby we build on what came before and identify new directions and opportunities. As such, I view the contributions made in the five papers of this dissertation as snapshots of different aspects of my overall objective of theorizing information infrastructure risk management practices. Each paper builds on

and contributes to existing IS discourses on risk and information infrastructure.

Methodological assumptions and considerations

Research assumptions

Research is mostly about practicing science rather than philosophizing about it (unless, of course, you happen to be a philosopher of science). Still, all forms of research build on specific (implicit or not) assumptions about the nature of the world we are investigating and how we can go about investigating it, i.e. ontological and epistemological assumptions. While these are not usually discussed explicitly in our research efforts, they are at the core of what we do. Van de Ven (2007) observes that "*Whether explicit or implicit, we rely on a philosophy of science to interpret the meanings, logical relations, and consequences of our observational and theoretical statements*". Below, I attempt to explicate and contextualize my assumptions to justify the choices I made in terms of both ontology (the nature of what I study) and epistemology (how I have studied it).

The notion of risk is very much at the heart of this dissertation, and therefore any methodological or theoretical considerations and choices are intimately tied to whatever ontological and epistemological assumptions I associate it with. As evident from chapter 2 there is no commonly accepted definition of the term. However, on a fundamental level I align myself with the definition proposed by Renn (1998a), which states that any notion of risk concerns *the distinction between reality and possibility*. This seemingly simple statement becomes more complex when we translate the individual constructs to the context of information infrastructure risk and how to study it.

First, there is the notion of reality and what that is – something that philosophers have debated for as long as philosophy has existed. Given the content and focus of this dissertation, certain aspects of reality stand out as more important than others, e.g. technology, causality, agency, organizations and change. My ontological position in terms of these notions is manifested by the choice of information infrastructure theory as a perspective throughout the different studies in the dissertation. The discourse on information infrastructure, as illustrated in chapter 2, is diverse, and researchers within it adhere to different philosophies of science, ranging from critical realism, pragmatism, and critical realism (see e.g. Van de Ven, 2007 for an overview). What is important, though, is the commonality of ontological properties within the discourse – i.e. what "things" are

considered essential, how they are framed, and how are they related. Information infrastructure theory includes both social and technological entities, highlights the infrastructural character of technology, recognizes both human and non-human agency, and adopts an emergent perspective on change processes. Walsham (2006) argues that the choice of theory is essentially subjective, and that we choose theories that we feel are insightful to us. My choice of information infrastructure is very much based on just that. It is not, however, random. It reflects my ontological position, manifested in a particular way through the constructs of the theory. There are other theories that build on very similar ontological assumptions – e.g. platform theory, which would have yielded similar (but different) research results and would be compatible (albeit in slightly different ways) with the other concepts, frameworks, and perspectives I've used in theorizing risk. In short, in this thesis I adopt information infrastructure theory as a perspective that reflects my ontological assumptions about technology, causality, agency and change.

Second, there is the notion of possibility. This concept is complex in a different way to that of reality. It includes both what might actually happen, and also what we believe might happen. The distinction is important in several ways: (1) it separates "reality" from our interpretations of it; (2) it stresses the notion of knowledge, which is important because our interpretations of what might happen are based on our knowledge (tacit or explicit) and assumptions about the world; (3) it highlights our ability to be imaginative based on what we know; (4) it makes our values and goals important, as they will guide whatever decisions are made on the basis of our predictions about what might happen; and (5) it makes risk fundamentally related to the perspective of the risk identifier. Understood like this, risk becomes highly pragmatic because it is rooted in the knowledge, goals, and values of specific actors and connected to our actions and decisions about future action. Drawing on the discourse on knowledge, I position myself in line with e.g. Lave and Wenger (1991) and Brown and Duguid (1991) and understand knowledge to be local, social, situated and closely linked to practice. The relationship between knowledge and practice is important in this dissertation. In addition, I agree with authors such as Hawthorne and Stanley (2008), who argue that the rationality of our action is based on our knowledge, i.e. we do what we think is best at the time (to the best of our knowledge). As such, even seemingly irrational, counterproductive, or paradoxical actions can be understood as rational behavior if we uncover the knowledge that shaped them. Much of the literature on normative decision theory instead builds on rational action theory, where the idea is that action is a matter of maximizing expected utility based on subjective belief rather than knowledge (Hawthorne & Stanley, 2008).

Third, it begs the question of how it can be investigated. My answer to that is largely based on the assumptions outlined above, and the theoretical choices I have made in accordance with them. While my assumptions as materialized through the theoretical constructs impose certain limitations on what might be considered feasible in terms of research methodology, they still leave a vast number of viable options open. Information infrastructure theory implies a need to generate rich datasets as it includes investigation of both social and technical aspects, as well as the idiosyncrasies of the installed base. My position on knowledge and action also makes it necessary to focus on stakeholders, action, and knowledge (both tacit and explicit) related to the specifics of practices. As I frame IT related risk as a particular instantiation of IT-implicated organizational consequences, time has also a been relevant factor in making methodological decisions. In order to manage these implications I have opted for practice theory as the foundation for my empirical approach.

Practice approaches have become established within management and organization studies (Newell, Robertson, Scarbrough, & Swan, 2009), and have become increasingly common in IS research (Feldman & Orlikowski, 2011; Leonardi & Barley, 2010; Orlikowski, 2000, 2007). They are particularly useful in addressing knowledge-related work (Cetina, 2009) and offer powerful analytical tools to investigate organizational dynamics and complexities (Feldman & Orlikowski, 2011). As with most theories, there are a number of different manifestations and interpretations. Feldman and Orlikowski (2011), in their overview of practice theory, describe it as an umbrella term for theories investigating *"specific instances of situated action and the social world in which the action takes place"*. They categorize the positioning of a practice lens as either empirical, theoretical, or philosophical (Feldman & Orlikowski, 2011). Practice theory reflects the assumptions previously described, highlighting a pragmatic view of knowledge as embodied in the everyday activities of social life, and thus inextricably tied to practice. In this dissertation I use practice theory as an empirical approach to investigate *what,* and a theoretical approach to investigate *how,* information infrastructure risk is implicated.

Qualitative research, interpretative case studies and generalizability

Broadly, research approaches can be described as either quantitative or qualitative. While quantitative approaches, rooted in natural sciences and positivist traditions, strive to generate knowledge through the measurement

of variables or testing pre-specified hypotheses (Kaplan & Duchon, 1988), qualitative approaches are grounded in an interpretative (or critical) philosophical tradition that is concerned with how the social world is interpreted, understood, constituted or produced. Qualitative approaches are based on data generation methods that are both flexible and sensitive to the context within which data is produced, and based on methods of analysis which involve understanding of complexity, detail and context (Mason, 2002). Given the discussion of the underpinning assumptions of this dissertation, it should not come as a surprise that my general research approach is qualitative rather than quantitative. Importantly, this is not to imply that quantitative research approaches and designs are useless in the investigation of information infrastructure risk, only that given my ontological and epistemological assumptions, qualitative approaches are a better fit.

Specifically, this dissertation is based on qualitative case studies. There are other examples of qualitative studies, such as ethnography and action research (Myers, 1997). Case studies, it should be noted, can be positivist, interpretative or critical in nature (Myers, 1997; Walsham, 2006) all depending on the underlying philosophical assumptions. Yin (2013), widely cited by interpretative researchers, assumes a positivist stance, as do Benbasat, Goldstein, and Mead (1987) in their suggestions for how case study research should be conducted within IS research.

Case studies have been used extensively within IS research for quite some time (Benbasat et al., 1987), having originally been adopted by positivist researchers (Walsham, 1995). As interpretative approaches gained momentum there was a need to develop research criteria for case studies based on interpretative assumptions (Klein & Myers, 1999), as these differ significantly from the established positivist criteria (Benbasat et al., 1987). The most well-known and cited work on criteria for interpretative case studies is that of Klein and Myers (1999), who propose seven principles for conducting and evaluating interpretative field studies:

The fundamental principle of the hermeneutic circle – This is a meta-principle for all interpretative research work, and the other six principles can be understood as specific instantiations of it. It highlights the reciprocal relationship between the whole and its parts, which implies that in order to understand (something) we must shift between looking at the whole and looking at its parts; our understanding of the one affects our understanding of the other. Since our understanding of the whole and its parts change in each iteration of the analytical process, it is sometimes referred to as the hermeneutic spiral (Paterson & Higgs, 2005). In this dissertation, the best

example of the hermeneutic circle can be found in paper no 4, where my co-workers and I had a very rich and complex data set to analyze. When we looked at certain parts of the data, it changed the way we understood the whole, and when our notion of the whole changed we went back to re-analyze data we had previously considered. The first process characterization we constructed changed significantly over the course of the study.

The principle of contextualization – This principle highlights the relationship between the researcher, the text, and the audience. It shows how interpretations of a text can and will differ (c.f. Langefors' infological equation) over time and with different readers. Therefore it is important to provide sufficient social and historical context in interpretative research, bearing in mind what aspects of the context are most important to tell the story the researcher wants to tell. All of the papers in this dissertation (barring perhaps paper 5) place considerable emphasis on their contextualization. This was challenging because the formatting of papers (for journals and conferences) does not always cater to rich contextual descriptions, so tough choices have been made. These choices were guided by the specific analytical framework adopted in each paper and the story I wanted to tell (which always includes more contextualization than would be needed just to fit into the chosen analytical framework).

The principle of interaction between researchers and the subjects – This highlights how both researchers and the participants they study should be understood as interpreters and analysts. In short, facts are generated as part of the social interaction between researchers and the participants, and may change the way participants interpret their situation – causing changes in how they think (and act). It also emphasizes that a story always is told through the filter of the researcher's preconceptions, ideas and values. This is sometimes referred to as double hermeneutics (Giddens, 1984), where we report our interpretations of others' interpretations (as we understand them). In the paper mill case study presented in this dissertation, we used this principle to help the organization to find new ways of managing its risks. We did this through a workshop attended by all of the key participants in which they were presented with our feedback and were able to use this feedback to explore new ways of dealing with the challenges that our research had helped to clarify and make explicit.

The principle of abstraction and generalization – This principle deals with ways for interpretative researchers to create knowledge that goes beyond purely descriptive reports of unique situations. Instead of relying on claims of causality and natural laws, interpretative researchers generalize through different processes of theorizing. Generalization is crucial for research

efforts, as noted by Mintzberg (2005, p. 361) *"If there is no generalizing beyond the data, no theory. No theory, no insight. And if no insight, why do research?"* Below, I go into more detail on the positions and ways of generalizing from case studies.

