Information & Management 55 (2018) 80–93

Contents lists available at ScienceDirect

Information & Management

journal homepage: www.elsevier.com/locate/im

IT managers' vs. IT auditors' perceptions of risks: An actor–observer asymmetry perspective

Arno Nuijten[a,*], Mark Keil[b], Gert van der Pijl[a], Harry Commandeur[a]

[a] Erasmus University Rotterdam, Erasmus School of Accounting & Assurance, P.O. Box 1738, NL-3000 DR, Rotterdam, Netherlands
[b] Georgia State University, Department of Computer Information Systems, J. Mack Robinson College of Business, 35 Broad Street, Atlanta, GA 30303, USA

ARTICLE INFO

Keywords:
IT risk perception
Actor–observer asymmetry
IT audit

ABSTRACT

With the growing role of information technology (IT), many organizations struggle with IT-related risks. Both IT managers and IT auditors are involved in assessing, monitoring, and reporting IT risks, but this does not necessarily mean that they share the same views. In this study, we draw upon the actor–observer asymmetry perspective to understand differences in IT managers' vs. IT auditors' perceptions of risks. Through a quasi-experiment with 76 employees of a financial institution, we found that IT managers and IT auditors showed the expected actor–observer differences. Implications for both research and practice are discussed.

1. Introduction

Identifying and managing IT risks has become ever more important, and this has led to an increased interest in IT auditing. The idea behind IT auditing is that employees who have a position that is independent from management perform assessments of how IT risks are managed within the organization. The argument is that IT audits can help avoid surprises by properly assessing IT risks so that appropriate action can be taken to minimize either the chance that a risk will materialize or the impact of a risk that does materialize.

Although one could argue that a good IT manager can perform the same risk assessment function as an IT auditor, the movement toward IT auditing is based on the premise that IT auditors will improve an organization's capacity to identify and manage IT risks especially because they are in a position to act as independent observers.[1] Whether or not this premise is true, the effectiveness of IT auditors hinges to a large degree on whether they differ from IT managers in terms of risk perceptions. Here, we suggest that the risk perceptions of IT auditors (who are in the position to observe) may differ from the risk perceptions of IT managers (who are in the position to act).

Several years ago, Liu et al. [1] pointed to the need for research on the risk perceptions of IT auditors, but to date there has been no research comparing the risk perceptions of IT auditors with those of IT managers. As many documented IT disasters have exhibited a pattern in which key IT professionals in the organization failed to assess and report IT risks properly because of biases in their observations [2–5], understanding whether IT auditors differ from IT managers in their perceptions of risk has important implications for both theory and practice.

In this study, we draw upon the actor–observer perspective to examine differences in IT managers' vs. IT auditors' perceptions of IT risks. To test our ideas, we conducted a quasi-experiment in which we compared risk assessments of 44 IT managers and 32 IT auditors who worked for the same financial institution. The remainder of our paper is organized as follows: first, we offer an overview of the literature and the theoretical perspective that we draw upon. Then, we introduce our research model and hypotheses. Next, we discuss the method used to test our research model and the results that were obtained. We conclude with a discussion of the implications of our study for both research and practice.

2. Literature review and theoretical perspective

2.1. IT risks in information systems literature

The existence of various IT risks and the need to manage them is well documented in the information systems literature (see, e.g., [6,7]). Indeed, failure to manage these risks is often cited as a contributing factor in IT failures [8–15]. Bharadwaj et al. [16,p. 68] distinguished between "operating failures that impact existing systems and implementation failures that involve new systems development projects." Clearly, there is a broad range of risks that one must be concerned

* Corresponding author.
E-mail addresses: nuijten@ese.eur.nl (A. Nuijten), mkeil@gsu.edu (M. Keil), vdpijl@home.nl (G.v.d. Pijl), hcommandeur@ese.eur.nl (H. Commandeur).

[1] Throughout this document, we will further use the term "IT auditors" where we refer to IT auditors who work at an internal audit department. We are not referring to external IT auditors who work at a different organization and are only involved on an occasional basis.

http://dx.doi.org/10.1016/j.im.2017.04.002
Received 17 August 2015; Received in revised form 15 March 2017; Accepted 9 April 2017
Available online 13 April 2017
0378-7206/

about, and these include risks that affect the development and implementation of IT systems and risks that affect the smooth operation of IT systems such as security risks [7,15]. Both IT managers and IT auditors can play important roles in managing these risks. Prior research suggests that in terms of information security, insiders often represent the greatest risk and that protecting against these threats requires a combination of both in-role and extra-role behaviors [17].

