Received: 16 May 2014 | Revised: 30 November 2017 | Accepted: 1 December 2017

DOI: 10.1111/isj.12178

RESEARCH ARTICLE

WILEY

The interstitiality of IT risk: An inquiry into information systems development practices

Lars Öbrand[1] | Nils-Petter Augustsson[1,2] | Lars Mathiassen[3] | Jonny Holmström[1]

[1] Swedish Center for Digital Innovation, Department of Informatics, Umeå University, Umeå, Sweden

[2] Industrial Doctoral School, Umeå University, Umeå, Sweden

[3] Georgia State University, Atlanta, GA, USA

Correspondence
Lars Öbrand, Department of Informatics, Umeå University, Umeå, Sweden.
Email: lars.obrand@umu.se

Abstract

Information systems development (ISD) has been part of the core of information systems for over 40 years. Throughout its history, the issue of risk has been closely related to ISD projects, and significant efforts have been made by researchers and practitioners to improve their quality. While important headway has been made in assessing and resolving ISD risk, the literature shows that new and salient risks emerge outside the scope of extant risk management regimes. As a consequence, organizations still struggle with leveraging new technology as projects continue to fail at almost the same rate, albeit for different reasons. Understood as the distinction between reality and possibility, risk is inherently intertwined with practice and rooted in the knowledge, goals, power, and values of specific actors in particular contexts. Hence, to understand how risks emerge, we present a longitudinal case study in which we trace the origin and locus of risks in contemporary ISD practices. We draw on these insights to theorize information technology risk as increasingly interstitial, originating from sources positioned in between established practices and therefore outside the scope of conventional risk analyses. In conclusion, we discuss interstitial risks as an important form of emergent risk with implications for both research and practice.

KEYWORDS

risk management, interstitiality, emergence, ISD

1 | INTRODUCTION

Since its advent, information technology (IT) has had a fundamental impact on the conditions for organizing (Orlikowski & Robey, 1991; Tilson, Lyytinen, & Sørensen, 2010) and become a key operational and strategic issue

for contemporary organizations. Consequently, success and failure in information systems development (ISD) has been a core concern in the information systems (IS) field throughout much of its history (Dwivedi, et al., 2015; Hassan & Mathiassen, 2017). Substantial efforts, in both research and practice, have been made to improve the ways in which IT is developed, implemented, and appropriated to achieve better results. Unfortunately, these efforts have not had the desired effect (Conboy, 2010; Lim, Sia, & Yeow, 2011). After a low point in 1994 (Standish Group Chaos Report) when only 16% of IT projects were considered successful, the situation seemed to be slowly improving. Recently, however, things have become worse. In 2009, the International Data Corporation reported that 25% of all IT projects fail outright, 20% to 25% fail to meet ROI, and up to 50% require material rework. A study conducted by KPMG in 2013 found that only 35% of IT projects consistently delivered according to stated requirements, 33% delivered on budget, and 29% on time. In 2017, KPMG reported increased failure rates, with only 29% of projects delivering to budget and 20% of them delivering on their planned benefits. A similar report by Innotas (2015) shows an increase in the number of IT professionals who reported they had failed projects, from 32% in 2013 to 55% in 2015. Other recent studies within our field tell similar tales (Bannerman, 2008; Schwalbe, 2015; Taylor, Artman, & Woelfer, 2012). There is a variation in the perception and role of risk across industries (Kim, Mithas, & Kimbrough, 2017), and for ISD organizations, identifying and managing risk seems to present a key challenge (Narayanaswamy, Grover, & Henry, 2013).

A review of the literature on risk and risk management in IS reveals a rich and diverse discourse. Although it covers a wide range of areas, phenomena, theories, tactics, and levels of analysis, it shows a historical predilection for focusing on software development projects. Indeed, more than half of the reviewed publications on risk within IS (67 of 128) concern risk in relation to software development or implementation projects, characterized by increasingly sophisticated and comprehensive checklists (Schmidt, Lyytinen, Keil, & Cule, 2001), process models (ISO31000, 2009), analytical frameworks (Persson, Mathiassen, Boeg, Stenskrog Madsen, & Steinson, 2009), and contingency models (Taylor et al., 2012). While these have had a significant impact on our ability to systematically and efficiently identify and manage ISD risks, they neglect the continuous emergence of new and salient risks outside the scope of extant risk management regimes (Carlo, Lyytinen, & Boland Jr, 2012).

The notion of emergence is by no means new to the field of IS—it has been an important part of the discourse for decades (Robey & Boudreau, 1999; Truex, Baskerville, & Klein, 1999). Still, it is only recently that attention has been paid to the issue of emergence in the IS risk discourse. Our analysis shows how these efforts share recognition of the role of complexity in addition to the traditional focus on uncertainty in relation to risk. Following this logic, risks emerge in situations where both complexity and uncertainty are high. Similarly, the literature on information infrastructure (Ciborra, Braa, & Cordella, 2000) has introduced a sociological perspective on risk, drawing on the works of Beck (1992, 1998; Beck, Giddens, & Lash, 1994) and Giddens (1990) to understand and explain the side effects. In this context, Hanseth and Ciborra (2007) argue that emergence is a consequence of the increasingly infrastructural character and use of technology because this leads to complexity and uncertainty—both intimately connected to risk. In the same vein, the notion of systemic risk has gained traction over the last 10 years (Hu, Zhao, Hua, & Wong, 2012) as a way of explaining why risks emerge in socio-technical contexts.

The practice of ISD is becoming increasingly distributed (Sarker & Sarker, 2017), diverse (Bergvall-Kåreborn & Howcroft, 2014; Ramasubbu, Bharadwaj, & Tayi, 2015), and characterized by multiple actors with divergent but interacting spheres of interest, knowledge, and authority (Baskerville & Pries-Heje, 2004; Kautz, Madsen, & Nørbjerg, 2007; Markus & Mao, 2004), and studies have shown how ISD practice has developed, driven by structural and rapid technological changes. As a result of 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). Consequently, because contemporary ISD practice involves increasing numbers of stakeholders such as developers, users, managers, and investors, it is governed through polycentric arrangements involving independent but related authority spheres such as platform owners, service providers, customers, and government agencies (Constantinides & Barrett, 2014). As such, ISD exhibits all

the hallmarks of high complexity and uncertainty (Kudaravalli, Faraj, & Johnson, 2017; Windeler, Maruping, & Venkatesh, 2017).

In defining risk as "the distinction between reality and possibility," Renn (1998) highlights the consequentiality of human activities in the production of both reality and possibility. Furthermore, he emphasizes that risk is inherently rooted in practice, produced in part by the knowledge, goals, power, and values of different actors in specific contexts. He also notes how "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) and constructed meanings with respect to these events, and to abstract notions" (p. 61). To investigate how risks are implicated in ISD, we must therefore examine ISD practices with a particular focus on the intrinsic interplay between social context and technological manifestations.

Against this backdrop, we present a longitudinal case study of the development, support, and sales of an increasingly integrated IT services at *ISD-org* (pseudonym), a global consultancy firm, to investigate the following research question: *How do risks emerge in the development of complex information technology services*? To uncover the origin and locus of IT risk emergence, we focus on the everyday practices of ISD professionals and the structural conditions at ISD-org over a 10-year period. A key finding is that salient risks emerged interstitially at ISD-org. More commonly used in medicine and physics, the term interstitiality refers to the space between established structures or bodies. Here, we use it to theorize how the origin and locus of IT risks moved as the technology changed, from being located within practices, services, and projects to the spaces between them. This led to new insights into the area of ISD risk, with implications for both research and practice.

1.1 | ISD risk

Risk management is considered fundamental to project performance (Kutsch, Denyer, Hall, & Lee-Kelley, 2013), and the discourse on risk and risk management within IS research has evolved over more than 4 decades. The earliest works 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 theoretical approaches and diverse in both methodological choices and studied phenomena. Research relating to ISD has consistently formed a stable core of the discourse (Alter & Ginzberg, 1978; Bannerman, 2008; Boehm, 1989; Charette, 1989; Currie, 1998; Keil, Tiwana, & Bush, 2002; Lyytinen, Mathiassen, & Ropponen, 1996; McFarlan, 1981; Persson et al., 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. As a result, research on risk in IS encompasses a great richness of conceptualizations and theories. 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 behavioural (March & Shapira, 1987). While many analyses have been conducted at the project level, studies conducted at the organizational (Dhillon & Backhouse, 1996), interorganizational (Aron, Clemons, & Reddi, 2005), and even societal (Mumford, 1996) levels have also been reported. Complementing the extensive research on software development projects are investigations of risk related to various other phenomena and areas, such as outsourcing (Aubert, Patry, & Rivard, 2005; Bahli & Rivard, 2003), enterprise resource planning (Aloini, Dulmin, & Mininno, 2007; Sumner, 2000), security (Cremonini & Nizovtsev, 2010; Straub, 1990), knowledge management (Alhawari, Karadsheh, Talet, & Mansour, 2012; Massingham, 2010), and IT investment (Otim, Dow, Grover, & Wong, 2012). However, the bulk of the reviewed publications (67 of 128) concern ISD. This is also reflected in previous literature reviews summarizing the discourse on ISD risk (Bannerman, 2008; Ciborra, 2004; Lyytinen et al., 1996; Taylor et al., 2012).