The principle of dialogical reasoning – The preconceptions interpretative researchers have at the start of a project will, inevitably, guide the first steps of the research process. However, it is important for researchers to be both conscious and reflexive about their own preconceptions, as they might not be sufficient (or relevant) at later stages (e.g. if the findings do not support the preconceptions). Throughout my work on this dissertation, I have had to kill more than a few darlings. Most of my initial ideas and early understandings of a context through a particular concept or perspective have proven either wrong or inadequate to make a research contribution, and have therefore been replaced by others (often more than once) throughout the research process. In addition to discussions with co-authors and colleagues, the feedback from reviewers and research conference participants has been instrumental in the development of my research efforts.

The principle of multiple interpretations – This principle recognizes that any event, action or process can be viewed and understood differently by different actors. Conflicts and other contextual factors such as the role of politics and power are likely to be interpreted in different ways depending on the role, goals, and knowledge of the participants involved. It is therefore important to include multiple participants related to the context under investigation. A clear example of this from the research reported in this dissertation is the paper mill case, where we investigated risks related to the production process. We included as many different roles as possible in our selection of participants in order to multiple viewpoints and interpretations of the production process risk. The findings show how the interpretations, goals and knowledge differed quite a lot and as a result my own preconceptions were altered.

The principle of suspicion – This principle builds on observations from critical theory that emphasize the risk of conscious or unconscious distortion of narratives, i.e. what we say can be colored by what we want to achieve (e.g. certain actions or changes) and therefore obscure alternative explanations.

While these principles have become established as a standard for conducting and evaluating interpretative case studies, both Walsham (2006) and Klein and Myers (1999) have noted that simply adhering to these principles does not guarantee interesting or relevant research contributions. Of particular importance when seeking to generate relevant results from interpretative

case studies is the principle of abstraction and generalization. Unless qualitative, interpretative research can be generalized, its contribution will be limited to the telling of interesting, rich stories. Indeed, this has been one of the most prevalent criticisms aimed at case study research (Benbasat et al., 1987; Tsang, 2014). In response, proponents of qualitative research have explicated different ways of generalizing from interpretative case studies (Eisenhardt, 1989; Myers, 1997; Tsang, 2014; Walsham, 1995).

Generalizations can be either empirical or theoretical (Tsang, 2013). Empirical generalizations, e.g. statistical, are made by inferring characteristics from a sample to a population. These kinds of generalizations are common in quantitative research approaches, and have unfortunately become the typical way we think about generalization. In contrast, qualitative (whether it be positivist, interpretivist, or critical) research builds on theoretical generalization when developing explanations of the particular. Walsham (1995) identifies four types of theoretical generalizations in interpretative case studies: (1) development of concepts; (2) generation of theory; (3) drawing of specific implications; and (4) contribution of rich insights. These four are not mutually exclusive and as such, multiple types of generalizations can be made in the same research effort.

In this dissertation I generalize, theoretically, in different ways. For example, I develop the concept of "interstitiality" to theorize how risks are implicated in information infrastructure evolution, and the concept of the "risk dilemma" in paper number 2. In the same paper I propose a framework of risk based on a practice approach in contrast to an instrumental one. In paper 1 I provide rich insight into the challenges of IT adaptation in the process industry, and in paper 5 I draw specific implications for information infrastructure risk management.

Research context and data collection

The papers reported in this dissertation are based on three different case studies. This section briefly describes the contexts of each case study and the associated data collection procedures. More detailed descriptions can be found in the corresponding papers.

The first case study (reported in paper 1) differs somewhat from the other two because it was conducted before I had articulated practice as an epistemological lens or chosen to focus on risk. Instead, the research design was exploratory rather than specifically oriented towards practice, and came from my interest in information infrastructure theory as a tool for

conceptualizing organizational change and the use of technology. The subsequent focus on risk was very much an outcome of this first case study its analysis. The study focused on IT adaptation challenges in a process industry setting, and a total of 8 interviews were conducted with representatives from both a paper mill and their main IT-vendor. The choice of a process industry setting was opportunistic rather than intentional, but became important for the rest of my dissertation because I was both fascinated and intrigued by the integration of mechanical technology with IT. The study also radically altered my preconceptions of how contemporary process industries work.

The first paper highlighted a number of interesting issues that process industry organizations need to deal with, one of which was new kinds of risk. This interested me and became the focus of my next study. With the help of my supervisor and the IT manager of a large paper mill, I designed a study of IT-related risks in the process management of the plant. In addition to generating research results, the case study aimed specifically to help the paper mill find ways of addressing the new risks they could identify but not yet fully manage. For these purposes we included a representative of their IT-vendor and an external senior risk management consultant in the study, both of whom were interviewed and later took part in a workshop with the key actors from the paper mill. The workshop confirmed the relevance of the research results and also impacted the relationship between the paper mill and their IT-vendor, as they re-negotiated the boundaries of their relationship and their responsibilities in order to better be able to cope with the newly identified risks. This case study is presented in papers 2 and 3, and used as an illustration in paper 5.

While the first and second case studies were carried out in industrial settings, the third was set in a significantly different context. The second author on the fourth paper was an industrial Ph.D.-student who spent the majority of his time working as a senior project manager in a global IT consultancy firm. At the time of the case study, his team had successfully developed and supplied infrastructural solutions to internal and external customers for over a decade. I was interested in investigating what kinds of risks they had identified and encountered during these years, and how they had managed them (or not). The data generated in this case study covers 10 years of information infrastructure supplier practices, and includes records of workshops, interviews, and documentation (e-mails, proposals, presentations, agreements, etc.). The analysis of the data was conducted by myself and the insider researcher, and during the analysis the insider researcher supplied additional information as we delved into deeper layers of practice.

Data analysis

Previous sections have addressed a number of issues related to data analysis, e.g. the role of theory and generalization, and the individual papers will give the details of the data analysis conducted for each paper. Here I aim to present and discuss the choices of theories and perspectives I have made in my efforts to theorize information infrastructure risk practices.

This dissertation began with my interest in information infrastructure theory, and in the first paper it serves as a theoretical lens for exploring IT-adaptation challenges. The description of the paper mill contexts is based on information infrastructure constructs. In second paper, it is used in two different ways. As a perspective, in the sense that it helped frame the contours of the context, and as an example of a theory that had introduced an alternative notion of risk into the IS field. Drawing on this notion, we argue for the need to investigate risk in new ways. As an analytical framework, however, we chose concepts from the organizational learning discourse – more specifically Schön's (1983) notion of governing variables and action strategies – and practice theory. Combining different concepts or theories is never straight forward, and our framework would have been much more difficult to construct had not Schön's (1983) constructs been reflective of practice theory (in that they share common epistemological assumptions).

The third paper analyzes the same data as the second paper, but with a different analytical lens. It elaborates on the practice approach and focus more specifically on the different epistemic strategies employed by the practitioners in their risk management approaches. We theorized the risk management practices by drawing on the growing literature on sociomateriality and, as a result, we could show how and why the different strategies emerged.

In the fourth paper, we investigate the evolution of information infrastructure in a longitudinal case study. Whereas the main contributions from papers 2 and 3 had been towards the discourse on risk in the IS field, here the main contribution is towards information infrastructure theory. Practice theory informed the paper empirically, and is also part of the paper's analytical framework. In addition, we adopt a notion of reflexivity that differs from that used in the extant literature on information infrastructure theory in order to analyze *how* risk was implicated in information infrastructure evolution. We theorize risk emergence as a result

of interstititality, i.e. risks emerge between established structures as a result of a dialectical interplay between organizational structures (including technology) and practice.

Unlike the dissertation's first four papers, the final paper focuses specifically on how information infrastructure risk can be managed. Here, I adopt theoretical constructs from the literature on High-reliability organizations (HRO) (see e.g. Weick, 2008) to develop a model for how information infrastructure risk can be sustainably managed. The rationale being that information infrastructure risks are increasingly systemic and emergent, and HRO focus specifically on organizations that have proven to be resilient under such circumstances.

The choices of theoretical framing in the different paper projects might seem haphazard or random. While I agree that there is a large degree of eclecticism in the choices, I argue that it is a result of an informed eclecticism (Barker, Nancarrow, & Spackman, 2001). My choices have been informed by the empirical material as well as my ontological and epistemological assumptions. Within those boundaries there are, of course, many potential alternatives and I the choices I have made have been the theories that made most sense to me at the time. Along the way, I have used theories that did not end up in the finished version of a paper because they could not help me theorize, or were not a good fit for the content of the empirical material. These have still been influential in the way I have interpreted the cases. While these theories never are disclosed in our papers they often helped shape my understanding and pointed towards what kind of theory or constructs I needed in order to make a useful contribution.

Summary of papers

This section summarizes the five individual papers in the dissertation.

Paper 1

Rönnbäck, L., Holmström, J. & Hanseth, O. (2007) "*IT-adaptation challenges in the process industry: an exploratory case study*" Industrial Management & Data Systems, Vol. 107, No. 9, pp. 1276-1289

This paper builds on the idea that large-scale IT infrastructures deployed in an organizational setting should be characterized as "infrastructures" rather than "tools" because their deployment is often constrained by an installed

base. The purpose of the paper is to identify and explore critical challenges for the process industry in IT infrastructure integration and adaptation. As an example of a process industry, the study presented in this paper is focused on IT integration in an organization in the paper and pulp industry. It builds on a growing literature on information infrastructures, and in particular the picture painted in this literature of IT infrastructure as stable rather than flexible, as they have been recognized as hard to change due to the inertia of the installed base. The study's results highlighted the need to further elaborate upon our chosen theoretical framework. The concepts of stability and fragility of the installed base in particular are identified as areas in need of further elaboration. Another is the concept of risk and risk management. Our proposed shift from the system to infrastructure as the core object of study clearly lends a different perspective on risk and risk management. The challenges we identify in this study can undoubtedly be regarded as serious risks for process industry organizations. IT infrastructures that contradict deep-seated local professional identities because of the assumptions articulated by or inscribed in the infrastructure instill feelings of "meaninglessness" and "existential anxiety" among the users. This underscores a critical problem associated with IT infrastructure projects – the need to balance the local with the global in a way that empowers local staff rather than disempowering them. For the process industry, attempts to increase control over production processes by adopting more sophisticated technologies can create such side effects if the process operators feel disempowered by new technology.