In recent years, there has been a growing interest in the role of IT auditors who provide assurance on "the implementation of policies, plans, procedures, and organizational structures designed to achieve business objectives and prevent, detect, or correct undesired events" [18,p. 599]. An IT risk is defined here as a condition that can present a serious threat to business operations. Consistent with the study by Bharadwaj et al. [16,p. 68], our study covers a range of IT risks classified in the domains Delivery & Support (existing systems) and Acquisition & Implementation (implementation of new systems) of the control objectives of information and related technology (CobiT) framework [19]. These domains cover IT risks that are relevant to both IT management and IT auditors [20,p. 49] and as such serve the purpose of our study, which is to compare the perception of IT risks across these two roles. Examples of the types of IT risk that we focus on are security risks that can arise from a lack of antivirus controls and a lack of adequate back-up facilities and recovery plans in the event that a disaster or emergency should occur.

Early research on IT security focused on checklists for security procedures and controls and assessing the risk of various security threats. More recent work has focused on compliance with security policies and has shown that there is a relationship between the severity of a perceived threat and the intention to comply with security policies [21]. This stream of research tends to investigate the factors that promote compliance with security policies among employees of an organization [22]. Although interesting and useful, this line of research is less relevant to our work as it does not speak about role-based differences in risk perceptions, which is the focus of our research.

Because our aim is to compare the risk perceptions of IT managers and IT auditors, we focus here on a relatively small number of papers in the security risk area and the IT project risk area that focus on risk perceptions and how these perceptions may differ depending upon an employee's role.

2.2. IT risks in accounting and auditing literature

Although the existence of various IT risks and the need to manage them are well documented in the information systems literature, IT risks have also received increased attention in the field of accounting and auditing [23–25]. In a review of judgment and decision research in auditing, Solomon and Trotman [26] stated that the most common form of auditing has been audits of financial statements but that the role of auditors has expanded beyond financial statements and now includes other activities including assessment of IT-related risks. They suggest that further research using the experimental method is warranted and that such research needs to consider the changes that have occurred in terms of accounting and auditing practices. A number of studies have emphasized the emerging role of information technology and information systems in the daily practice of accounting [27,28] and auditing [29,30], and increased attention is now being assigned to the role of IT auditors, i.e., auditors with dedicated expertise on IT risks as compared to the more financial-oriented auditors who are less familiar with IT risks. According to Curtis et al. [31], the involvement of IT auditors is key in many audit engagements, and they claim that the role of IT auditors is likely to increase in the near future because of the increased importance and complexity of IT in today's audit environment [31]. For the same reason, Weidenmier and Ramamoorti [25] call for IT auditing research in the domain of internal auditing specifically, which is the context of our study as well. To date, however, research in this area is quite limited and mainly focused on the involvement of IT auditors in audit assignments and on how to improve cooperation between IT auditors and other auditors. Such work, while valuable, remains within the borders of research in accounting and auditing.

In a call for research crossing the borders between research in information systems and research in accounting, Debreceny [24] referred to the specific fields of IT governance, enterprise resource planning systems [23], outsourcing [32], data and information quality [33], and information security [34] that are of high relevance to the accounting literature. Debreceny [24] emphasized that the governance of IT risks is a longstanding concern of the accounting and assurance community and specifically mentioned CobiT as a structure and a *lingua franca* in which auditors, IT managers, operational managers, and board members communicate about IT risks.

We conclude from this review of IT risks in the accounting and auditing literature that (1) IT is receiving increased attention in the field of accounting and auditing, (2) research that crosses the borders of information systems and accounting is warranted, specifically if it relates to IT risks as identified in the CobiT framework, and (3) adopting a common language to discuss IT risks does not necessarily mean that IT auditors and IT managers will have the same perceptions when it comes to assessing such risks.