Our literature review yielded several insights. First, the most prevalent approaches in ISD risk management are standardized checklists of project-level risk factors, building on a monolithic view of risk from the perspective of individuals such as project leaders. By assuming that individual risks can be generalized across contexts, analyses of such lists have contributed significantly to practice by revealing common ISD risks (Alter & Ginzberg, 1978;

Boehm, 1989; Gemino, Reich, & Sauer, 2007; Schmidt et al., 2001; Tesch, Kloppenborg, & Frolick, 2007). At the same time, this approach has been criticized for shaping the attention of risk managers in ways that increase the likelihood of overlooking potential risks absent from the list (Keil, Li, Mathiassen, & Zheng, 2008; Lyytinen et al., 1998), and for offering little guidance as to which list should be used in specific situations (Bannerman, 2008). These efforts view risk in terms of uncertainty, on the basis of the idea that risk managers can obtain sufficient knowledge for both risk assessment and risk resolution at the start of a project. As such, they cannot account for risk emergence.

Second, situated approaches offer an alternative way of thinking about risk. Both process and nonprocess frameworks are common in the literature. Process frameworks usually prescribe a stepwise sequence of actions in relation to risk assessment and resolution (eg, ISO31000, 2009). Nonprocess frameworks focus on aggregated risk categories on the basis of sources of risk (Huang, Chang, Li, & Lin, 2004; McFarlan, 1981; Persson et al., 2009; Ropponen & Lyytinen, 2000) rather than on specific risks and require risk managers to account for the specifics of their situation. Like contingency approaches (Barki, Rivard, & Talbot, 2001; Ghobadi & Mathiassen, 2016; Mathiassen, Tuunanen, Saarinen, & Rossi, 2007; McFarlan, 1981; Taylor et al., 2012), these frameworks recognize emergence to the extent that they offer decision support for risk managers as events unfold. Still, these situated approaches build on the same basic notion of risk as the standardized approaches, ie, they treat risk as a form of uncertainty. In relation to Renn's (1998) definition of risk, they emphasize "possibility," directing risk managers' attention towards certain sources, characteristics, and specific risks commonly occurring in ISD projects. However, they only indirectly address "reality" and do not account for the role and nature of technology.

Third, and in keeping with the general trajectory of the IS field, there have been recent attempts to account for the impact of increasing complexity on issues of risk. Information infrastructure theorists have adopted a sociological notion of risk on the basis of the work of Beck (1992, 1998) and Giddens (1990) to describe the logic and evolution of control and change in complex socio-technical contexts. Hsu, Backhouse, and Silva (2014) build on the work of Giddens to analyse operational risk management. Scott and Perry (2009) draw on practice theory to investigate how risk management is enacted. Finally, 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., 2012; Carlo, Lyytinen, & Boland, 2004; Hu et al., 2012). In addition, an alternative conceptualization of risk has been introduced into the IS discourse through work on information infrastructure theory (Blechar & Hanseth, 2007; Ciborra et al., 2000; Hanseth, Ciborra, & Braa, 2001; Hanseth, Monteiro, & Hatling, 1996). This body of work largely builds on a notion of risk developed by Beck (1992; Beck et al., 1994) and Giddens (1999) in their research on reflexive modernization as a way to characterize and explain the dynamics of contemporary society. At the core of Beck's argument is the assumption that the world is becoming increasingly unpredictable and unmanageable because of the development and use of complex technology and organizational forms. In this context, the dynamics of change are understood as consequences of unintended side effects. Side effects are effects that propagate through multiple layers of a complex system and are ultimately reflected back onto the thing that triggered them, either directly or by changing the conditions in a way that calls the initial action into question (Beck, Bonss, & Lau, 2003). Research on information infrastructure (Blechar & Hanseth, 2007; Ciborra et al., 2000; Hanseth et al., 2001) has thus shown how technology intended to increase control has had the side effect of reducing it.

Similarly, the notion of systemic risk (Carlo et al., 2004; Hu et al., 2012) has been advanced as a way of addressing issues of risk emergence based on the relationship between risk and complexity. Systemic risk refers to risks that cascade through interconnected parts of a network—ie, when failure in one part of a system triggers failure in other parts. The main difference between the notion of systemic risk and that of side effects is the nature of the source: While both notions build on the idea of risks cascading through multiple interconnected layers, systemic risk starts with a failure whereas side effects can come from any action. Put differently, systemic risk refers to the process of how risks propagate outwards through networks, while side effects relate to the way actions trigger effects that ultimately reflect back on their source. As such, side effects do not necessarily create risks or become risky in other layers or parts of the system or network.

Both side effects and systemic risk can be seen as comments on the changing nature of ISD reality because they build on ideas about how the character of technology has changed and thereby increased the likelihood of emergent risks. Both approaches reflect the general movement within IS towards recognizing emergence as a salient feature of IT use and have thus opened up the risk discourse in important ways. In this paper, we extend these contributions to explaining IT risk emergence on the basis of a detailed and empirically grounded longitudinal study of how emergent risks are managed in a contemporary ISD context.

1.2 | ISD practice

Understanding risk as "the distinction between reality and possibility" (Renn, 1998) implies that we must consider both realms and their relationship to understand and explain how risks emerge in an ISD setting. First, philosophers have debated the notion of reality and its nature for as long as they have been around. However, certain aspects of reality stand out as more important than others in the context of IT risk and ISD—in particular, notions of technology, agency, and structures. The organizational consequences of IT are a long-standing 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 technology. As such, IT risks result from and can be managed by specific agencies that are intended to shape the use of IT as part of the ongoing structuring of organizations.

In this paper, we position our ontological assumptions within the emergent perspective on causal agency (Markus & Robey, 1988), meaning that we understand organizational change as an effect of forces that simultaneously promote and oppose social change as reflected in information infrastructure theory (Hanseth & Braa, 1998), structuration theory (Orlikowski, 1992), actor-network theory (Walthsam, 1997), sociomateriality (Leonardi, 2012), and practice theory (Feldman & Orlikowski, 2011). Building on the emergent perspective, we view digitalization as a driving force that changes the foundations of all aspects of organizational life (Brynjolfsson & Saunders, 2010; Tilson et al., 2010; Yoo, Henfridsson, & Lyytinen, 2010). This change in the fabric of reality has made ISD practices increasingly complex (Baskerville, Ramesh, Levine, Pries-Heje, & Slaughter, 2003; Lyytinen & Robey, 1999; Lyytinen, Rose, & Yoo, 2010) as increased processing power and higher storage and transmission capacities have tied together systems, actors, and functions within and across organizational boundaries (Hanseth & Lyytinen, 2010).

The context of ISD is also characterized by constant adaptations to turbulent environments (Holmberg & Mathiassen, 2001) as green field development of single, isolated systems sold and maintained as products has transitioned to adaptation of standardized software solutions and software service provisioning (Syed, Barqawi, & Mathiassen, 2017) and platform-based development by third-party developers (Bergvall-Kåreborn & Howcroft, 2014). The installed base of standards, practices, and technologies to which new technology must be adapted during development and implementation is increasingly heterogeneous, interconnected, and deeply embedded, both socially and technologically (Tilson et al., 2010). Moreover, ISD increasingly operates in hypercompetitive markets introduced by the internet boom (Lyytinen et al., 2010), where the ability to cope with rapid change is essential (Baskerville et al., 2003; Pries-Heje, Baskerville, Levine, & Ramesh, 2004). At the same time, the move from product orientation to a service-dominant logic (Mathiassen & Sørensen, 2008; Barqawi, Syed, & Mathiassen, 2016) has significantly affected the way ISD organizations operate and are structured. Information systems development has therefore become increasingly polycentric (Constantinides & Barrett, 2014), with control being continuously negotiated between multiple spheres of authority including platform owners, service providers, customers, and government agencies. Moreover, control is multivocal (Bernardi, 2009) because ISD processes involve many different interdependent practices and stakeholders, each with their own knowledge, goals, and needs (Markus & Mao, 2004) with new levels of complexity across projects as a result (Kang, Hahn, & De, 2017).

Second, there is the notion of possibility—which includes both what we think will happen and what will actually happen. This distinction is significant in several ways: (1) It separates "reality" from our interpretations of it; (2) it highlights the notion of knowledge as the foundation of our assumptions about the world and how it works; (3) it recognizes our ability to be imaginative based on our knowledge; (4) it stresses the importance of our values and goals as

they guide our decisions; (5) it makes risk fundamentally related to the perspective of the risk identifier; and (6) it emphasizes the importance of authority with regard to which interpretations will be prioritized and whether they can be acted upon. Risk is thus highly pragmatic, rooted in the knowledge, goals, power, and values of specific actors and connected to their decisions about future actions in particular contexts.