Paper 2

Öbrand, L., Holmström, J. & Mathiassen, L. "*Between a rock and a hard place: facing dilemmas in IT risk management*" Currently under review (first round) at an international journal

This paper presents a case study on IT-related risk in the process management at a paper mill. A comprehensive review of the literature on risk in IS research is reveals a bias towards an instrumental approach to risk management. Risk management is in this view a rational problem solving activity, where risks, once identified, can be successfully mitigated. As such, multiple, or conflicting, ends cannot be accounted for, nor situations where rational acts by risk managers increase risks rather than mitigate them. The expansion and increased integration of systems, within e.g. the paper and pulp industry, creates complex socio-technical infrastructures in which new risks may emerge, and new ways of risk management may be needed. Although the current literature strives to provide rich analyses for how to deal with IT risks, it fails to explain why it is increasingly difficult to manage

risk. The paper argues for an information infrastructure perspective and proposes a practice approach to risk as an alternative to an instrumental one. The paper focuses on learning issues, an important and overlooked area of inquiry in IT risk management research. A key concern is how organizational actors associated with successes and failures in IT risk management learn from their actions, and whether these learning processes reinforce or transform existing practices. Adopting concepts from Argyris and Schön it focuses on risk strategies as they play out in the context of the day-to-day management of organizational processes. The paper contributes to IT risk management theory by moving beyond the instrumental notion of risk and introducing an alternative, practice-based, approach to risk management. It also contributes by developing the notion of a risk dilemma.

Paper 3

Öbrand, L., Holmström, J. & Newman, M. "*Recalcitrant technologies and unfolding ontologies: exploring epistemic strategies in IT risk management*" Currently under review (first round) at an international journal

This paper is based on the same case study as paper 2, but with a particular focus on the character of the risk management processes enacted at the paper mill. It approaches the study of IT risk management in a process industry plant from a performative perspective building on the assumption that risks are socially constructed and sociomaterial by nature, and the proposition that risks are emergent over time. As the growing literature on sociomateriality notes, it is the character of IT that makes sociomaterial change difficult to foresee and manage. Indeed, there are many "unknown unknowns" associated with sociomaterial change, something which is rarely considered in extant risk management literature. There is therefore a need to empirically investigate how the social and material implicate or differ from one another, and how digital technologies impact the social, the technical and the material. This paper addresses the issue of IT-triggered risk by exploring the risk management practices in a process industry setting, where traditional, mechanical technology has been replaced by digital technologies. The risk management strategies employed in the factory are characterized as reactive, proactive and adaptive to denote the different epistemic strategies employed by the practitioners and to focus in on the role of established "mechanisms for knowledge production" within a knowledge system, i.e. the methods, tools, practices, instruments and institutions that are being deployed in IT risk management practices. This paper contributes to the literature on risk in the IS field by highlighting the limitations of checklist

approaches and by providing an empirical account of how risks management practices are shaped in a sociomaterial context.

Paper 4

Öbrand, L., Augustsson, N-P., Holmström, J. & Mathiassen, L. "*Information infrastructure risk: longitudinal study of risk emergence in supplier practices*" Currently under review (2nd round), at an international journal

This paper traces how risk was implicated in the practices of an information infrastructure supplier. IT products are becoming increasingly infrastructural and, therefore, IT professionals need to manage the dynamics involved in infrastructure evolution. Acknowledging risk management as a useful approach for dealing with the complexities and uncertainties associated with new product development, it draws on a practice approach to explore how an IT service provider team identified and managed risks in infrastructure development, support and sales. In the paper we review extant literature on information infrastructure theory, and conclude that it establishes risk as inherently emergent (through e.g. side-effects) but does not explain how risks are implicated. By conducting a longitudinal case study, spanning 10 years of development, support, and sales of information infrastructure services at a global IT-consultancy organization, we investigate how IT professionals identify and manage risks emerging from evolving information infrastructures. As a result, it contribute new insights into the specific area of information infrastructure risk management. At the same time, it reveals new forms of risk that contribute to the general discourse on IT risk management.

Paper 5

Öbrand, L. "*Managing information infrastructure risk: problems, causes, cures*" Currently under review (first round), at an international journal

This article argues that, ironically, extant risk management research and practices do not solve the problems they target; instead, they are a key cause of these problems! While IT has become increasingly infrastructural, complex and integrated, blurring technical, organizational and social boundaries, risk management models still build on the idea of stability and predictability. This paper explores the problems, causes and potential cures associated with information infrastructure risk management by reviewing

the state of the research field on information infrastructure risk and providing concrete examples from a case study. It concludes by drawing on lessons from research on high-reliability organizations (HRO) as an alternative way of managing risks related to the use of IT in contemporary organizations, by adapting the key points in the process of collective mindfulness – preoccupation with failure, reluctance to simplify operations, sensitivity to operations, commitment to resilience, and deference to expertise (rather than experts) – to information infrastructure risk management.

Discussion

Information technology has had a fundamental impact on the conditions for contemporary organizing (Tilson et al., 2010; Yoo et al., 2010), including the character and dynamics of risk (Carlo et al., 2004; Hanseth & Ciborra, 2007; Hu et al., 2012). Despite more than 30 years of practice and research on IT-related risk in the field of IS, projects continue to fail at largely the same level (Bannerman, 2008; Taylor et al., 2012) and organizations struggle to leverage IT as an organizational resource (Kohli & Grover, 2008; Sambamurthy et al., 2003). The situation is less than satisfactory, for both research and practice. Salience is a key driver of research legitimacy (Lyytinen & King, 2004) and in this dissertation I have explored reasons for why we cannot seem to make improvements, and made suggestions for how we should proceed in both research and practice.

Previous research efforts on risk and risk management in the IS field have emphasized risk factors, process and non-process models, and contingency models as alternative ways for organizations of addressing risk and risk management issues (Bannerman, 2008; Ciborra, 2004; Taylor et al., 2012). While these have been successful in helping risk managers address important risks, and thereby significantly improved practice, they have not significantly improved the overall success rate of IT projects or helped organizations leverage IT as a resource. Plasticity is another primary driver of legitimacy (Lyytinen & King, 2004) and a point of departure for this dissertation is the idea that the changing character of technology is a key reason for our inability to explain, understand, or manage risk. This dissertation suggests that the discourse on risk in the IS field needs to re-assess old truths and assumptions as digitalization has irrevocably changed the playing field.

I have problematized extant literature on risk and risk management by analyzing its underlying ontological and epistemological assumptions. Firstly, the analysis shows how the literature is based on technical risk analyses and economic perspectives, manifested in instrumental approaches to risk management. While effective in stable, predictable and unambiguous situations, these kinds of approaches have been criticized for their limited scope, inability to take the problem setting into account, and focus on individual decision makers. Some approaches address risk on an aggregate level (non-process frameworks of risk areas), and can be helpful for risk managers in situations with a high degree of uncertainty, but they are only applicable to pre-defined and unambiguous risk areas. Contingency approaches can be effective tools for risk managers to prepare options when

they face situations where equivocality is high, but will not help risk managers to identify or manage risks that fall outside of established options. None of the approaches found in the extant literature deal with risk as it manifests in situations characterized by a high degree of both uncertainty and equivocality, in which risks are emergent. This is unfortunate because there is ample evidence that these kinds of situations are typical for organizational consequences of IT (Cecez-Kecmanovic et al., 2014; Ciborra, 2000; Orlikowski & Baroudi, 1991; Robey & Boudreau, 1999), including risk (Ciborra, 2004; Hanseth & Ciborra, 2007). The case studies in this dissertation all illustrate risk and risk management practices in contexts characterized by a high degree of uncertainty and equivocality.

Secondly, the dissertation's analysis shows how information infrastructure theory introduces an alternative, sociological, notion of risk, drawing on the work of Beck (1992, 2000) and Giddens (1999) to understand and explain why situations in contemporary organizations are increasingly equivocal and uncertain. Risk is used as a concept to define logic of the process of change in organizations relying on increasingly interconnected layers and systems of IT. Simply put, as technology becomes infrastructural, complexity increases. Increased complexity means increased risk as actions create side-effects by propagating through multiple layers of loosely interconnected systems and finally reflecting back adversely onto the aim of the action itself. Risks are therefore emergent. While the literature in this sense addresses the situation and identifies the emergent character of risk, it does not provide any detailed descriptions of how risks emerge, or empirical evidence of information infrastructure risk management practices.

Theorizing information infrastructure risk

Grasping the logic of practice

The problematization of the extant literature reveals a gap between theory and practice such that existing research cannot account for or address significant aspects of the reality faced by organizations and organizational risk managers. Gaps of this nature have long been of concern for applied social sciences (Argyris & Schön, 1974; Lindblom & Cohen, 1979; Van de Ven, 2007) and there is evidence that research produces knowledge that is distant from, rather than useful for, practice (Mintzberg, 2004; Schön, 1983; Van de Ven & Johnson, 2006). Remembering Lyytinen & King's (2004) call for salience, it is problematic that there seems to be a gap between extant research on risk in the IS field and practice.

In an effort to overcome the problem of the theory – practice gap in management research, Sandberg & Tsoukas (2011) develop strategies for theorizing based on the richness of practice as an alternative to theorizing based on scientific rationality frameworks:

"Practical rationality offers a coherent onto-epistemological framework for generating what we call "practical rationality theories" – namely that, insofar as they explore how organizational practices are constituted and enacted by actors, capture essential aspects of the logic of practice […] therefore, make it possible to significantly reduce the theory-practice gap" (Sandberg & Tsoukas, 2011, p.339)

Their framework is reflective of the turn towards practice in the social sciences (Feldman & Orlikowski, 2011; Schatzki, Knorr-Cetina, & Von Savigny, 2001) and as such, of my epistemological position in this dissertation. Sandberg & Tsoukas (2011) propose two different strategies for theorizing in order to build theories relevant for practice: (1) strategies of entwinement; and (2) strategies of temporary breakdowns. Strategies for entwinement implicate taking sociomaterial practice as a point of departure, i.e. *"what practitioners routinely do, with others and tools, for what purposes"* (Sandberg & Tsoukas, 2011, p.351); looking at what practitioners competently do and say, and what it results in; identifying distinct ways practices are enacted; investigate how accountability is established, i.e. what is reportable and recognizable to others. By focusing on these aspects researchers can grasp the logic of practice and the scope of the sociomaterial whole that shapes human action. Theorizing through strategies for temporary breakdowns helps reveal the taken-for-granted distinctions that*"practitioners cannot articulate while absorbed in practice"* (Sandberg & Tsoukas, 2011, p. 351) and that are not captured by entwinement strategies. Temporary breakdown strategies means a focus on: instances when expectations are not met, boundaries are crossed, or differences in awareness are noticed; situating the breakdowns in a broader sociomaterial practice in which they occur; and identifying how practitioners are absorbed in their everyday activities within the practice.