2.3. Role-based differences in risk perception

Consistent with Sitkin and Pablo [35,p. 12], we define risk perception as an individual's "assessment of the risk inherent in a situation." As Schmidt et al. [14,p. 29] observed, "it is quite possible that different stakeholders will have divergent opinions" regarding risk. Prior research in the security risk area and IT project risk area has shown that this is indeed the case. More generally, research on risk perceptions has shown that experts' perceptions differ from those of nonexperts [36].

With regard to security risk, Baskerville et al. [7] differentiated between prevention and response paradigms. Here, we focus on the prevention paradigm (i.e., information systems security principles and practices "intended to prevent security incidents from happening") [7,p. 139]. Posey et al. [37] conducted 33 interviews with a mix of "ordinary organizational insiders" and information security professionals. They observed both similarities and differences in how these two groups viewed security threats. In terms of differences, for example, insiders had a much greater tendency than security professionals to view hackers as a threat. Posey et al. [37,p. 557] concluded that differences in perception of security threats "suggests that organizational insiders might not appraise threats as accurately as security professionals would like." Mouratidis et al. [38] conducted a survey at a bank (n = 60), followed by e-mail interviews with a subset of respondents (n = 20), and found that personnel from general management have different perspectives toward network security than network security specialists. Taken together, these two studies suggest that role-based differences can exist in how individuals view security risks.

With regard to IT project risk, Keil et al. [39] reported that project managers and users have different perceptions of risk. Using a Delphi study approach, they found that users tend to focus on the importance of certain risks associated with project management capabilities and skills, while project managers tend to focus on the importance of certain risks associated with the user (e.g., user commitment and scope creep). From their results, Keil et al. [39] suggested the importance of understanding the risk perceptions of *other* stakeholders. Addison [40] explored e-commerce project development risks through a Delphi survey, which included the viewpoints of developers, project managers, clients/users, and academics. His results suggested that different stakeholders might apply different rankings to the same set of risks, consistent with the findings of Keil et al. [39]. Liu et al. [1] used the Delphi method to compare the risk perceptions of senior executives and project managers. They found that project managers tend to focus on lower-level risks (e.g., those associated with requirements and user involvement), whereas senior executives tend to focus on higher-level

risks (e.g., those associated with politics, organization structure, and culture). Taken together, these studies suggest that role-based differences can exist in how individuals view IT risks.

However, the question of whether *IT auditors* perceive risks differently than *IT managers* has not been studied. Moreover, although prior research has established that role-based differences in risk perception exist, a theoretical perspective has not been advanced to understand these differences. To summarize, although prior research shows differences in risk perceptions across various stakeholders, there is a gap in our understanding of whether *IT auditors* perceive risks differently than *IT managers*, and if so, what theoretical logic might provide insight concerning such differences. To address this gap in the literature, we turn to the concept of actor–observer asymmetry.

2.4. Actor–Observer asymmetry between IT managers and IT auditors

Liu et al. [1] suggested that further research is needed to examine the risk perceptions of IT auditors. Their call for further research in this area is particularly salient, given that some organizations are now assigning auditors (both internal and external to the organization) to examine IT risks under the assumption that individuals who are role prescribed to detect anomalies will have heightened risk perceptions relative to IT managers who are too close to a situation to be objective about its risk profile.

Given that there is a gap in our knowledge regarding the impact of audit role on risk perceptions, and the importance that many organizations are now placing on the IT audit process,[2] additional research in this area is warranted. Moreover, although many of the prior studies have found role-based differences in risk perception, they have not provided a theoretical logic for these differences. In this paper, we suggest that role-based differences shape the information processing and decision-making heuristics that individuals use. As Kahneman [42] noted, decision-making is heavily influenced by heuristics when we engage in System 1, or fast thinking. Here, we posit that role-based differences give rise to the use of different heuristics and information-processing patterns over time and that this influences risk perceptions.

More specifically, we propose that differences between IT auditors' and IT managers' risk perceptions result from the fact that IT auditors are most often in the role of observing and monitoring IT risks, whereas IT managers are most often in the role of acting upon reported risks. For our theorizing, we were drawn to the actor–observer asymmetry perspective and inspired by a car driving experiment by Horswill and McKenna [43], which provides evidence that people who are placed in the driver's position (i.e., driving the car and taking actions) perceive risks differently than people who are placed in the passenger's position (i.e., in the position of an observer). Their results indicated that an illusion of control is in operation, such that those who are in control (i.e., drivers) are comfortable with a higher level of risk than those who are not in control (i.e., passengers). Drawing on this distinction, we conceive of IT managers as being in a position that is similar to that of a car driver (i.e., one who is supposed to take actions), and we conceive of IT auditors as being in a position that is similar to that of a passenger (i.e., one who is supposed to observe and be prepared to issue risk warnings).