Practice theory is useful for addressing the "possibility" aspect of risk because it offers a way to chart changes in "reality" through longitudinal studies that trace the interplay between reality and possibility. Practice approaches have recently made inroads into IS research (eg, Leonardi & Barley, 2010; Orlikowski, 2007; Schultze & Orlikowski, 2004) and have become important in management and organization studies in general (Newell, Robertson, Scarbrough, & Swan, 2009). For example, Marabelli and Newell (2012) revealed how conventional views of knowledge in the literature are inconsistent with knowledge management practices. As contemporary organizing is increasingly performed in uncertain, novel, and indeterminate circumstances, practice approaches offer powerful analytical tools to investigate organizational dynamics and complexities (Feldman & Orlikowski, 2011). Practice approaches have also been used previously to explore the design and implementation of infrastructures (Kuk & Janssen, 2013). There is no "one true" practice theory (Feldman & Orlikowski, 2011; Marabelli & Newell, 2012); instead, practice theory can be seen as an umbrella term encompassing a range of theories for investigating "specific instances of situated action and the social world in which the action takes place" (Feldman & Orlikowski, 2011, p. 1241).

Against this backdrop, we use a practice lens to investigate how risks emerged in the development of a complex IT service. We pay particular attention to the technology being developed, and the actions taken by individual actors, including how, where, and why they acted, as well as the organizational context in which their actions were taken. As such, we understand practice as "the coordinated activities of individuals and groups in doing their 'real work' as it is informed by a particular organizational context" (Cook & Brown, 1999, p. 386).

2 | RESEARCH METHOD

We adopted a qualitative methodology to gain a detailed understanding of the development of a complex and dynamic character within an information infrastructure service (Benbasat, Goldstein, & Mead, 1987; Walsham, 1993; Yin, 2013). To investigate the emergence of IT risks in this context, we adopted a process perspective (Newman & Robey, 1992; Pettigrew, 1997). This allowed us to focus on the sequence of events that occurred over time and to explain how and why certain outcomes were reached. Adopting a practice approach, we traced everyday information infrastructure practices at ISD-org, focusing on their constituting activities and conditioning structures over a 10-year period. Data were gathered through interviews, document analysis, and participatory observations by an insider-researcher (the second author).

2.1 | Research site

ISD-org is a global IT consultancy firm delivering IT services such as process consulting, systems integration, and outsourcing services based on customer requirements and billable hours. During the studied period, external customers were charged significantly higher hourly rates than were internal ISD-org customers. ISD-org offices operated locally with external customers while also participating in the organization's general service deliveries. All projects were required to use a standard risk management model (Predictive Risk Model (PRM); see Figure 1) focused on 4 processes: general business management processes (including sales, delivery, support, and improvement), information security review, financial review, and technical review. The PRM focuses primarily on financial risks to help determine a project's price tag. The greater the financial risk for ISD-org, the higher the price.

2.2 | Data collection

We first made contact with ISD-org in 2005, when the second author was employed by the firm. From 2009 to 2014, he acted as an insider-researcher as active member of an industrial PhD program. This approach afforded rich

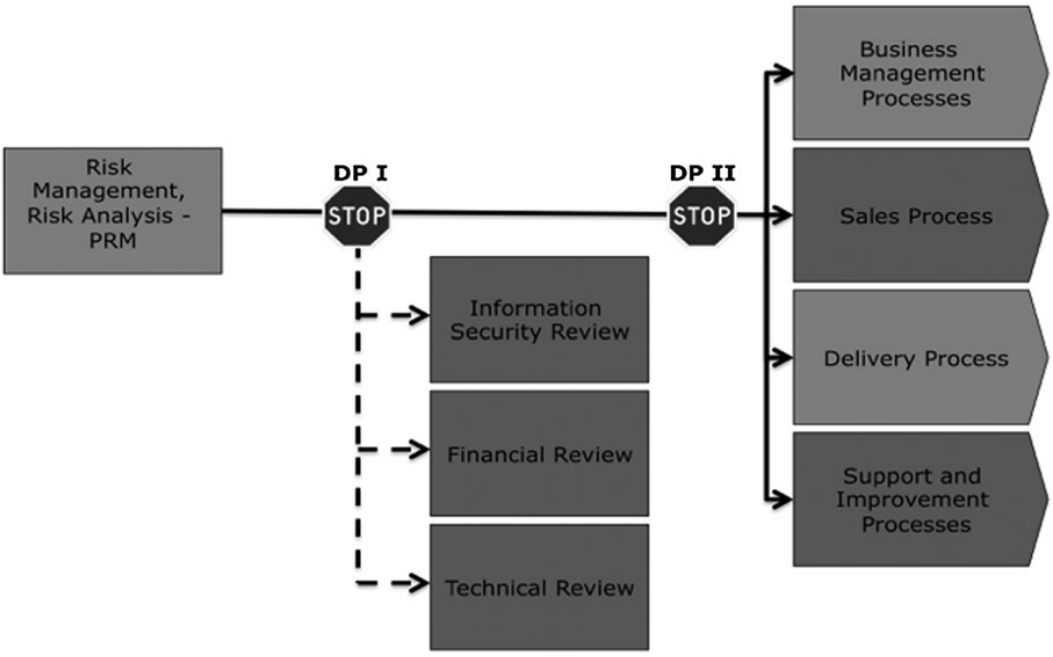

FIGURE 1 The standard risk management model used at ISD-org

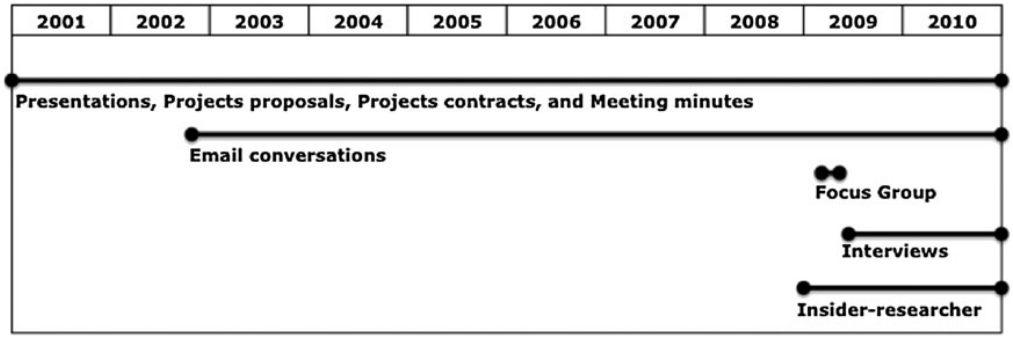

FIGURE 2 Overview of data sources used during the studied period

access to relevant data sources (Coghlan & Brannick, 2014) and created an opportunity to obtain a detailed understanding of the intricacies and nuances of the empirical setting (Adler & Adler, 1994). Moreover, ISD-org provided access to multiple data sources on the basis of purposeful sampling (Patton, 2002; Yin, 2013). As noted by Pettigrew (1997), such rich access is especially relevant for longitudinal process studies. To ensure the credibility of our insider-researcher approach (Unluer, 2012), it is important to state that the second author worked as a project and maintenance manager in the team central to this study. As such, he was a native of the group being studied and familiar with the organization as a whole. To mitigate the risk of bias, we triangulated using several different data collection techniques and sources (Figure 2 and Table 1). Furthermore, the insider-researcher did not conduct any of the interviews.

First, a focus group was conducted with 4 key actors: the 3 core team members (the architect, developer, and project manager) and the head of their ISD-org office. An outsider-researcher (the third author) acted as the moderator. The topic was "challenges and risks related to ISD." In addition, we used qualitative interviews (Mason, 2002) to generate data related to risk identification and risk management strategies. Three rounds of interviews were conducted during 2009 and 2010. The first round concentrated on the period from the initiation of the infrastructure project to 2009. The second round focused on follow-ups as new questions were raised by the initial data analysis. The third round centred on events that had occurred since the first round. The aim was to generate data regarding risks, risk management practices, team practices, and interrelated ISD practices more generally as they played out over

TABLE 1 Data sources

Data Sources	Description	Use of Data
Focus group	One focus group session with 4 key actors, the insider-researcher, and one outsider-researcher (moderator). The session was recorded and transcribed.	We used the transcripts to identify key events and major challenges connected to risk management in the context of ISD-org.
Qualitative interviews	Eleven interviews lasting approximately 1 h each. The interviews were recorded and transcribed.	We used these data as the primary source for analysing risk and risk management, as well as other aspects of practice related to the research question.
Participant observation	The insider-researcher's daily informal discussions concerning ISD services.	These data complemented data from the focus group and the interviews and provided an in-depth source of data on contextual backgrounds, structural conditions, and everyday risks and challenges in the firm's ISD practices.
Projects proposals	Ten proposals from the period, including approved and rejected proposals.	We used these data to chart the changing nature of technology over time, to corroborate data from the interviews, and to provide detailed descriptions of, eg, functionality.
Project contracts	Six project contracts.	We used these data to chart changes in formal arrangements and trace changes in the nature of technology.
Meeting minutes	Formal minutes from monthly and weekly meetings within the management group and internal team, totalling nearly 200 meeting minutes.	We used these data to trace risk identification and risk resolution actions throughout the timespan of our study. They also provided detail concerning when and how internal, customers, and exogenous actors and practices related to the team's ISD efforts.
Email conversations	Email conversations between the project and maintenance manager (insider-researcher) and internal and external stakeholders during the period, totalling over 1100 emails.	We used these data to trace relationships between actors within and across practices.
Presentations	The various presentations used to describe the technology service to internal and external stakeholders during this period, totalling close to 40 presentations.	We used these data to analyse how the technology's character changed over time, to identify changes in stakeholders related to the ISD practice, and to trace changes in the kinds of service the technology afforded.