The theorization of information infrastructure risk in this dissertation reflects the framework proposed by Sandberg & Tsoukas (2011). They note that it is unusual to see all of the components of a given problem in any single study or paper due to the pragmatic constraints of both case studies and research outlets. However, viewed as a whole this dissertation includes all components and thus strengthens my claim for the salience of my research efforts. In addition, I would argue that the third case in this dissertation, reported in paper 4, includes all components. Below, I will

discuss in more detail how I have theorized information infrastructure risk, and how the result of my theorizing present distinct perspectives on how information infrastructure risk emerges and how it is managed.

A practice-based view of risk

By examining the microdynamics of organizing, the work in this dissertation has uncovered and contributed to understanding of how risk is produced and managed in different information infrastructure contexts. Based on my case studies I argue for a practice-based view of risk as a complementary alternative to the instrumental view that dominates extant research. The practice-based view should be understood as complementary in the sense that it offers a way of identifying, understanding, and managing the new kind of risks related to information infrastructures.

Evident in all three cases in this dissertation, it was abundantly clear that information infrastructure risk cannot be captured, understood or explained with an instrumental view of risk. Risks were defined by the perspective, knowledge, and situated goals of practitioners and practices rather than objective, quantifiable and related to shared and unequivocal organizational goals. Furthermore, they were to a large extent collectively made sense of within and between teams of involved practitioners. While a number of important risks were identified through the use of risk management methods in both case 2 and 3, these did not include emergent risks emanating from the information infrastructure dynamics. The investigation of risk management practices also showed how risk identification, assessment and resolution activities were enacted by all practitioners in the organizations, and was thus not only the responsibility of experts or appointed risk managers. Risk management was collaborative, situated, and dependent on conflicting goals, practitioner knowledge and established practices.

The practice base view thus captures the *pragmatic* nature of risk, as it allows us to uncover how risk is inextricably related to the shifting and situated goals and knowledge of practitioners and practices. This means that what constitutes a risk for one practitioner or practice might be seen as an opportunity for another and as a simple irrelevance for a third. Practitioners make sense of risk through continuous interaction with others and with the situation as it unfolds, and employ different epistemic strategies depending on the type of risk they identify. If uncertainty and equivocality are low, i.e. when both the risks and the risk resolution techniques were known, practitioners could employ proactive risk management strategies. Situations with low equivocality but a high degree of uncertainty, i.e. where the risks are known but the actions required for their resolution are not, were

characterized by reactive risk management strategies. Adaptive risk management strategies were adopted when both equivocality and uncertainty was high. These were characterized by continuous monitoring of the situation, boundary spanning and situated generation of knowledge. Put another way, the practitioners carried out "reflective conversations with the situation" (Schön, 1983).

Construct	Instrumental view	Practice-based view
Risk	Risk is a discrete event that may occur and have a quantifiable impact on organizational goals and sustainability.	Risk is a matter of perspective, shaped by risk managers' views of the practice, situated goals and knowledge.
Risk analysis	Risks can be comprehensively identified and assessed through use of appropriate methods.	Risks are made sense of through networking within and between teams of involved practitioners.
Risk resolution	Risks are resolved through pre-determined courses of action as an expression of single loop learning.	Risks trigger situated learning activities and are resolved through these activities.
Risk management	Risk management is carried out by risk experts and managers based on risk management methods. Risks, once properly identified, can be mitigated.	Risk management is carried out by the practitioners involved in and between practices. Risk management is situated and dependent on conflicting goals, practitioner knowledge, and established practices.
Philosophical foundations	Grounded in a realist philosophy, risks can be pre-conceived and divorced from the context.	Grounded in a pragmatist philosophy, risks are emergent and socially constructed through practice.
Risk research	Risk research aims at identifying potential risk factors and developing risk management methods to address them.	Risk research aims at theorizing practice in order to understand how risks are produced and managed as part of everyday life in organizations.

The practice-based view of risk proposed in this dissertation makes a distinct contribution to the IS discourse on risk and risk management. It offers an alternative to the instrumental view, based on different ontological and

epistemological assumptions that embraces the logic of practice in an effort to bridge the gap between theory and practice.

The interstitiality of information infrastructure risk

Extant literature on information infrastructure suggests that unplanned events and side-effects are characteristic of the evolution dynamics (Blechar & Hanseth, 2007; Hanseth & Ciborra, 2007), and the notion of emergence is well established. However, there are no detailed accounts of how risk emerges in information infrastructures, or how it is managed in practice. The practice approach adopted in this dissertation, and the richness of the case studies, made possible a particular focus on the sources and tensions, events and interactions that caused risk to emerge.

In both case 2 (the paper mill) and case 3 (the information infrastructure supplier) it is evident that risk was linked to multiple, rather than individual, practices. Practices became increasingly entwined with each other and organizational structures, and at the boundaries of these risks emerged. In paper 4 we identify three types of practices of information infrastructures between which risk was implicated: customer practices, internal practices, and exogenous practices. Risks tended to emerge at the interstices of these practices and were over time affected by the interplay between structure and practices. The configuration of these forces will differ for any given risk, but over time these types of boundaries became apparent in all cases. These types of inter-related practices were found in all of the cases examined in the dissertation. In paper 4, which focused on the information infrastructure supplier, they were perhaps most clearly visible in the multiple sets of requirements the team had to balance in every project. An illustration from case 2, the paper mill, would be how changes in the IT vendor's practices had a direct impact on the conditions that the paper mill had to maintain to sustain continuous production. Indeed, as an outcome of our case studies, the paper mill and their IT vendor re-negotiated some of these boundaries in order to reduce risk.

INFORMATION INFRASTRUCTURE
RISK FORCES

EXOGENOUS
PRACTICES

INTERNAL
PRACTICES

CUSTOMER
PRACTICES

In this dissertation I theorize information infrastructure risk as *interstitial* because it emerges over time and falls between established practices and organizational functions. Emergence is a consequence of the dynamics of an evolving organizational, technological and social context, while interstitiality stems from the complex interplay of the organizational structures and practices that shape the on-going make-up of the infrastructure.

Unpacking technology

In all of the cases considered in this dissertation, digital artifacts were embedded in a wider context that became increasingly editable, interactive, reprogrammable and distributable. As technology became increasingly interconnected and infrastructural, boundaries were blurred and transcended. As information infrastructures evolve and grow in complexity and heterogeneity, new risks emerge at the interstices between different but dependent practices. Understanding technology from an information infrastructure perspective recognizes opposing forces and the variable ontology of technology (Latour & Porter, 1996). Risk is socially constructed, based on the knowledge and aims of particular actors, situated and rooted in practice. When the knowledge and experience of practitioners do not develop in tune with changes in the character of technology, risks will either be left unidentified (and thus unmanaged) or (mis-)managed with risk resolution techniques that will result in side-effects or worse. In short, even if risk is a socially constructed notion, the studies in this dissertation suggest that reality is not. Indeed, information infrastructure technologies can be characterized as recalcitrant with regards to their impact on risk:

"Natural objects are naturally recalcitrant; the last thing one scientist will say about them is that they are fully masterable. On the contrary, they

always resist and make shambles of our pretensions to control" (Latour, 2000, p.116)

The cases investigated in this dissertation clearly show how the character of technology became increasingly infrastructural and how that affected both the emergence of risk and the conditions for its management. As the complexity and integration of technologies increased, so did the heterogeneity of the installed bases. The interrelationships between practices both within and across organizational boundaries increased and became more complex and affected one another in unpredictable ways. As the character of technology changed, risk became *systemic* (Carlo et al., 2004; Hu et al., 2012) as it originates from multiple sources between established practices, affects multiple actors and propagates quickly through multiple levels of practice.

Managing information infrastructure risk

After problematizing the underlying assumptions of extant research on risk in the IS field, and based on an information infrastructure perspective and a practice approach, I have theorized risk as pragmatic, interstitial, and systemic. This, I suggest, explains why research based on technical rationality and an instrumental view of risk cannot address the risks faced by practitioners in contemporary organizations. The backdrop for the dissertation as a whole is the fact that we, after several decades of risk research, still see the same, unacceptably high, number of failed projects and difficulties in leveraging IT as an organizational resource. This final section of the discussion in the dissertation deals with the question of whether we can manage information infrastructure risk, and how to go about doing it if it is possible.

The bad news is that risk management models based on an instrumental view can in fact contribute to the propagation and diffusion of information infrastructure risk. Research has shown how risk models tend to "shape the attention" (Lyytinen et al., 1998) of practitioners by directing them to certain risk factors and ways of thinking about risk. While this is potentially effective in stable, predictable situations it could make for an illusory feeling of control in situations where the most important risks will be overlooked. As such, instrumental risk management constitutes a real risk in contemporary organizational settings. The good news is that the cases in this dissertation show how skilled and reflexive practitioners collaborate to sense emerging risks, something that is made possible by their intimate knowledge of the idiosyncrasies of practice and technology, and manage them by employing

adaptable strategies involving generating relevant knowledge and using the resources they have at hand.

Research on high reliability organizations (HROs) focuses on risk control in complex socio-technical systems (Roberts, 1990; Rochlin, 1993) characterized by complex interactions and tight coupling, suffering from systemic risks. To manage in these kinds of situations, Weick et al. (2008) suggest that HROs are able to sustain complex socio-technical systems despite facing emerging systemic risk by processes of *collective mindfulness*. The practitioners in my cases worked in ways that resembled the key points of collective mindfulness: (1) preoccupation with failure; (2) reluctance to simplify interpretations; (3) sensitivity to operations; (4) commitment to resilience; and (5) deference to expertise.

Conclusions

In this dissertation I have investigated how information infrastructure risk emerges and is managed. By problematizing the underlying assumptions of extant research, I have shown how it fails to address an increasing number of risks typically encountered by contemporary organizations. These risks stem from the increasingly infrastructural character of IT. While information infrastructure theory explains why organizational contexts are characterized by a high degree of equivocality and uncertainty, and why risks are increasingly emergent, it has yet to investigate in detail how emergence takes place or provide empirical evidence of information infrastructure risk management practices.

Adopting practice theory as an empirical lens, I have theorized information infrastructure risk as pragmatic, interstitial, and systemic. It is rooted in the situated knowledge and goals of practice, it emerges at the interstices of dependent, but different, practices and organizational structures, it affects multiple practices, and it propagates through layers and networks of practices within and across organizational boundaries. Successful examples of sustainable information infrastructure risk management have many aspects in common with the characteristic traits of high reliability organizations.

References

Aanestad, M., & Blegind Jensen, T. (2011). Building nation-wide information infrastructures in healthcare through modular implementation strategies. *The Journal of Strategic Information Systems, 20*(2), 161-176.