In this paper, we therefore suggest that actor–observer asymmetry offers a useful theoretical perspective for understanding differences in risk perception between actors who work with IT systems and operations (e.g., IT managers) and observers who monitor such systems and operations (e.g., IT auditors).

[2] According to a 2013 survey conducted by KPMG that covered over 400 organizations across Europe, the Middle East, and Africa, "Demand for assurance over technology-related risk has never been higher." [41,p. 6] and "IT Internal Audit is a key resource that many organizations look to for insights. It has a critical role to play in helping organizations understand their overall IT risk profile, providing assurance for the controls currently in place and highlighting opportunities for improvement" [41,p. 6].

Prior research has shown that risk taking "is more pronounced for actors than for observers" [44,p. 5]. Using a gambling experiment involving a card task, Fernandez-Duque and Wifall [44] randomly assigned subjects to either play the game or observe another player (a confederate). Ten cards were displayed face down, and subjects were told that nine cards were "good" and would produce rewards (at the rate of $1 per card) for the player, but that one card was "bad" and would cause the player to lose everything. Subjects in the actor condition played the game and could turn over as many cards as they wanted (one card at a time), while subjects in the observer condition watched a confederate play the game and were asked at each decision point whether the player (i.e., the confederate) should turn over the next card. Actors were not only more willing to take risks than observers as evidenced by the number of cards they were willing to turn over but also "reported relying less on probabilities for deciding when to stop" [44,p. 4]. A subsequent experiment was conducted to rule out the possibility that the observed differences between actors and observers might be because of the asymmetric reward scheme.

Fernandez-Duque and Wifall [44,p. 6] suggested that actor–observer asymmetry results from differential access to experiential systems (i.e., the heuristics associated with System 1 thinking). In addition, they suggested that actors are "more prone to a confirmation bias than observers and thus gain a false sense of skill" [44,p. 6]. Such an interpretation would be consistent with Langer and Roth's [45] work on illusion of control in which it was found that individuals exhibit biased processing of information even in task situations in which the outcomes are based purely on chance and not on one's ability, such as predicting the results of coin tosses. In an experiment, participants who performed the coin tosses (i.e., actors) rated themselves better at the task and predicted that they would have more successes than those who merely observed the coin tosses [45]. This suggests that actors have a tendency to produce upwardly biased estimates of success (and correspondingly lower estimates of risk) than observers, even in situations where it is clear that their actions do not affect the outcomes, such as in the pure chance conditions of a coin toss.

Drawing on the actor–observer asymmetry perspective, we propose that IT managers are used to playing the role of actors in the context of IT systems and operations and will therefore tend to exhibit an assessment of the risks that is consistent with this role. We further propose that IT auditors are used to play the role of observers and will likely assess risks in a manner that is consistent with this role. Therefore, we expect that IT managers and IT auditors will perceive risks differently and in ways that are predictable based on actor–observer asymmetry.

Specifically, we suggest that because IT managers are in a role that requires them to be actively involved in managing IT risks, they are likely to experience a higher level of control over these risks, thus leading to lower risk perceptions. Given their role as observers, IT auditors will likely experience a lower level of control and thus perceive greater risks than IT managers, but we do not mean to suggest that IT auditors would necessarily be unbiased in assessing risks. Indeed, IT auditors may have a tendency to overestimate risk due to their role. To summarize, we suggest that IT managers will tend to have lower risk perceptions relative to IT auditors consistent with the actor–observer asymmetry perspective.

There has been no research that we are aware of comparing the risk perceptions of IT auditors with those of IT managers. We did, however, find one study by Helliar et al. [46] that surveyed accountants and managers and compared their attitudes toward risk. Their results suggest that when a situation involves the possibility of future losses, accountants' perceptions of risk are significantly higher than nonaccountants' perceptions of risk, but they do not offer any theoretical logic that might shed light on such differences. Thus, our study addresses a gap in the literature by drawing on the actor–observer asymmetry perspective to hypothesize and test for possible differences in risk perceptions between IT auditors and IT managers.