Abbreviation: ISD, information systems development.

time. Because the data were mostly retrospective, we analysed project proposals, project contracts, meeting minutes, presentations, and email conversations to corroborate and substantiate team member narratives (Table 2). This documentation included specifics about the content of change, eg, characteristics of the technology. The insider-researcher was the main data source for the context of the changes.

2.3 | Data analysis

We conducted data analysis in stages. First, we performed an open coding procedure where the insider-researcher and an outsider-researcher (Coghlan & Brannick, 2014) independently coded the empirical data. The interviews were the point of departure, but all results were verified against the written documentation. The following coding steps were taken:

1. The first round of interviews and the focus group session were transcribed and entered into Atlas TI together with other documentation.
2. The data were arranged chronologically to establish a timeline.

TABLE 2 Coding scheme

Category	Subcategories	Code Examples
Context	Structure	Project, hierarchy
	Financing	Consultancy, team resources
	Stakeholders	Internal customer, external customer
	Technology	Competing technology
	Events	Economic downturn
Technology	Functionality	Administration, configurability
	Level of integration	Stand alone, standardized
	Architecture	Idiosyncratic, modularized
	Infrastructure	Standards, compatibility
Practice	Objective	Sales, maintenance, marketing
	Routines	Development method, coordination
	Structure	Collaborative, division of labour
	Scope	Authority, team role
	Practitioners	IT architect, project manager
	Knowledge	Formal, informal, tacit
	Actions	Sales meeting, requirements engineering
Risk	Risk identification	Objectives, risk cause, knowledge
	Risk treatment	Standardization, modularization
	Unidentified risks	Stakeholder decisions, knowledge management

Abbreviation: IT, information technology.

3. Transcripts were analysed and coded using 4 categories of codes building on our practice approach and theoretical framing: context, technology, practice, and risk.
4. Subsequently, each category was coded in detail using the subcategories in Table 2.
5. The insider-researcher and one of the outsider-researchers iteratively coded and discussed the events that occurred over the observed period to identify specific and meaningful codes.
6. The analysis formed the foundation for the second and third interview rounds, which focused on collecting data that would allow us to analyse blind spots in the first data set relating to the research question and the insights from the first round of analysis.
7. These transcripts were coded using the scheme developed in the first sequence.
8. The insider-researcher and one of the outsider-researchers independently coded the transcripts with respect to subcategories for each outcome. These subcategories were discussed, and the final number of instantiations of our analytical framework was agreed by merging or separating codes as required.

We conducted 3 rounds of data analysis. The first round was exploratory and consisted of the aforementioned steps 1 to 5. These 5 steps generated significant insights into how the technology had developed over the years, how the team had identified and managed what they remembered as significant risks, and how their way of performing their everyday work had changed. This first round of analysis allowed us to identify 3 distinct phases on the basis of the shifting character of the technology. After analysing the other data sources, we had an overall view of the technology, practices, and risks connected to ISD but lacked detail; we needed specifics regarding stakeholder changes, structural changes, and in the particularities of the evolving practices. The second round of analysis and additional interviews therefore focused much more on specifics and the details of IT risks and risk management across the 3 phases, in contrast to the broader focus and more exploratory approach of the first round. The coding in the second round followed the same logic as in the first round, but the new data (and insights from the first round) affected our analytical subcategories. The coding scheme developed during the second round is depicted below. After the first 2 rounds, some time had passed, and the ISD team had continued their work. We therefore conducted a third round of interviews to gather data on events and decisions taken during this period. The third round of analysis

and follow-up interviews therefore focused on the 2 years that had passed since the second round. We applied the coding scheme developed during the second round. In this round, we also discussed our first 2 rounds of analysis with key stakeholders at ISD-org, allowing us to rectify some small mistakes and obtain additional insights into previously discussed issues.

3 | RESULTS

We describe how risks were implicated in the development of the studied information infrastructure service at ISD-org over a 10-year period. We detail the key supplier practices related to the development of technology and provisioning of the service, along with the key risks and risk management approaches used by the practitioners. The 10-year period is presented in 3 phases: developing systems, developing a platform, and growing a digital infrastructure. These phases are distinct in terms of the character of the technology, the related ISD practices, and the implicated risks.

3.1 | Developing systems (2001-2004)

In early 2001, *FinanceCorp* approached ISD-org with a very specific request. FinanceCorp was a rapidly growing organization whose growth was primarily due to acquisitions. Consequently, it needed a system to manage inventory and user accounts in terms of information, system, and process rights. At the time, no suitable tools were readily available, so the local ISD-org office allocated 2 of their 10 consultants to develop a web-based network management system, Alpha, for FinanceCorp. Alpha was developed collaboratively on-site using a beta version of Microsoft's .Net environment. It was locally hosted by FinanceCorp, and no maintenance agreement was signed. The unit manager at ISD-org described the initial period as follows: "We had a solution, and we were partially financed by the customers. We partially financed it ourselves simply because we saw that this was an area where there was a great need and a possibility for us to develop expertise […] If we could develop a solution for this customer and retain the rights to the code, we could reuse it." During the implementation of Alpha, FinanceCorp was bought by another organization, and the requirements changed to include email administration through integration with MS Exchange. Further functionality was added in response to new developments and increased integration of the network technology targeted by Alpha. Alpha was subsequently sold to 5 different customers, in each case as a unique installation that was locally hosted and customized to the specific customer context and requirements. With each new installation, however, the team strove to keep the code base as generic as possible to minimize maintenance costs. Keeping the code base generic also facilitated future market expansion.

In this phase, there were 3 different, albeit interrelated, practices related to the platform—development, support, and sales. A small team of 2 developers was responsible for *development*, working on-site in close collaboration with the customer. This included all aspects of the development cycle: requirements analysis, customization, installation, and support. With each new project, the team focused on understanding the idiosyncrasies of the customer organization's business practices, thereby increasing the challenge of retaining a generic code base. Influenced by FinanceCorp's ideas of Alpha's potential use, ISD-org cofinanced its development to secure ownership of the code base, a precondition for developing Alpha as a platform rather than a one-off solution. While the FinanceCorp project was a joint venture, the next 4 customers paid for their own solution, and the continued development of the code base was based on the small team's resources because code base ownership was at odds with ISD-org's strategy as consultancy firm: "I was the solution manager, so I designed the solution. The whole time we've had this [standardization] in front of us, because we know that we would never get the support from our organization to develop something like this" (team architect).

There was no clear boundary between development and *support*, and because no maintenance agreements were signed, the team provided customer-driven, ad hoc, support for the installations, on the basis of time and material

contracts. In addition, the team needed to engage in *sales* to both internal and external customers owing to a recession in the Swedish economy (2000-2002). The team members risked losing their jobs unless the sale of Alpha was successful because ISD-org was downsizing throughout the organization. Consequently, during the 2 years after the FinanceCorp installation, the team focused locally on face-to-face meetings with potential customers. They also marketed Alpha nationally within ISD-org to promote the use of Alpha in ISD-org projects outside the local region. The successful sale of Alpha during this phase ensured that the team members avoided layoffs. The marketing effort within ISD-org gave the team opportunities to share the technical and organizational knowledge generated through the development, support, and installation of Alpha with other ISD-org practices. It also allowed them to establish contacts and develop an understanding of how other areas within ISD-org operated.

Throughout this phase, the team members identified several risks. During the initial development of Alpha, the main risk was *immature technology*: There were no pre-existing or competing technologies, and no readily available way to meet customer requirements. Consequently, the team had to acquire knowledge about FinanceCorp's organizational needs and the network technology on which Alpha was based. Because of ISD-org's strategy as a consultancy firm, the team also had *limited resources* to develop the platform; as one team developer put it, "We are consultants and we are supposed to charge for each hour of work that we do for customers […] It messes things up, that we are not a product company that has a budget." In each project, customer requirements had to be negotiated against the team's platform building strategy, so they ran the risk of *insufficient customization* of the platform because of their long-term strategy of consolidating a generic code base. Beyond these organizational and technical risks, the team faced the risk of being *discontinued* because both members could be transferred to other assignments at any time, and because as the most junior consultants in the office, they were first in line for redundancy. As it turned out—thanks to their successful development and sale of Alpha—both team members stayed on board while more senior consultants were laid off.