Ackoff, R. L. (1967). Management misinformation systems. *Management Science, 14*(4), B-147-B-156.

Addison, T., & Vallabh, S. (2002). Controlling Software Project Risks: an Empirical Study of Methods used by Experienced Project Managers. *Proceedings of SAICSIT*.

Ahn, J.-H., & Skudlark, A. (2002). Managing risk in a new telecommunications service development process through a scenario planning approach. *Journal of Information Technology, 17*(3), 103-118. doi: 10.1080/02683960210161258

Alavi, M., Carlson, P., & Brooke, G. (1989). *The ecology of MIS research: a twenty year status review*. Paper presented at the International Conference on Information Systems: Proceedings of the tenth international conference on Information Systems: Boston, Massachusetts, United States.

Alavi, M., & Leidner, D. E. (2001). Review: Knowledge management and knowledge management systems: Conceptual foundations and research issues. *MIS Quarterly*, 107-136.

Alhawari, S., Karadsheh, L., Talet, A. N., & Mansour, E. (2012). Knowledge-Based Risk Management framework for Information Technology project. *International Journal of Information Management, 32*(1), 50-65. doi: Doi 10.1016/J.Ijinfomgt.2011.07.002

Aloini, D., Dulmin, R., & Mininno, V. (2007). Risk management in ERP project introduction: Review of the literature. *Information & Management, 44*(6), 547-567. doi: 10.1016/j.im.2007.05.004

Alter, S., & Ginzberg, M. (1978). Managing uncertainty in MIS implementation. *Sloan Management Review, 20*(1), 23-31.

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

Alvesson, M., & Sandberg, J. (2011). Generating Research Questions Through Problematization. *Academy of Management Review, 36*(2).

Argyris, C., & Schön, D. A. (1974). *Theory in practice*. San Francisco: Jossey-Bass.

Arnold, V., Benford, T., Hampton, C., & Sutton, S. G. (2010). Competing pressures of risk and absorptive capacity potential on commitment and information sharing in global supply chains. *European Journal of Information Systems, 19*(2), 134-152. doi: 10.1057/ejis.2009.49

Aron, R., Clemons, E. K., & Reddi, S. (2005). Just Right Outsourcing; Understanding and Managing Risk. *Journal of Management Information Systems, 22*(2).

Arvidsson, V., Holmström, J., & Lyytinen, K. (2014). Information systems use as strategy practice: A multi-dimensional view of strategic information system implementation and use. *The Journal of Strategic Information Systems, 23*(1), 45-61.

Aubert, B. A. P., Michel; Rivard, Suzanne. (2005). A Framework for Information Technology Outsourcing Risk Management. *The DATA BASE for Advances in Information Systems, 36*(4).

Avison, D. E., Dwivedi, Y. K., Fitzgerald, G., & Powell, P. (2008). The beginnings of a new era: time to reflect on 17 years of the ISJ. *Information Systems Journal, 18*(1), 5-21.

Avison, D. E., Lau, F., Myers, M. D., & Nielsen, P. A. (1999). Action research. *Communications of the ACM, 42*(1), 94-97.

Avison, D. E., & Malaurent, J. (2014). Is theory king?: questioning the theory fetish in information systems. *Journal of Information Technology*.

Bahli, B., & Rivard, S. (2003). The information technology outsourcing risk: a transaction cost and agency theory-based perspective. *Journal of Information Technology, 18*(3), 211-221. doi: 10.1080/0268396032000130214

Bai, X., Krishnan, R., Padman, R., & Wang, H. J. (2013). On Risk Management with Information Flows in Business Processes. *Information Systems Research, 24*(3), 731-749. doi: Doi 10.1287/Isre.1120.0450

Bannerman, P. L. (2008). Risk and risk management in software projects: A reassessment. *Journal of Systems and Software, 81*(12), 2118-2133. doi: 10.1016/j.jss.2008.03.059

Bansler, J. (1989). Systems development research in Scandinavia: three theoretical schools. *Scandinavian Journal of Information Systems, 1*(9), 3-20.

Banville, C., & Landry, M. (1989). Can the Field of MIS be Disciplined? *Communications of the ACM, 32*(1), 48-60.

Barker, A., Nancarrow, C., & Spackman, N. (2001). Informed eclecticism: A research paradigm for the twenty-first century. *International journal of market research, 43*(1), 3.

Barki, H., Rivard, S., & Talbot, J. (1993). Towards an Assessment of Software Development Risk. *Journal of Management Information Systems, 10*(2).

Barki, H., Rivard, S., & Talbot, J. (2001). An Integrative Contingency Model of Software Project Risk Management. *Journal of Management Information Systems, 17*(4).

Barley, S. R. (2015). Why the Internet Makes Buying a Car Less Loathsome: How Technologies Change Role Relations. *Academy of Management Discoveries, 1*(1), 5-34.

Barley, S. R., & Kunda, G. (2001). Bringing work back in. *Organization Science, 12*(1), 76-95.

Baskerville, R. L., & Myers, M. D. (2002). Information systems as a reference discipline. *MIS Quarterly*, 1-14.

Beck, U. (1992). *Risk society: Towards a new modernity* (Vol. 17): Sage.

Beck, U. (1994). *Reflexive modernization: Politics, tradition and aesthetics in the modern social order*: Stanford University Press.

Beck, U. (2000). Risk society revisited: theory, politics and research programmes. *The risk society and beyond: Critical issues for social theory*, 211-229.

Beck, U., Bonss, W., & Lau, C. (2003). The theory of reflexive modernization problematic, hypotheses and research programme. *Theory, culture & society, 20*(2), 1-33.

Benaroch, M. (2002). Managing Information Technology Investment Risk: A Real Options Perspective. *Journal of Management Information Systems, 19*(2).

Benbasat, I., & Barki, H. (2007). Quo vadis TAM? *Journal of the Association for Information Systems, 8*(4), 7.

Benbasat, I., Goldstein, D. K., & Mead, M. (1987). The Case Research Strategy in Studies of Information Systems. *MIS Quarterly, 11*(3).

Benbasat, I., & Schroeder, R. G. (1977). An experimental investigation of some MIS design variables. *MIS Quarterly*, 37-49.

Benbasat, I., & Weber, R. (1996). Research commentary: Rethinking "diversity" in information systems research. *Information Systems Research, 7*(4), 389-399.

Benbasat, I., & Zmud, R. W. (2003). The identity crisis within the IS discipline: Defining and communicating the discipline's core properties. *MIS Quarterly*, 183-194.

Beniger, J. (2009). *The control revolution: Technological and economic origins of the information society*: Harvard University Press.

Berente, N., & Yoo, Y. (2012). Institutional contradictions and loose coupling: Postimplementation of NASA's enterprise information system. *Information Systems Research, 23*(2), 376-396.

Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, N. (2013). Digital business strategy: toward a next generation of insights. *MIS Quarterly, 37*(2), 471-482.

Bjerknes, G., & Bratteteig, T. (1995). User participation and democracy: A discussion of Scandinavian research on system development. *Scandinavian Journal of Information Systems, 7*(1), 1.

Blechar, J., & Hanseth, O. (2007). 7. From risk management to 'organized irresponsibility'? Risks and risk management in the mobile telecom sector. *Risk, Complexity and ICT*, 136.

Blumer, H. (1931). Science without concepts. *American Journal of Sociology*, 515-533.

Boehm, B. W. (1973). Quantitative Assessment. *Datamation, 19*(5), 49-57.

Boehm, B. W. (1989). *Software risk management*: Springer.

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

Boudreau, M.-C., & Robey, D. (2005). Enacting integrated information technology: A human agency perspective. *Organization Science, 16*(1), 3-18.

Braa, J., Hanseth, O., Heywood, A., Mohammed, W., & Shaw, V. (2007). Developing health information systems in developing countries: the flexible standards strategy. *MIS Quarterly*, 381-402.

Braa, K., Sørensen, C., & Dahlbom, B. (Eds.). (2000). *Planet Internet*. Lund: Studentlitteratur.

Bradbury, J. A. (1989). The policy implications of differing concepts of risk. *Science, Technology & Human Values, 14*(4), 380-399.

Broadbent, M., Weill, P., & St. Clair, D. (1999). The implications of information technology infrastructure for business process redesign. *MIS Quarterly*, 159-182.

Brown, J. S., & Duguid, P. (1991). Organizational learning and communities-of-practice: Toward a unified view of working, learning, and innovation. *Organization Science, 2*(1), 40-57.

Brynjolfsson, E., & Saunders, A. (2010). Wired for innovation: how information technology is reshaping the economy.

Burton-Jones, A., & Gallivan, M. J. (2007). Toward a deeper understanding of system usage in organizations: a multilevel perspective. *MIS Quarterly*, 657-679.

Bygstad, B. (2010). Generative mechanisms for innovation in information infrastructures. *Information and Organization, 20*(3), 156-168.

Bødker, K., Kensing, F., & Simonsen, J. (2009). *Participatory IT design: designing for business and workplace realities*: MIT press.

Carlo, J. L., Lyytinen, K., & Boland, R. J. (2004). Systemic Risk, IT Artifacts, and High Reliability Organizations: A Case of Constructing a Radical Architechture. *Sprouts: Working Papers on Information Systems, 4*(2).

Carlo, J. L., Lyytinen, K., & Boland, R. J. (2012). Dialectics of Collective Minding: Contradictory Appropriations of Information Technology in a High-Risk Project. *MIS Quarterly, 36*(4), 1081-1106.

Cecez-Kecmanovic, D., Galliers, R. D., Henfridsson, O., Newell, S., & Vidgen, R. (2014). The sociomateriality of information systems: current status, future directions. *MIS Quarterly, 38*(3), 809-830.

Cetina, K. K. (2009). *Epistemic cultures: How the sciences make knowledge*: Harvard University Press.

Charette, R. N. (1989). *Software engineering risk analysis and management*: Intertext Publications.

Charette, R. N. (1996). The mechanics of managing IT risk. *Journal of Information Technology, 1*, 373-378.

Checkland, P. (2000). Soft systems methodology: a thirty year retrospective. *Systems Research and Behavioral Science, 17*, S11-S58.

Churchman, C. W. (1971). Design of inquiring systems: basic concepts of systems and organization.

Ciborra, C. (1996). The platform organization: Recombining strategies, structures, and surprises. *Organization Science, 7*(2), 103-118.

Ciborra, C. (2000). *From control to drift: the dynamics of corporate information infastructures*: Oxford University Press.

Ciborra, C. (2004). Digital Technologies and the Duality of Risk *CARR - Centre for Analysis of Risk and Regulation at London School of Economics*.