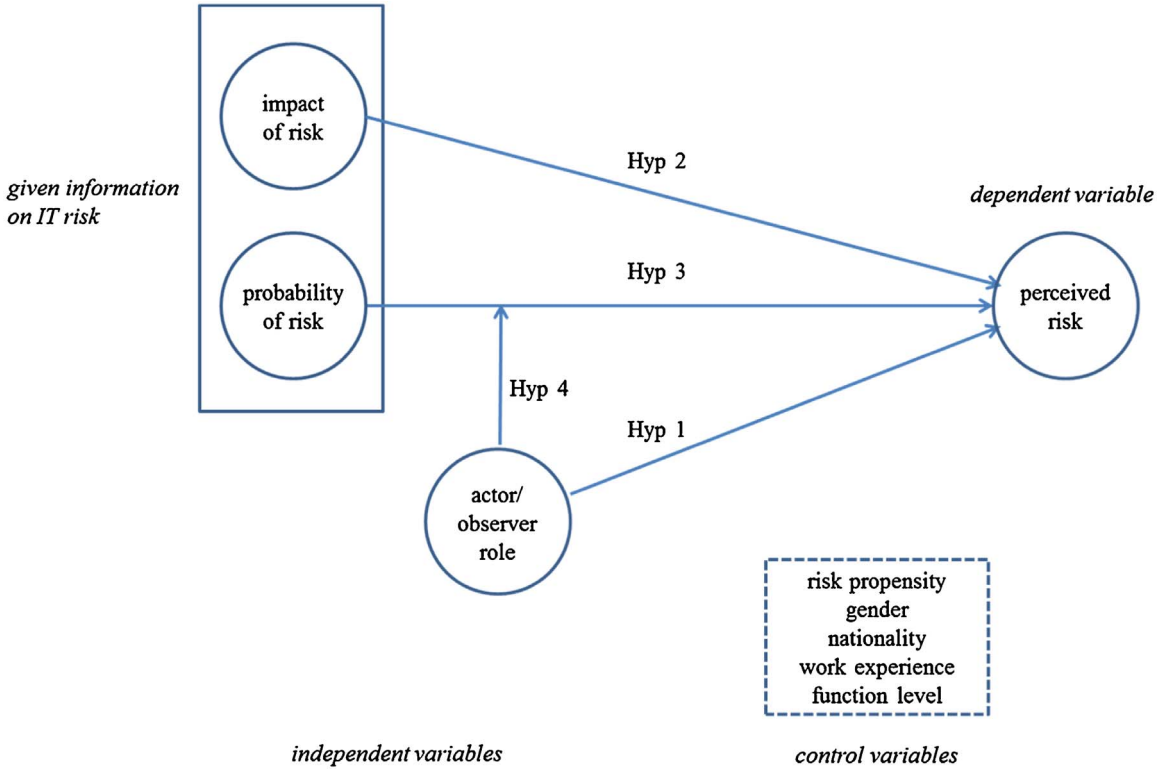

Fig. 1. Research Model.

3. Research model and hypotheses

Drawing on the extant literature on risk perception and actor–observer asymmetry, we propose our research model as represented in Fig. 1. *Perceived risk* is the dependent variable in our model because we want to test for possible differences in risk perceptions between IT auditors and IT managers. Perceived risk is defined "as a decision maker's assessment of the risk inherent in a situation" [35]. The main independent variable in our research model is *actor–observer role*, which represents whether the employee has a role as an actor (IT manager) or as an observer (IT auditor). We expect that the actor–observer role will influence risk perception across a wide range of situations in which there is access to information on specific IT risks.

Risk is generally regarded as the combination of the probability of an undesirable event occurring and the magnitude of the loss that is associated with the event [47] and has been treated as such in the IS literature (see, e.g., Barki et al. [13]). Therefore, these two factors have often been used together to define and describe risk [12,48,49]. As both probability of risk and impact of risk can, in theory, influence risk perception, we included both elements in our model. As explained later, we also theorize that the actor–observer role will moderate the relationship between risk probability and perceived risk.