During the first project with FinanceCorp, the PRM risk management model (Figure 1) highlighted a number of risks and helped the 2 developers, who were both junior consultants at the time, to implement basic project management disciplines. The team's internal and external sales efforts helped address other risks. As Alpha was developed, they identified markets beyond smaller, local companies by looking at ISD-org's internal processes and service production as a gateway to large customers outside the region. This exploration across internal boundaries had a significant impact on the trajectory of the information infrastructure. Finally, the team's development strategy afforded opportunities to cater to both the requirements of different customers and their own requirement to build a sustainable platform. "Throughout, we've had the same basic idea of recycling, that we are able to use the work already performed in one organization in another without us having to re-do everything. I have no doubt: this is the single most important reason for the success we have had" (team architect). Because the team was in control of both customer projects and the code base, they could influence the convergence of the dual requirement sets.

3.2 | Developing a platform (2004-2008)

In 2004, the internal marketing efforts paid off, and Beta, a customized version of Alpha, was requested by ISD-org's service production—the channel through which day-to-day ISD-org services were produced for external customers. Compared with Alpha, Beta had increased connectivity to support network management of multiple data sources but scaled down functionality to align with ISD-org's service production infrastructure. Unlike Alpha, Beta was centrally hosted by ISD-org and customizable for multiple concurrent customers. "When we started working on a proposal for ISD-org service production, we realized immediately that the hard coded configuration approach of Alpha was not going to work as we were supposed to manage 15 to 20 customers at the same time […] We needed to develop something that made configurations less expensive and required less work" (team architect). The central hosting of Beta was made possible to use the existing infrastructure for ISD-org's service delivery as the gateway to external customers. During this phase, 17 external customers either purchased new configurations of Beta or migrated to Beta from other network management systems. This growth highlighted the need to increase Beta's

functionality to meet customer demands. However, although the team developed Beta accordingly, ISD-org's service production relied on a conservative strategy without adding the new functionality.

In 2006, the team decided to develop a new version of Alpha, Gamma, prompted by an external technological shift in which the network provider moved towards a more generic and integrated platform. Gamma included extended network management functionality and increased connectivity. Unlike Alpha, Gamma was modularized, allowing for standardization and more efficient configuration. Its development was also an attempt to address the customers' changing needs. Drawing on knowledge and experience gained while working on Beta, the team recognized some customer demands that were not met by ISD-org's service: "We shifted focus from expert users to end users, from administrative functions to configurability […] to support organizational processes rather than administrators. This was a way of keeping costs down and of differentiating us from other solutions that already had larger customer bases" (team architect). Gamma was hosted by the team, and, during this phase, 4 external customers were enrolled and supported. The Alpha installations from previous years remained active, and, together with Beta and Gamma, the 3 versions were shared across multiple community boundaries and kept open for new components to afford opportunities for customization to a wide variety of contexts. Consequently, the 3 information infrastructure versions were heterogeneous, spanning boundaries of user communities, governance structures, operators, and operations.

During this phase, the information infrastructure was affected by *practices* outside development, support, and sales. The introduction of Beta increased the importance of ISD-org's service production practices and sales practices at the central level. The *development* practice changed because of the boundary between the team and end customers; consequently, the team had to rely on second-hand knowledge of contexts and requirements. Beta was developed as an infrastructure component of ISD-org's service production, in close collaboration with the internal customer. This increased the complexity of its development because there were 3 different sets of requirements: those of ISD-org's service production, those of external customers as filtered through ISD-org's service production, and the team's own requirement to keep the information infrastructure code base sustainable. In 2005, the scope of the information infrastructure had grown, and, as a consequence, the team's organization was formalized and a new team member was added. Three team roles were defined—architect, developer, and project manager—to cope with the increasing development and support workload. This helped with managing the important relationship between the team and ISD-org's service production. The initial development of Gamma was financed by the local ISD-org office. Although this decision was at odds with ISD-org's principles, the office made a strategic investment choice: "We have certain possibilities for investments, but we are not supposed to take on any financial risk […] The office had grown and the circumstances were better than a few years earlier. Even though we are a consultancy firm, there are ways of creating opportunities like this. It is also a matter of creating a profile for ourselves within ISD-org. But, by and large, we can only make these shifts within the scope of larger delivery projects, so it's a matter of timing as well" (office manager).

The conditions relating to *support* and *sales* also changed and affected infrastructure practices. While Alpha customers were still supported on the basis of informal time and material contracts, maintenance agreements had been signed for Beta, and a maintenance manager was appointed. A team member also worked across boundaries for 2 years, assigned to ISD-org's general service line to support Beta. "The opportunity for me to work on the general service line gave us, as a group, access to a new internal network, and we also became much more involved in the dialogue with the external clients regarding changes and configuration" (team project manager). The team wanted to sign maintenance agreements with all Gamma customers but only succeeded with one customer. In one case, the support of customer-defined functionality was outsourced to another ISD-org office. To reduce costs, the general support line for Gamma was provided by ISD-org's offshore unit in India. The defined roles helped the team focus its efforts and manage its increasingly important relationship with ISD-org's service production. There were ongoing discussions about replacing Beta with Gamma as part of a redevelopment of ISD-org's service. There was also a focus on external sales meetings because external customers paid significantly more per hour than did ISD-org's internal customers. ISD-org's central sales became an important facilitator for the sale of Gamma, and a downturn in the economy created pressure on the team to participate in local ISD-org offices' sales initiatives. This created a boundary between sales and development. "We kind of lost touch with the end customer; instead, the architect and the project

manager participated in sales meetings, trying to gather as much information as possible. Let's just say that they didn't bring a lot of documentation back […] This made everything more difficult in terms of development" (team developer). During this phase, ISD-org's service production practices, including service sales and service development, were increasingly important, not only for Beta but also for the whole information infrastructure. Although the team had a heavy workload managing the many customers of Alpha, Beta, and Gamma, they also had to engage in 2 new local ISD-org projects that were independent of the information infrastructure.

The risks identified by the team members shifted during this phase. In the case of Beta, balancing *the dual requirements* of infrastructure sustainability and ISD-org service production was increasingly difficult because the team had no direct relationship with the end customer whose processes Beta supported. The way ISD-org's service production viewed Beta also affected the potential for efficient infrastructure management by the team because for new functionality to have any effect on the end customers, the ISD-org services needed to be developed as well. Within ISD-org, there were other *competing technologies*, both for internal use and for the external customers of ISD-org's service production, as well as boundaries between conflicting goals of ISD-org units. This *organizational protectionism* was an important risk during the efforts to establish Beta and when subsequently advocating for the integration of Gamma into ISD-org's service production. "It became a threat internally as well, and that's one of the reasons we keep running into opposition. People see this as a potential threat to those working in service production because we can automate what now is done manually […] It becomes really important who you talk to in the organization" (team architect). The team's sustainability also depended on *the market scope*: It needed Gamma (and Alpha, to some extent) to reach a wider market of external customers because internal sales yielded significantly lower rates than did external ones.

Even though it was mandatory for all project proposals to go through the PRM risk management model (Figure 1), this model had little to do with the risk management strategies that the team used during this phase. Hosting Beta and Gamma centrally was vital to keep the cost of customization and configuration low. The explicit focus on standardization and customization was an important part of the team's risk management strategies, especially in terms of managing the market scope and competing technology risks. "Thanks to our focus on standardization we have had a great advantage. We can actually customize our solution while keeping the price down, no other system could do that" (team architect). Financing the initial stages of Gamma was an important part of managing the risk of multiple requirements and limited control. Knowledge about new technologies and customer demands played a significant role in finding new market niches and continuously developing the infrastructure. "We have some really hungry wolfs here […] The team architect, for example, he is always the frontrunner, eating new technologies for breakfast and always seeing the possibilities with them" (office manager).

3.3 | Growing a digital infrastructure (2008-2010)

By 2008, the information infrastructure had grown to 4 external Gamma installations in addition to those based on Beta and Alpha. Gamma now included support for centralized computer and application management, and the team saw Gamma as a potential replacement for Beta within ISD-org's service production. While Beta was an integrated part of the service delivery infrastructure at ISD-org, Gamma competed with other technologies for participation in service delivery projects. The code base was now comprehensive and allowed for customization with only minor development work as part of ISD-org's service delivery projects. During a large project in 2009, the customer requested an end-user portal in addition to the existing administrative focus. In response, the team developed Delta—an end-user interface partially decoupled from Gamma. "Gamma was part of a large project proposal, and it was very important for ISD-org to get this deal. The customer wanted certain functionality that we couldn't deliver with existing technology, and I was assigned to develop what would become Delta. There were competing technologies at the time, but nothing with the specific functionality the customer wanted" (team project manager). Delta offered customers a SharePoint-based interface in addition to the administrative interface provided by Gamma. It was locally hosted, and decoupling the interface from Gamma made it highly configurable to suit end-user preferences without the constraints of the underlying layers. Outside this project, Delta was sold to 2 external customers during this period.