Ciborra, C., Braa, K., & Cordella, A. (2000). *From control to drift: The dynamics of global information infrastructures*: Oxford University Press.

Ciborra, C., & Failla, A. (2000). Infrastructure as a Process: The Case of CRM in IBM. *From control to drift: The dynamics of corporate information infrastructures*, 105-124.

Clarke, L., & Short Jr, J. F. (1993). Social organization and risk: Some current controversies. *Annual Review of Sociology*, 375-399.

Clemons, E. K., & Weber, B. W. (1990). Strategic Information Technology Investments: Guidelines for Decision Making. *Journal of Management Information Systems, 7*(2).

Cooper, R. B. (1988). Review of management information systems research: a management support emphasis. *Information Processing & Management, 24*(1), 73-102.

Croon Fors, A. (2006). Being-with Information Technology: Critical explorations beyond use and design.

Currie, W. L. (1998). Using multiple suppliers to mitigate the risk of IT outsourcing at ICI and Wessex Water. *Journal of Information Technology, 13*, 169-180.

Currie, W. L., & Willcocks, L. P. (1998). Analysing four types of IT sourcing decisions in the context of scale, client/supplier interdependency and risk mitigation. *Information Systems Journal, 8*, 119-143.

Daft, R. L., & Lengel, R. H. (1986). Organizational information requirements, media richness and structural design. *Management Science, 32*(5), 554-571.

Dahlbom, B. (1995). Göteborg Informatics. *Scandinavian Journal of Information Systems, 7*(2), 2.

Dahlbom, B., & Langefors, B. (1995). *The infological equation: Essays in honor of Börje Langefors*: Department of Informatics, School of Economics and Commercial Law, Univ.

Dahlbom, B., & Mathiassen, L. (1993). *Computers in context: The philosophy and practice of systems design*: Blackwell Publishers, Inc.

Davis, G. B. (2000). Information systems conceptual foundations: looking backward and forward *Organizational and social perspectives on information technology* (pp. 61-82): Springer.

Dhillon, G. B., J. (1996). Risks in the Use of Information Technology Within Organizations. *International Journal of Information Management, 16*(1), 65-74.

Dickson, G. W. (1981). Management information systems: Evolution and status. *Advances in computers, 20*(1), 1-37.

Dickson, G. W., Senn, J. A., & Chervany, N. L. (1977). Research in management information systems: The Minnesota experiments. *Management Science, 23*(9), 913-934.

Dionne, G. (2013). Risk Management: History, Definition, and Critique. *Risk Management and Insurance Review, 16*(2), 147-166.

Drummond, H. (2011). MIS and illusions of control: an analysis of the risks of risk management. *Journal of Information Technology, 26*(4), 259-267. doi: Doi 10.1057/Jit.2011.9

Ehn, P. (1988). Work-oriented design of computer artifacts.

Ehn, P. (1993). Scandinavian design: On participation and skill. *Participatory design: Principles and practices*, 41-77.

Eisenhardt, K. M. (1989). Building theories from case study research. *Academy of Management Review, 14*(4), 532-550.

Engwall, L. (1995). Management research: a fragmented adhocracy? *Scandinavian Journal of Management, 11*(3), 225-235.

Featherman, M. S., Valacich, J. S., & Wells, J. D. (2006). Is that authentic or artificial? Understanding consumer perceptions of risk in e-service encounters. *Information Systems Journal, 16*.

Feldman, M. S., & Orlikowski, W. J. (2011). Theorizing Practice and Practicing Theory. *Organization Science, 22*(5), 1240-1253. doi: 10.1287/orsc.1100.0612

Fischhoff, B., Watson, S. R., & Hope, C. (1984). Defining risk. *Policy Sciences, 17*(2), 123-139.

Galliers, R. D., & Sutherland, A. (1991). Information systems management and strategy formulation: the 'stages of growth'model revisited. *Information Systems Journal, 1*(2), 89-114.

Gaskin, J., Berente, N., Lyytinen, K., & Yoo, Y. (2014). Toward generalizable sociomaterial inquiry: a computational approach for zooming in and out of sociomaterial routines. *MIS Quarterly, 38*(3), 849-871.

Gemino, A., Reich, B. H., & Sauer, C. (2007). A Temporal Model of Information Technology Project Performance. *Journal of Management Information Systems, 24*(3), 9-44. doi: 10.2753/mis0742-1222240301

Giddens, A. (1984). Hermeneutics and social theory. *Hermeneutics-Questions and Prospects*, 215-230.

Giddens, A. (1999). Risk and Responsibility. *The Modern Law Review, 62*(1), 1-10.

Goldkuhl, G. (2004). Meanings of Pragmatism: Ways to conduct information systems research. *Action in Language, Organisations and Information Systems.*

Gregor, S. (2014). Theory–still king but needing a revolution. *Journal of Information Technology, 29*(4), 337-340.

Haeckel, S. H. (1995). Adaptive enterprise design: the sense-and-respond model. *Planning Review, 23*(3), 6-42.

Haeckel, S. H. (2013). *Adaptive enterprise: Creating and leading sense-and-respond organizations*: Harvard business press.

Hanseth, O., Aanestad, M., & Berg, M. (2004). Guest editors' introduction: Actor-network theory and information systems. What's so special? *Information Technology & People, 17*(2), 116-123.

Hanseth, O., & Braa, K. (1998). *Technology as traitor: Emergent SAP infrastructure in a global organization.* Paper presented at the Proceedings of the international conference on Information systems.

Hanseth, O., & Ciborra, C. (2007). *Risk, complexity and ICT*: Edward Elgar Publishing.

Hanseth, O., Ciborra, C., & Braa, K. (2001). The control devolution: ERP and the side effects of globalization. *ACM SIGMIS Database, 32*(4), 34-46.

Hanseth, O., Jacucci, E., Grisot, M., & Aanestad, M. (2006). Reflexive Standardization: Side Effects and Complexity in Standard Making. *MIS Quarterly, 30*, 563-581.

Hanseth, O., & Lyytinen, K. (2010). Design theory for dynamic complexity in information infrastructures: the case of building internet. *Journal of Information Technology, 25*(1), 1-19.

Hanseth, O., & Monteiro, E. (1997). Inscribing behaviour in information infrastructure standards. *Accounting, Management and Information Technologies, 7*(4), 183-211.

Hanseth, O., Monteiro, E., & Hatling, M. (1996). Developing information infrastructure: The tension between standardization and flexibility. *Science, Technology & Human Values, 21*(4), 407-426.

Hawthorne, J., & Stanley, J. (2008). Knowledge and action. *The Journal of Philosophy, 105*(10), 571-590.

Heemstra, F. J., & Kusters, R. J. (1996). Dealing with risk: a practical approach. *Journal of Information Technology, 11*, 333-346.

Henfridsson, O. (2014). The power of an intellectual account: developing stories of the digital age. *Journal of Information Technology, 29*(4), 356-357.

Henfridsson, O., & Bygstad, B. (2013). The generative mechanisms of digital infrastructure evolution. *MIS Quarterly, 37*(3), 907-931.

Hirschheim, R., Klein, H. K., & Lyytinen, K. (1996). Exploring the intellectual structures of information systems development: a social action theoretic analysis. *Accounting, Management and Information Technologies, 6*(1), 1-64.

Hirschheim, R., Saunders, C., & Straub, D. (2012). Historical Interpretations of the IS Discipline: An introduction to the special issue. *Journal of the Association for Information Systems (JAIS), 13*(4).

Holmström, J., & Stalder, F. (2001). Drifting technologies and multi-purpose networks: the case of the Swedish cashcard. *Information and Organization, 11*(3), 187-206.

Hsieh, J. P.-A., Rai, A., & Keil, M. (2008). Understanding digital inequality: Comparing continued use behavioral models of the socio-economically advantaged and disadvantaged. *MIS Quarterly*, 97-126.

Hsu, C., Backhouse, J., & Silva, L. (2014). Institutionalizing operational risk management: an empirical study. *Journal of Information Technology, 29*(1), 59-72.

Hu, D., Zhao, J. L., Hua, Z., & Wong, M. C. S. (2012). Network-Based Modeling and Analysis of Systemic Risk in Banking Systems. *MIS Quarterly, 36*(4), 1289-1291.

Huang, S.-M., Chang, I. C., Li, S.-H., & Lin, M.-T. (2004). Assessing risk in ERP projects: identify and prioritize the factors. *Industrial*

Management & Data Systems, 104(8), 681-688. doi: 10.1108/02635570410561672

Iivari, J., & Lyytinen, K. (1999). Research on information systems development in Scandinavia. *Rethinking Management Information Systems*, 57-102.

ISO31000. (2009). Risk management - Principles and guidelines: International Standards Organization.

Ivanov, K. (2001). The systems approach to design, and inquiring information systems: Scandinavian experiences and proposed research program. *Information Systems Frontiers, 3*(1), 7-18.

Iversen, J. H., Mathiassen, L., & Nielsen, P. A. (2004). Managing risk in software process improvement: an action research approach. *MIS Quarterly*, 395-433.

Jaeger, C. C., Webler, T., Rosa, E. A., & Renn, O. (2013). *Risk, uncertainty and rational action*: Routledge.

Janlert, L.-E., & Stolterman, E. (1997). The character of things. *Design Studies, 18*(3), 297-314.

Jonsson, K., Holmström, J., & Lyytinen, K. (2009). Turn to the material: Remote diagnostics systems and new forms of boundary-spanning. *Information and Organization, 19*(4), 233-252.

Kallinikos, J. (2004). *Farewell to constructivism: Technology and context-embedded action*: Citeseer.

Kallinikos, J. (2007). *The consequences of information: Institutional implications of technological change*: Edward Elgar Publishing.

Kaplan, B., & Duchon, D. (1988). Combining qualitative and quantitative methods in information systems research: a case study. *MIS Quarterly*, 571-586.

Keil, M., Li, L., Mathiassen, L., & Zheng, G. (2008). The influence of checklists and roles on software practitioner risk perception and decision-making. *Journal of Systems and Software, 81*(6), 908-919. doi: 10.1016/j.jss.2007.07.035

Keil, M., Tiwana, A., & Bush, A. (2002). Reconciling user and project manager precepetions of IT project risk: a Delphi study. *Information Systems Journal, 12*, 103-119.

King, J. L., & Lyytinen, K. (2006). *Information systems: The state of the field*: John Wiley & Sons Chichester, UK.

Klang, M. (2006). *Disruptive technology: Effects of technology regulation on democracy*: Department of Applied Information Technology.

Klein, H. K., & Hirschheim, R. (2008). The structure of the IS discipline reconsidered: Implications and reflections from a community of practice perspective. *Information and Organization, 18*(4), 280-302.

Klein, H. K., & Myers, M. D. (1999). A set of principles for conducting and evaluating interpretive field studies in information systems. *MIS Quarterly*, 67-93.

Kling, R. (2000). Learning about information technologies and social change: The contribution of social informatics. *The information society, 16*(3), 217-232.

Knight, F. H. (2012). *Risk, uncertainty and profit*: Courier Dover Publications.

Kohli, R., & 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), 1.

Kumar, R. L. (2002). Managing risks in IT projects: an options perspective. *Information & Management, 40*, 63-74.

Lacity, M. C., Khan, S. A., & Willcocks, L. P. (2009). A review of the IT outsourcing literature: Insights for practice. *The Journal of Strategic Information Systems, 18*(3), 130-146.

Langefors, B. (1966). *Theoretical analysis of information systems.* Lund, Sweden: Studentlitteratur.

Latour, B. (2000). When things strike back: a possible contribution of 'science studies' to the social sciences. *The British Journal of Sociology, 51*(1), 107-123.

Latour, B., & Porter, C. (1996). *Aramis, or, The love of technology* (Vol. 1996): Harvard University Press Cambridge, MA.

Lauer, T. W. (1996). Software project managers' risk preferences. *Journal of Information Technology, 11*, 287-295.

Lave, J., & Wenger, E. (1991). *Situated learning: Legitimate peripheral participation*: Cambridge university press.

Lee, A. S. (2014). Theory is king? But first, what is theory? *Journal of Information Technology, 29*(4), 350-352.

Leonardi, P. M. (2011). When flexible routines meet flexible technologies: Affordance, constraint, and the imbrication of human and material agencies. *MIS Quarterly, 35*(1), 147-167.

Leonardi, P. M. (2012). Matriality, Sociomateriality, and Socio-Technical Systems: What Do These Terms Mean? How Are They Different? Do We Need Them? In P. M. N. Leonardi, Bonnie A.; Kallinikos, Jannis (Ed.), *Materiality and Organizing*: Oxford University Press.

Leonardi, P. M., & Barley, S. R. (2010). What's under construction here? Social action, materiality, and power in constructivist studies of technology and organizing. *The academy of management annals, 4*(1), 1-51.

Leonardi, P. M., Nardi, B. A., & Kallinikos, J. (2012). *Materiality and organizing: Social interaction in a technological world*: Oxford University Press.

Levén, P., Holmström, J., & Mathiassen, L. (2014). Managing research and innovation networks: Evidence from a government sponsored cross-industry program. *Research Policy, 43*(1), 156-168. doi: 10.1016/j.respol.2013.08.004

Light, B., & Wagner, E. (2006). Integration in ERP environments: rhetoric, realities and organisational possibilities. *New Technology, Work and Employment, 21*(3), 215-228.

Lindblom, C. E., & Cohen, D. K. (1979). *Usable knowledge: Social science and social problem solving* (Vol. 21): Yale University Press.

Lindgren, R., Henfridsson, O., & Schultze, U. (2004). Design principles for competence management systems: a synthesis of an action research study. *MIS Quarterly*, 435-472.

Ljungberg, F. *Networking, September 1997*. Doctoral Thesis.

Lyytinen, K., & Hirschheim, R. (1988). Information systems as rational discourse: An application of Habermas's theory of communicative action. *Scandinavian Journal of Management, 4*(1), 19-30.

Lyytinen, K., & King, J. L. (2004a). Nothing at the Center?: Academic Legitimacy in the Information Systems Field. *Journal of the Association for Information Systems, 5*(6).

Lyytinen, K., & King, J. L. (2004b). Nothing at the center?: Academic legitimacy in the information systems field. *Journal of the Association for Information Systems, 5*(6), 8.

Lyytinen, K., Mathiassen, L., & Ropponen, J. (1996). A framework for software risk managment *Journal of Information Technology, 11*, 275-285.

Lyytinen, K., Mathiassen, L., & Ropponen, J. (1998). Attention Shaping and Software Risk: A Categorical Analysis of Four Classical Risk Management Approaches. *Information Systems Research, 9*(3).

MacLean, D. (1986). *Values at risk*: Rowman & Littlefield Pub Inc.

Malhotra, A., Gosain, S., & Sawy, O. A. E. (2005). Absorptive capacity configurations in supply chains: gearing for partner-enabled market knowledge creation. *MIS Quarterly*, 145-187.

March, J. G., & Shapira, Z. (1987). Managerial Perspectives on Risk and Risk Taking. *Management Science, 33*(11).

Markus, M. L. (1983). Power, politics, and MIS implementation. *Communications of the ACM, 26*(6), 430-444.

Markus, M. L., & Robey, D. (1988). Information technology and organizational change: causal structure in theory and research. *Management Science, 34*(5), 583-598.

Markus, M. L., & Silver, M. S. (2008). A foundation for the study of IT effects: A new look at DeSanctis and Poole's concepts of structural features and spirit. *Journal of the Association for Information Systems, 9*(10), 5.

Mason, J. (2002). *Qualitative researching*: Sage.

Massingham, P. (2010). Knowledge risk management: a framework. *Journal of Knowledge Management, 14*(3), 464-485.

Mathiassen, L., & Nielsen, P. A. (2008). Engaged scholarship in IS research. *Scandinavian Journal of Information Systems, 20*(2), 1.

Mathiassen, L., & Purao, S. (2002). Educating reflective systems developers. *Information Systems Journal, 12.*

Mathiassen, L., & Stage, J. (1990). The principle of limited reduction in software design. *Information Technology & People, 6*(2/3), 171-185.

Mathiassen, L., Tuunanen, T., Saarinen, T., & Rossi, M. (2007). A Contingency Model for Requirements Development. *Journal of the Association for Information Systems, 8*(11).

Mazlish, B. (1989). *A new science: the breakdown of connections and the birth of sociology*: Oxford University Press.

McFarlan, F. W. (1981). Portfolio Approach to information systems. *Harvard Business Review.*

Melville, N., Kraemer, K., & Gurbaxani, V. (2004). Review: Information technology and organizational performance: An integrative model of IT business value. *MIS Quarterly, 28*(2), 283-322.

Miller, E. M. (1977). Risk, uncertainty, and divergence of opinion. *The Journal of Finance, 32*(4), 1151-1168.

Mintzberg, H. (2004). *Managers, not MBAs: A hard look at the soft practice of managing and management development*: Berrett-Koehler Publishers.

Mintzberg, H. (2005). Developing theory about the development of theory. *Great minds in management: The process of theory development*, 355-372.

Mitev, N. (2011). Beyond health warnings: risk, regulation, failure and the paradoxes of risk management. *Journal of Information Technology, 26*(4), 271-273. doi: Doi 10.1057/Jit.2011.15

Monteiro, E., Pollock, N., Hanseth, O., & Williams, R. (2013). From artefacts to infrastructures. *Computer supported cooperative work (CSCW), 22*(4-6), 575-607.

Monteiro, E., Pollock, N., & Williams, R. (2014). Innovation in Information Infrastructures: Introduction to the Special Issue. *Journal of the Association for Information Systems, 15*(4), IX.

Moynihan, T. (1996). An inventory of personal constructs for information systems project risk researchers. *Journal of Information Technology, 11*, 359-371.

Mumford, E. (1974). Computer systems and work design: Problems of philosophy and vision. *Personnel Review, 3*(2), 40-49.

Mumford, E. (1996). Risky ideas in the risk society. *Journal of Information Technology, 11*, 321-331.

Myers, M. D. (1997). Qualitative research in information systems. *Management Information Systems Quarterly, 21*, 241-242.

Nakatsu, R. T., & Iacovou, C. L. (2009). A comparative study of important risk factors involved in offshore and domestic outsourcing of software development projects: A two-panel Delphi study. *Information & Management, 46*(1), 57-68. doi: 10.1016/j.im.2008.11.005

Newell, S., Robertson, M., Scarbrough, H., & Swan, J. (2009). *Managing knowledge work and innovation*: Palgrave Macmillan.

Nizovtsev, D., & Cremonini, M. (2009). Risks and Benefits of Signaling Information System Characteristics to Strategic Attackers. *Journal of Management Information Systems, 26*(3), 241-274. doi: 10.2753/mis0742-1222260308

Nygaard, K., & Terje Bergo, O. (1975). The trade unions-New users of research. *Personnel Review, 4*(2), 5-10.

Nylén, D. (2015). *Digital Innovation and Changing Identities*. (PhD), Umeå University, Umeå

Orlikowski, W. J. (1991). Integrated information environment or matrix of control? The contradictory implications of information technology. *Accounting, Management and Information Technologies, 1*(1), 9-42.

Orlikowski, W. J. (1992). The duality of technology: Rethinking the concept of technology in organizations. *Organization Science, 3*(3), 398-427.

Orlikowski, W. J. (2000). Using Technology and Constituting Structures: A Practice Lens for Studying Technology in Organizations. *Organization Science, 11*(4).

Orlikowski, W. J. (2007). Sociomaterial practices: Exploring technology at work. *Organization Studies, 28*(9), 1435-1448.

Orlikowski, W. J., & Baroudi, J. J. (1991). Studying information technology in organizations: Research approaches and assumptions. *Information Systems Research, 2*(1), 1-28.

Orlikowski, W. J., & Iacono, C. S. (2001). Research commentary: Desperately seeking the "IT" in IT research—A call to theorizing the IT artifact. *Information Systems Research, 12*(2), 121-134.

Orlikowski, W. J., & Robey, D. (1991). Information technology and the structuring of organizations. *Information Systems Research, 2*(2), 143-169.

Orlikowski, W. J., & Scott, S. V. (2008). 10 Sociomateriality: Challenging the Separation of Technology, Work and Organization. *The academy of management annals, 2*(1), 433-474.

Otim, S., Dow, K. E., Grover, V., & Wong, J. A. (2012). The Impact of Information Technology Investments on Downside Risk of the Firm: Alternative Measurement of the Business Value of IT. *Journal of Management Information Systems, 29*(1), 159-194. doi: 10.2753/mis0742-1222290105

Paterson, M., & Higgs, J. (2005). Using hermeneutics as a qualitative research approach in professional practice. *The Qualitative Report, 10*(2), 339-357.

Pentland, B. T. (1995). Information systems and organizational learning: the social epistemology of organizational knowledge systems. *Accounting, Management and Information Technologies, 5*(1), 1-21.

Persson, J. S., Mathiassen, L., Boeg, J., Stenskrog Madsen, T., & Steinson, F. (2009). Managing Risks in Distributed Software Projects: An Integrative Framework. *IEEE Transactions on Engineering Management, 56*(3).