The introduction of Gamma and Delta increased the number of *practices* related to the information infrastructure and affected the way the team worked on development, support, and sales. ISD-org had developed its services, and both Gamma and Delta competed with other technologies to be part of the organization's service delivery projects. The team saw Gamma as a replacement for Beta and pushed its development in that direction in every project. To ensure efficient customization and support, there was a sustained focus on modularization and standardization. In terms of functionality, the development of Gamma and Delta was based on extensive team experience and knowledge. "10-15 of ISD-org's largest customers are in Sweden—I've configured those installations, so we have a pretty good grasp of the requirements now. We have built up a knowledge base over these ten years, and we're always on the lookout for where things are heading" (team project manager). The team grew from 3 to 15 members as the number and scale of projects increased, and ISD-org's offshore team was used as an additional development resource. As a consequence, the need for coordination and task specification across boundaries grew significantly, and the control over infrastructure development declined.

The team was involved in several parallel projects in which they no longer controlled customer requirements. "We are too far away from the customer nowadays […] That makes it really hard for us […] Other people interact with the customer and it's hard for us to know what exactly we are supposed to be doing" (team developer). The development of Delta was separated from Gamma as it was seen as a high-risk project that had the potential to help ISD-org establish a new large customer. Successful sales of the infrastructure were still vital for the team and were primarily organized and implemented by the architect and the project manager as part of other engagements.

Gamma's functionality and customizability had made it the "go to" technology for ISD-org service projects. However, after successfully completing the test period in a large project that included both Gamma and Delta, Gamma was suddenly terminated by the firm's management. In an unrelated ISD-org service production project, the Service Desk at ISD-org decided to adopt a competing technology for the administration of employee information and access control. Since the Service Desk was an important part of ISD-org's service production, Gamma was in effect dropped from all ISD-org service delivery projects. However, the Delta project, despite building on the Gamma workflow and integration logic, remained unaffected.

The risks identified by the team were, to a large extent, connected to increased infrastructural complexity and team size. As the team became part of large-scale projects, they became *increasingly dependent* on other actors and subprojects for information and specifications. They also had to balance the *multiple requirements* of end customers, ISD-org's service production and service delivery projects, and the information infrastructure itself, all while depending on second-hand information about customer requirements for ISD-org service projects. As the team expanded, they identified *knowledge transfer* as a risk: "In 2008, when we began letting new developers in we kept a lot of it in our heads, so there was definitely a threshold […] I think the quality has gone down a lot. You can't blame the new developers, I mean, they didn't have any specs. They did their best. And the project manager had to focus on sales, sales, and sales. It was a difficult situation" (team developer). As the situation became increasingly complex, so did the dependence on *key members*. While the strategy for managing the increased workload of key members had been to expand the team, they had no strategies for coping with the risks resulting from the expansion. Nevertheless, to manage the growing information infrastructure and find new opportunities, the team continued with the strategy of standardization and modularization of the infrastructure components.

4 | DISCUSSION

Building on a longitudinal case study of risk emergence in IT service provisioning at ISD-org, we investigated how ISD professionals identified and managed risk. While emergence has long been established as a salient feature of IT use in the literature (Robey & Boudreau, 1999; Truex et al., 1999), it has only recently been recognized in the IS discourse on risk. Work on information infrastructure theory and the introduction of side effects (Ciborra et al., 2000; Hanseth et al., 2001; Henfridsson & Bygstad, 2013) and systemic risks (Carlo et al., 2004, 2012; Hu et al., 2012) has opened

up the discourse in important ways. Understanding risk emergence as a consequence of situated complexity and uncertainty, we traced how changes in ISD practices, technological characteristics, and structural conditions impacted the locus and origin of salient risks. We found that IT risks at ISD-org were typically *interstitial*; ie, they emerged over time and originated between established ISD practices. The longitudinal character of the study and the intimate access to data afforded by the insider-researcher allowed us to explore in detail the emergence of risks and the origin of their emergence, ie, how they moved from being primarily immersed within practices to being primarily interstitial in nature. This revelation of IT risk emergence as interstitial extends the literature by detailing how the origin and locus of salient risk changes as a result of the interplay between practice, the nature of technology, and structural conditions.

Our findings demonstrate how 3 general types of practices interacted to shape the evolution of the information infrastructure and the associated risk emergence: customer practices, internal practices, and exogenous practices (Figure 3). Throughout the 10 years of ISD service provisioning at ISD-org, varying levels of IT risk were introduced by the increasingly complex interplay between constituting activities and related conditioning structures. Although the nature of the relevant technology evolved significantly over the studied period, from isolated systems to platforms and digital infrastructures, the structures at ISD-org did not. At all times, projects were the primary organizational structures within the firm, and a consultancy logic dictated the funding and governance of operations. As a result, the ISD team and their practices became increasingly dependent on other types of practices. Notably, the formal risk management method offered less and less support as the situation unfolded. Consequently, during the development of Gamma and Delta, team practices became dependent not only on ISD-org service production practices, infrastructure, and end customers but also on a range of customers independent of ISD-org's service production, each with their own customized versions of Alpha, Beta, Gamma, or Delta.

Adopting a practice lens (Feldman & Orlikowski, 2011; Marabelli & Newell, 2012) helped us identify the sources, tensions, events, and interactions that caused risks to emerge. We identified 3 main types of interstitial IT risks. First, risks emerged in the interstices of different spheres of authority. Interstitial IT risks of this kind are identified by actors involved in a practice, but these actors cannot control the risks without negotiating with related practices. As the character of technology evolved from the development of isolated systems to platforms and digital infrastructures, the ISD context became increasingly polycentric (Constantinides & Barrett, 2014; Mindel & Mathiassen, 2015). The ISD-org development team therefore had less and less control over issues directly related to the risks they identified. With Beta, they lost control over the development of the code base in terms of functionality to ISD-org's central

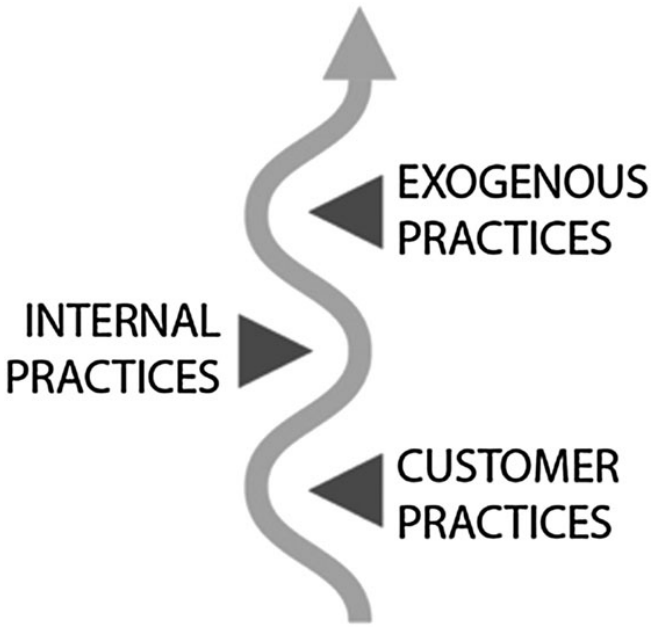

FIGURE 3 Information systems development risk forces

service production, and they were forced to develop Gamma to manage the risk of not meeting changing customer demands. Working through ISD-org's service production, they also lost control over customer requirements in the project. The team identified this as a major risk but was unable to manage it within their development practice or through negotiations with other ISD-org service production practices.

Second, risks emerged in the interstice of diverging goals or interests. Information technology risks of this kind are difficult to identify because they emerge in the blind spots between the goals of related practices. The ISD context became increasingly multivocal (Bernardi, 2009) as the number of stakeholders with different goals, needs, and knowledge grew during the different phases, increasing the levels of complexity across projects (Kang et al., 2017). For example, following their previous strategy, the team focused on end customer demands as a strategy for platform development and spent internal resources on developing a new version of the platform for the next generation of ISD-org service deliveries. However, ISD-org's service production had other goals, leading to the termination of Gamma during a large project and the selection of a competing platform for service delivery by Weilgo. The termination of Gamma created a situation where the team relied on old and insufficient knowledge of related practices and structural dynamics, making them unprepared for the way events unfolded. The decoupling of Delta from Gamma turned out to be vital for the infrastructure's survival, but ironically, it was a serendipitous consequence of ISD-org's policy of not taking on financial risks rather than the result of explicit design efforts.

Third, risks emerged in the interstices of spheres of knowledge, both lateral and temporal. This type of risk is difficult to identify and manage because both of these processes build on extant knowledge within practices. Our case shows how experienced individuals were able to bridge these gaps, but also how increased specialization, division of labour, and multiple dependent and interdependent practices increased the manifestations of such risks. ISD-org is a consultancy firm, and most of the studied work was done within the scope of projects financed by customers. From an organizational standpoint, every project was more or less regarded as an isolated entity. This was a source of risk for the long-term sustainability of the team and its technology. One associated risk related to knowledge transferability between projects. As long as the team consisted of 2 to 3 consultants, knowledge transfer was not a problem because the consultants collaborated closely and all members of the team participated in all projects and related practices. As the infrastructure grew, team roles were designed and implemented to cope with the heavier work load, and different practices (development, support, and sales) were more clearly defined. This affected knowledge transfer because the consultants became more specialized. However, it was the team's rapid growth to 15 consultants that highlighted the knowledge transfer risk. Experiences from previous projects and the shared understanding of the platform were largely not documented or formalized. This made it difficult for new team members to perform at a high level. Paradoxically, growing the team increased the workload of, and dependency on, key team members—especially since the digital infrastructure at this point was so complex. This interplay between structural conditions and practices shows how the effects of a single structural condition, ie, the project, can differ depending on practices and related structural conditions.