Pich, M. T., Loch, C. H., & Meyer, A. D. (2002). On uncertainty, ambiguity, and complexity in project management. *Management Science, 48*(8), 1008-1023.

Pollock, N., Williams, R., & Procter, R. (2003). Fitting standard software packages to non-standard organizations: the 'biography'of an enterprise-wide system. *Technology Analysis & Strategic Management, 15*(3), 317-332.

Power, M. (2008). Organized uncertainty: Designing a world of risk management. *OUP Catalogue.*

Rainer, R. K., Snyder, C. A., & Carr, H. H. (1991). Risk Analysis for Information Technology. *Journal of Management Information Systems, 8*(1).

Renn, O. (1992). Concepts of risk: a classification.

Renn, O. (1998a). The role of risk perception for risk management. *Reliability Engineering & System Safety, 59*(1), 49-62. doi: Doi 10.1016/S0951-8320(97)00119-1

Renn, O. (1998b). Three decades of risk research: accomplishments and new challenges. *Journal of Risk Research, 1*(1), 46-71.

Roberts, K. H. (1990). Some characteristics of one type of high reliability organization. *Organization Science, 1*(2), 160-176.

Robey, D. (1996). Research commentary: diversity in information systems research: threat, promise, and responsibility. *Information Systems Research, 7*(4), 400-408.

Robey, D., & Boudreau, M.-C. (1999). Accounting for the contradictory organizational consequences of information technology: Theoretical directions and methodological implications. *Information Systems Research, 10*(2), 167-185.

Rochlin, G. I. (Ed.). (1993). *Defining "High Reliability" Organizations in Practice: A Taxonomic Prologue.*

Rockart, J. F. (1978). Chief executives define their own data needs. *Harvard Business Review, 57*(2), 81-93.

Ropponen, J., & Lyytinen, K. (2000). Components of Software Development Risk: How to Address Them? A Project Manager Survey. *IEEE Transactions on Software Engineering, 26*(2).

Rose, J., Jones, M., & Truex, D. (2005). Socio-theoretic accounts of IS: The problem of agency. *Scandinavian Journal of Information Systems, 17*(1), 8.

Rönnbäck, L., Holmström, J., & Hanseth, O. (2007). IT-adaptation challenges in the process industry: an exploratory case study. *Industrial Management & Data Systems, 107*(9), 1276-1289.

Sambamurthy, V., Bharadwaj, A., & Grover, V. (2003). Shaping agility through digital options: Reconceptualizing the role of information technology in contemporary firms. *MIS Quarterly*, 237-263.

Sandberg, J., & Alvesson, M. (2011). Ways of constructing research questions: gap-spotting or problematization? *Organization, 18*(1), 23-44.

Sarker, S., Sarker, S., & Sidorova, A. (2006). Understanding business process change failure: An actor-network perspective. *Journal of Management Information Systems, 23*(1), 51-86.

Schatzki, T. R., Knorr-Cetina, K., & Von Savigny, E. (2001). *The practice turn in contemporary theory*: Psychology Press.

Schmidt, R., Lyytinen, K., Keil, M., & Cule, P. (2001). Identifying Software Project Risks: An International Delphi Study. *Journal of Management Information Systems, 17*(4), 5-36.

Schön, D. A. (1983). *The reflective practitioner: How professionals think in action* (Vol. 5126): Basic books.

Scott, S. V., & Perry, N. (2009). The enactment of risk categories: The role of information systems in organizing and re-organizing risk management practices in the energy industry. *Information Systems Frontiers, 14*(2), 125-141. doi: 10.1007/s10796-009-9223-7

Scott, S. V., & Wagner, E. L. (2003). Networks, negotiations, and new times: the implementation of enterprise resource planning into an academic administration. *Information and Organization, 13*(4), 285-313.

Shim, J. P., Warkentin, M., Courtney, J. F., Power, D. J., Sharda, R., & Carlsson, C. (2002). Past, present, and future of decision support technology. *Decision support systems, 33*(2), 111-126.

Smith, H. A., McKeen, J. D., & Staples, S. (2001). New Developments in Practice I: Risk Management in Information Systems: Problems and Potential. *Communications of the Association for Information Systems, 7.*

Sommer, S. C., & Loch, C. H. (2004). Selectionism and learning in projects with complexity and unforeseeable uncertainty. *Management Science, 50*(10), 1334-1347.

Star, S. L., & Ruhleder, K. (1996). Steps toward an ecology of infrastructure: Design and access for large information spaces. *Information Systems Research, 7*(1), 111-134.

Stolterman, E. (1991). Designarbetets dolda rationalitet: en studie av metodik och praktik inom systemutveckling.

Straub, D., W. (1990). Effective IS Security: An Empirical Study. *Information Systems Research, 1*(3).

Sumner, M. (2000). Risk factors in enterprise-wide/ERP projects. *Journal of Information Technology, 15*(4), 317-327. doi: 10.1080/02683960010009079

Suriadi, S., Weiß, B., Winkelmann, A., ter Hofstede, A. H., Adams, M., Conforti, R., . . . Rosemann, M. (2014). Current research in risk-aware business process management: overview, comparison, and gap analysis. *Communications of the Association for Information Systems, 34*(1), 933-984.

Symons, V., & Walsham, G. (1991). The evaluation of information systems: a critique. *The economics of information systems and software*, 71-88.

Taylor, H. (2006). Critical Risks in Outsourced IT Projects: The Intractable and the Unforseen. *Communications of the ACM, 49*(11).

Taylor, H., Artman, E., & Woelfer, J. P. (2012). Information technology project risk management: bridging the gap between research and practice. *Journal of Information Technology, 27*(1), 17-34. doi: 10.1057/jit.2011.29

Tesch, D., Kloppenborg, T. J., & Frolick, M. N. (2007). IT Project Risk Factors: The Project Management Professionals Perspective. *Journal of Computer Information Systems*(September).

Tilson, D., Lyytinen, K., & Sørensen, C. (2010). Research commentary-digital infrastructures: the missing IS research agenda. *Information Systems Research, 21*(4), 748-759.

Tsang, E. W. (2013). Case study methodology: causal explanation, contextualization, and theorizing. *Journal of international management, 19*(2), 195-202.

Tsang, E. W. (2014). Case studies and generalization in information systems research: A critical realist perspective. *The Journal of Strategic Information Systems, 23*(2), 174-186.

Vaast, E., & Walsham, G. (2009). Trans-situated learning: supporting a network of practice with an information infrastructure. *Information Systems Research, 20*(4), 547-564.

Van de Ven, A. H. (2007). *Engaged scholarship: a guide for organizational and social research: a guide for organizational and social research*: Oxford University Press.

Van de Ven, A. H., & Johnson, P. E. (2006). Knowledge for theory and practice. *Academy of Management Review, 31*(4), 802-821.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 425-478.

Verhagen, T., Meents, S., & Tan, Y.-H. (2006). Perceived risk and trust associated with purchasing at electronic marketplaces. *European Journal of Information Systems, 15*(6), 542-555. doi: 10.1057/palgrave.ejis.3000644

Vitale, M. R. (1986). The Growing Risks of Information Systems Success. *MIS Quarterly*.

Vlek, C. A. (1996). A multi-level, multi-stage and multi-attribute perspective on risk assessment, decision-making and risk control. *Risk decision and Policy, 1*(1), 9-31.

von Alan, R. H., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly, 28*(1), 75-105.

Wagner, E. L., Scott, S. V., & Galliers, R. D. (2006). The creation of 'best practice'software: Myth, reality and ethics. *Information and Organization, 16*(3), 251-275.

Wallace, L., Keil, M., & Rai, A. (2004). Understanding software project risk: a cluster analysis. *Information & Management, 42*(1), 115-125.

Walsham, G. (1995). Interpretive case studies in IS research: nature and method. *European Journal of Information Systems, 4*(2), 74-81.

Walsham, G. (1997). Actor-network theory and IS research: current status and future prospects *Information systems and qualitative research* (pp. 466-480): Springer.

Walsham, G. (2002). Cross-cultural software production and use: a structurational analysis. *MIS Quarterly*, 359-380.

Walsham, G. (2005). Agency theory: integration or a thousand flowers? *Scandinavian Journal of Information Systems, 17*(1), 11.

Walsham, G. (2006). Doing interpretive research. *European Journal of Information Systems, 15*(3), 320-330.

Wand, Y., & Weber, R. (2002). Research commentary: information systems and conceptual modeling—a research agenda. *Information Systems Research, 13*(4), 363-376.

Wasko, M. M., & Faraj, S. (2005). Why should I share? Examining social capital and knowledge contribution in electronic networks of practice. *MIS Quarterly*, 35-57.

Weber, R. (2003). Still desperately seeking the IT artifact. *MIS Quarterly, 27*(2), 183-183.

Weick, K. E. (1995). What Theory is Not, Theorizing Is. *Administrative Science Quarterly, 40*, 385-390.

Weick, K. E., & Roberts, K. H. (1993). Collective Mind in Organizations: Heedful Interrelating on Flight Decks. *Administrative Science Quarterly, 38*.

Weick, K. E., Sutcliffe, K. M., & Obstfeld, D. (2005). Organizing and the process of sensemaking. *Organization Science, 16*(4), 409-421.

Weick, K. E., Sutcliffe, K. M., & Obstfeld, D. (2008). Organizing for High-Reliability: Processes of Collective Mindfulness. In A. Boin (Ed.), *Crisis management* (Vol. III): Sage

Weill, P., Subramani, M., & Broadbent, M. (2002). Building IT infrastructure for strategic agility. *MIT Sloan Management Review. v44 i1, 57.*

Westergren, U. H. (2011). Disentangling sociomateriality: an exploration of remote monitoring systems in interorganizational networks.

Westergren, U. H., & Holmström, J. (2012). Exploring preconditions for open innovation: Value networks in industrial firms. *Information and Organization, 22*(4), 209-226.

Yin, R. K. (2013). *Case study research: Design and methods*: Sage publications.

Yoo, Y. (2010). Computing in Everyday Life: A Call for Research on Experiential Computing. *MIS Quarterly, 34*(2), 213-231.

Yoo, Y., Henfridsson, O., & Lyytinen, K. (2010). Research commentary-The new organizing logic of digital innovation: An agenda for information systems research. *Information Systems Research, 21*(4), 724-735.

Öbrand, L., Augustsson, N.-P., Holmstrom, J., & Mathiassen, L. (2012). The Emergence of Information Infrastructure Risk Management in IT Services. 4904-4913. doi: 10.1109/hicss.2012.565