Our theory complements existing research by considering how information infrastructure risks emerge. Whereas previous theories explain why information infrastructure risk emerges quite well (Ciborra et al., 2000; Hanseth & Ciborra, 2007; Hanseth, Jacucci, Grisot, & Aanestad, 2006), we have shown in detail *how* it emerged at ISD-org by tracing the interplay between reality and possibility, ie, between the evolving nature of technology and the knowledge, goals, interests, and reach of interrelated ISD practices. Our study shows how the origin and locus of risk in the ISD service provider setting moved from within structures and practices to being centred on the interstices between them as the technology became increasingly interconnected and complex. The notion of interstitiality is related to both side effects and the notion of systemic risk. Even though risks can be systemic, in that a failure or risk in any part of the infrastructure can propagate to the whole (Hu et al., 2012), systemic risks do not originate in the interstices between practices or structures. Conversely, an interstitial origin does not necessarily imply that risk is systemic because it does not always propagate throughout the network of interconnected practices. Similarly, while side effects are a fundamental part of the dynamics of information infrastructure evolution (Hanseth et al., 2006), they are reflected back onto the specific actions that triggered them, which may or may not be interstitial. The notion of interstitiality relates to the specifics of the origin and locus of risk in information infrastructures and can thus help

focus the attention of both researchers and practitioners onto sources of risk not otherwise captured by current risk management methods, frameworks, or tools.

The recognition of interstitial sources of risk thus offers new insights into IT risk management theory and practice. It questions the conventional wisdom of focusing on project-level analysis and extends our understanding of the limitations of risk lists (Bannerman, 2008; Barki et al., 2001). Moreover, it calls into question the ontological assumption of risk in the IS discourse and highlights the importance of reflexivity in both research on and the practices of risk management in ISD (Mathiassen, 1998). To identify relevant risks and find novel ways of managing them, IT professionals must be reflexive, must reassess their practices and the context of those practices, must approach risk management at levels other than those of models and projects, and must actively transform knowledge from outside their own practice context. Indeed, risk management must become a primary practice in its own right for ISD risk to be effectively identified and managed.

As with any research, this work has limitations. Our single qualitative case study design limits our ability to generalize and requires careful attention to data collection and analysis. As a result, we adopted systematic data coding and analysis procedures on the basis of our analytical framework (Table 1). Also, to manage the risk of retrospective bias, we triangulated using several different techniques and sources (see Figure 2 and Table 2). However, single qualitative case studies can and should go beyond idiosyncratic insights and explanations, so we leveraged our empirical investigations to advance new perspectives on managing information infrastructures and IT-related risks (Mason, 2002; Walsham, 1995; Yin, 2013). In doing so, we have interpreted the empirical material from the perspective of information infrastructure and risk practices. However, the application of other theories (possibly drawn from the literature on IT capability and governance) could potentially have highlighted additional interesting aspects of the case.

5 | CONCLUSIONS

Risk is concerned with the effects of complexity and uncertainty on objectives or goals. Where practices intersect, multiple—often conflicting—goals are in play. This work presents a longitudinal study of IT risks as they manifested in practices related to ISD service provisioning at a large consultancy firm. Our analysis shows that as the nature of technology evolved and grew in complexity, new and important risks emerged at the interstices between different but interdependent internal, exogenous, and customer practices, and between spheres of authority, spheres of interest, and spheres of knowledge. We characterized the origin of these risks as interstitial because they manifested between practices and outside the scope of established risk management approaches. As a result, this work extends the literature on emergence in IT risk research and contemporary ISD risk research.

ORCID

Lars Öbrand http://orcid.org/0000-0003-2573-5786

REFERENCES

Adler, P. A., & Adler, P. (1994). Observational techniques. In *Handbook of qualitative research, 1* (pp. 377–392).

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.

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

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

Aron, R., Clemons, E. K., & Reddi, S. (2005). Just right outsourcing: understanding and managing risk. *Journal of Management Information Systems*, 22(2), 37–55.

Aubert, B. A., Patry, M., & Rivard, S. (2005). A framework for information technology outsourcing risk management. *The DATA BASE for Advances in Information Systems*, 36(4), 9–28.

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.

Bannerman, P. L. (2008). Risk and risk management in software projects: A reassessment. *Journal of Systems and Software*, 81(12), 2118–2133.

Barki, H., Rivard, S., & Talbot, J. (2001). An integrative contingency model of software project risk management. *Journal of Management Information Systems*, 17(4), 37–69.

Barqawi, N., Syed, K., & Mathiassen, L. (2016). Applying service-dominant logic to recurrent release of software: an action research study. *Journal of Business & Industrial Marketing*, 31(7), 928–940.

Baskerville, R., & Pries-Heje, J. (2004). Short cycle time systems development. *Information Systems Journal*, 14(3), 237–264.

Baskerville, R., Ramesh, B., Levine, L., Pries-Heje, J., & Slaughter, S. (2003). Is "internet-speed" software development different? *IEEE Software*, 20(6), 70–77.

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

Beck, U. (1998). *World risk society*. Cambridge: *Polity Press*.

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

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

Benbasat, I., Goldstein, D. K., & Mead, M. (1987). The case research strategy in studies of information systems. *MIS Quarterly*, 11(3), 369–386.

Bergvall-Kåreborn, B., & Howcroft, D. (2014). Persistent problems and practices in information systems development: A study of mobile applications development and distribution. *Information Systems Journal*, 24(5), 425–444.

Bernardi, R. (2009). IT innovation in a health information system in Kenya: Implications for a sustainable open-source software model in developing countries. *In Proceedings of the 10th International Conference on Social Implications of Computers in Developing Countries, Dubai*

Blechar, J., & Hanseth, O. (2007). 7. From risk management to 'organized irresponsibility'? Risks and risk management in the mobile telecom sector. In O. Hanseth, & C. Ciborra (Eds.), *Risk, complexity and ICT*. Edward Elgar Publishing.

Boehm, B. W. (1973). *Software and its impact: A quantitative assessment*. TRW Systems, Engineering and Integration Division.

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

Boehm, B. W. (1991). Software risk management: Principles and practices. *IEEE Software*, 8(1), 32–41.

Brynjolfsson, E., & Saunders, A. (2010). Wired for innovation. In *How information technology in reshaping the economy*. USA: *Massachusetts Institute of Technology*.

Carlo, J. L., Lyytinen, K., & Boland, R. J. Jr. (2012). Dialectics of collective minding: Contradictory appropriations of information technology in a high-risk project. *MIS Quarterly*, 36(4), 1081–1108.

Carlo, J. L., Lyytinen, K., & Boland, R. J. (2004). Systemic risk, IT artifacts, and high reliability organizations: A case of constructing a radical architecture. *Sprouts: Working Papers on Information Systems*, 4(4).

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

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.

Coghlan, D., & Brannick, T. (2014). *Doing action research in your own organization*. Sage.

Conboy, K. (2010). Project failure *en masse*: A study of loose budgetary control in ISD projects. *European Journal of Information Systems*, 19, 273–287.

Constantinides, P., & Barrett, M. (2014). Information infrastructure development and governance as collective action. *Information Systems Research*, 26(1), 40–56.

Cook, S. D. N., & Brown, J. S. (1999). Bridging epistemologies: The generative dance between organizational knowledge and organizational knowing. *Organization Science*, 10(4), 381–400.

Cremonini, M., & Nizovtsev, D. (2010). Risks and benefits of signaling information system characteristics to strategic attackers. *Journal of Management Information Systems*, 26(3), 241–274.

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.

Dhillon, G., & Backhouse, J. (1996). Risks in the use of information technology within organizations. *International Journal of Information Management*, 16(1), 65–74.

Dwivedi, Y. K., Wastell, D., Laumer, S., Zinner Henriksen, H., Myers, M. D., Bunker, D., … Srivastava, S. C. (2015). Research on information systems failures and successes: Status update and future directions. *Information Systems Frontiers*, 17(1), 143–157.

Feldman, M. S., & Orlikowski, W. J. (2011). Theorizing practice and practicing theory. *Organization Science*, 22(5), 1240–1253.

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.

Ghobadi, S., & Mathiassen, L. (2016). Risks to effective knowledge sharing in Agile Software teams: A model for assessing and mitigating risks. *Information Systems Journal*, 26(2), 95–125.

Giddens, A. (1990). *The consequences of modernity*. Stanford, CA: Stanford University Press.

Giddens, A. (1999). Risk and responsibility. *The modern law review*, 62(1), 1–10.

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

Hassan, N., & Mathiassen, L. (2017). Distilling a body of knowledge for information systems development. *Information Systems Journal*, 26(2), 95–125.

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

Holmberg, L., & Mathiassen, L. (2001). Survival patterns in fast-moving software. *IEEE Software*, 18(6), 51–55.

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.

Innotas: The Project and Portfolio Management Landscape 2015. Available at: http://go2.innotas.com/rs/innotas/images/INN_survey-report-043015c.pdf?aliId=104493315

Kang, K., Hahn, J., & De, P. (2017) Learning effects of domain, technology, and customer knowledge in information systems development: An empirical study. *Information Systems Research*, articles in advance, 1–15.

Kautz, K., Madsen, S., & Nørbjerg, J. (2007). Persistent problems and practices in information systems development. *Information Systems Journal*, 17(3), 217–239.

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.

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

Kim, K., Mithas, S., & Kimbrough, M. (2017). Information technology investments and firm risk across industries: Evidence from the bond market. *MIS Quarterly*, 42(4), 1347–1367.

KPMG: Project management survey 2013. Available at: https://home.kpmg.com/nz/en/home/insights/2013/07/project-management-survey-2013.html

KPMG: Project management survey 2017. Available at: https://home.kpmg.com/nz/en/home/insights/2017/04/project-management-survey-2017.html

Kudaravalli, S., Faraj, S., & Johnson, S. L. (2017). A configural approach to coordinating expertise in software development teams. *MIS Quarterly*, 41(1), 46–64.

Kuk, G., & Janssen, M. (2013). Assembling infrastructures and business models for service design and innovation. *Information Systems Journal*, 23(5), 445–469.

Kutsch, E., Denyer, D., Hall, M., & Lee-Kelley, E. (2013). Does risk matter?: Disengagement from risk management practices in information systems projects. *European Journal of Information Systems*, 22, 637–649.

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, A. Bonnie, & J. Kallinikos (Eds.), *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.

Lim, W.-K., Sia, S. K., & Yeow, A. (2011). Managing risks in a failing IT project: A social constuctionist view. *Journal of the Association for Information Systems*, 12(6), 414–440.

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

Lyytinen, K., & Robey, D. (1999). Learning failure in information systems development. *Information Systems Journal*, 9(2), 85–101.

Lyytinen, K., Rose, G., & Yoo, Y. (2010). Learning routines and disruptive technological change: Hyper-learning in seven software development organizations during internet adoption. *Information Technology & People*, 23(2), 165–192.

Marabelli, M., & Newell, S. (2012). Knowledge risks in organizational networks: The practice perspective. *The Journal of Strategic Information Systems*, 21(1), 18–30.

March, J. G., & Shapira, Z. (1987). Managerial perspectives on risk and risk taking. *Management Science*, 33(11), 1404–1418.

Markus, M. L., & Mao, J. Y. (2004). Participation in development and implementation—Updating an old, tired concept for today's IS contexts. *Journal of the Association for Information Systems*, 5(11–12), 421–447.

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

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

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

Mathiassen, L. (1998). Reflective systems development. *Scandinavian Journal of Information Systems*, 10(1&2), 67–118.

Mathiassen, L., & Sørensen, C. (2008). Towards a theory of organizational information services. *Journal of Information Technology*, 23(4), 313–329.

Mathiassen, L., Tuunanen, T., Saarinen, T., & Rossi, M. (2007). A contingency model for requirements development. *Journal of the Association for Information Systems*, 8(11), 569–597.

McFarlan, F. W. (1981). Portfolio approach to information systems. *Harvard Business Review*, 59(5), 142–150.

Mindel, V., & Mathiassen, L. (2015, January). Contextualist inquiry into IT-enabled hospital revenue cycle management: Bridging research and practice. *Journal of the Association for Information Systems*, 16(12), 1016–1057.

Mitev, N. (2011). Beyond health warnings: Risk, regulation, failure and the paradoxes of risk management. *Journal of Information Technology*, 26(4), 271–273.

Mumford, E. (1996). Risky ideas in the risk society. *Journal of Information Technology*, 11(4), 321–331.

Narayanaswamy, R., Grover, V., & Henry, R. M. (2013). The impact of influence tactics in information systems development projects: A control-loss perspective. *Journal of Management Information Systems*, 30(1), 191–225.

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

Newman, M., & Robey, D. (1992). A social process model of user-analyst relationships. *MIS Quarterly*, 16, 249–266.

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

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

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

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.

Patton, M. Q. (2002). *Qualitative evaluation and research methods* (3rd ed.). Thousand Oaks, CA: Sage.

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), 508–532.

Pettigrew, A. M. (1997). What is a processual analysis. *Scandinavian Journal of Management*, 13(4), 337–348.

Pries-Heje, J., Baskerville, R. L., Levine, L., & Ramesh, B. (2004). The high speed balancing game: How software companies cope with internet speed. *Scandinavian Journal of Information Systems*, 16(1), 1.

Ramasubbu, N., Bharadwaj, A., & Tayi, G. K. (2015). Software process diversity: Conceptualization, measurement, and analysis of impact on project performance. *MIS Quarterly*, 39(4), 787–807.

Renn, O. (1998). Three decades of risk research: Accomplishments and new challenges. *Journal of Risk Research*, 1(1), 49–71.

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.

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), 98–112.

Sarker, S., & Sarker, S. (2017). Exploring agility in distributed information systems development teams: An interpretative study in an offshoring context. *Information Systems Research*, 20(3), 440–461.

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.

Schultze, U., & Orlikowski, W. J. (2004). A practice perspective on technology-mediated network relations: The use of internet-based self-serve technologies. *Information Systems Research*, 15(1), 87–106.

Schwalbe, K. (2015). *Information technology project management*. Cengage Learning.

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.

Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research*, 1(3), 255–276.

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

Syed, K., Barqawi, N., & Mathiassen, L. Accepted(2017). Release cycle management: A Contextualist inquiry into recurrent software development and improvement. *International Journal of Business Information Systems*.

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.

Tesch, D., Kloppenborg, T. J., & Frolick, M. N. (2007). IT project risk factors: The project management professionals perspective. *The Journal of Computer Information Systems*, 47(4), 61–69.

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

Truex, D. P., Baskerville, R., & Klein, H. (1999). Growing systems in emergent organizations. *Communications of the ACM*, 42(8), 117–123.

Unluer, S. (2012). Being an insider researcher while conducting case study research. *The Qualitative Report*, 17(58), 1–14.

Walsham, G. (1993). *Interpreting information systems in organizations*. John Wiley & Sons, Inc.

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. In *Information systems and qualitative research*. (pp. 466–480). US: Springer.

Windeler, J. B., Maruping, L., & Venkatesh, V. (2017). Technical systems development risk factors: The role of empowering leadership in lowering developers' stress. *Information Systems Research, Articles in advance*, 1–22.

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

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.

Lars Öbrand (lars.obrand@umu.se) is an associate professor in Informatics at Umeå University and part of the Swedish Center for Digital Innovation. His research focuses on issues related to risk within the broader area of IT management and organizational change processes. He is a senior lecturer with extensive teaching experience covering a wide range of topics and levels. His research has been published in journals and conferences such as Industrial Management and Data Systems, Technology in Society, Hawaii International Conference on System Sciences, European Conference of Information Systems, and European Group for Organizational Studies.

Nils-Petter Augustsson (nils-petter.augustsson@umu.se) is a PhD student within the Industrial Doctoral School at Umeå University. In parallel, he is working as a director within the information technology area with service delivery and solution management as his special areas. Prior to these positions, he has been working as a junior lecturer at the Department of Informatics, Umeå University, and as junior researcher at the Interactive Institute Tools studio in Umeå. Augustsson has presented his research at international conferences such as the International Conference of Information Systems, American Conference on Information Systems, Hawaii International Conference on System Sciences, Information Systems Research Seminar in Scandinavia, and the Nordic Conference.

Lars Mathiassen (lmathiassen@ceprin.org) is a Georgia Research Alliance Eminent Scholar, Professor at the Computer Information Systems Department, and cofounder of the Center for Process Innovation at Georgia State University. His research focuses on the development of software and information services, on IT-enabled innovation of business processes, and on management and facilitation of organizational change processes. He has published extensively in major information systems and software engineering journals and has coauthored several books. He has served as a senior editor for MIS Quarterly and serves as senior editor for Information and Organization and for the Journal of Information Technology.

Jonny Holmström (jonny.holmstrom@umu.se) is a professor of informatics at Umeå University and a director and cofounder of the Swedish Center for Digital Innovation. He writes, consults, and speaks on topics such as information technology management, digital innovation, digital strategy, digital entrepreneurship, and strategies for leveraging value from digitalization. His work has appeared in journals such as Communications of the AIS, Convergence, Design Issues, European Journal of Information Systems, Information and Organization, Information Systems Journal, Information Technology and People, Journal of the AIS, Journal of Strategic Information Systems, Research Policy, and The Information Society. He currently serves as a senior editor for Information and Organization.

How to cite this article: Öbrand L, Augustsson N-P, Mathiassen L, Holmström J. The interstitiality of IT risk: An inquiry into information systems development practices. *Info Systems J*. 2019;29:97–118. https://doi.org/10.1111/isj.12178