We also include a number of control variables in our model. Risk propensity serves as an important control variable that captures individual differences in orientation toward seeking or avoiding risks [35]. Prior research by Sitkin and Weingart [50] suggested that risk propensity is inversely related to risk perception. Thus, it is important to control for risk propensity in examining whether an actor–observer asymmetry exists between IT auditors and IT managers. Gender, nationality, and work experience were also included as control variables in our model, as these may also influence perceived risk.

The first and main hypothesis in our research model focuses on the relationship between the actor–observer role and an individual's perceived risk in IT situations. Langer and Roth [45] conducted a laboratory experiment involving a purely chance-based task (coin tossing) and showed that those who performed the task (i.e., actors) rated themselves better at predicting outcomes than those who merely observed the task being performed by another individual (i.e., observers). They theorized that the more involved an individual is, "the more likely it is that they will experience an illusion of control" [45,p. 954]. Langer [51,p. 313] defined illusion of control as "an expectancy of a personal success probability inappropriately higher than the objective probability would warrant."

Horswill and McKenna [43] conducted an experiment using video simulation with 96 drivers to determine their risk-taking behavior across a range of driving activities including speed choice. They manipulated participants into actor or observer roles by telling half of their participants to imagine that they were driving the vehicle and the other half to imagine that they were passengers. Those who were told to imagine that they were driving (i.e., actors) chose significantly faster speeds than did those who were told to imagine that they were passengers (i.e., observers). The authors theorized that their manipulation influenced risk-taking behavior by altering individuals' perceived control. Prior work [52] suggested that when people believe they are in control of a situation, they assume that their actions can increase the probability of a positive outcome (or decrease the probability of a negative outcome).

The above studies suggest that actors will have greater perceived control over outcomes than observers and that this actor–observer asymmetry can be used to predict differences in risk perception between IT managers (who are used to being in the driver's seat) and IT auditors (who are used to being in the passenger's seat). Specifically, we suggest that because IT managers are in a role that requires them to be actively involved in managing IT risks, they are likely to experience a higher level of control over these risks, thus leading to lower risk perceptions. Given their role as observers, IT auditors will likely experience a lower level of control, thereby leading to higher risk perceptions. Thus, consistent with the actor–observer asymmetry perspective, we expect that for a given risk situation, IT managers' risk perceptions will be lower than IT auditors' risk perceptions. Therefore, we state the following hypothesis:

H1) *IT managers and IT auditors will have different risk perceptions*

regarding the same underlying risk scenarios and consistent with the actor–observer asymmetry perspective, IT managers' risk perceptions will be lower than IT auditors' risk perceptions.

As noted earlier, both probability of risk and impact of risk can, in theory, influence risk perception. March and Shapira [53] suggested that managers' risk perceptions appear to be based more on the magnitude of potential loss (i.e., impact) as opposed to the probability that a loss will occur. Consistent with this, Helliar et al. [46] reported that both managers' and accountants' risk perceptions are shaped more strongly by the magnitude of negative outcomes as opposed to probability estimates. Keil et al. [54] conducted an experiment in which impact and probability were manipulated independently and found a significant effect of impact on risk perception, but they did not find any significant effect of probability on risk perception. Thus, although prior research shows unambiguous evidence that individuals' risk perceptions are strongly affected by impact information, the effect of probability information on risk perceptions is more ambiguous. Still, theory suggests that both probability and impact can influence risk perceptions. Therefore, we state the following two hypotheses:

H2) *The potential impact of a risk will be positively associated with risk perception.*

H3) *The probability of a risk occurring will be positively associated with risk perception.*

H2 represents a pure replication hypothesis, and H3 is intended to clarify ambiguity in prior studies.

As noted earlier, managers' risk perceptions appear to be based more on the magnitude of potential loss as opposed to the probability that a loss will occur [53–56]. This is very likely because managers tend to be loss averse and believe that they can, through their own behavior, influence (i.e., reduce) the odds of a risk materializing. Langer and Roth [45] showed in their coin toss experiment that when subjects were given initial feedback suggesting that they were accurate predictors of coin tosses, they developed a greater illusion of control over their ability to predict the outcome of coin tosses. As Langer [51,p. 313] observed, if the introduction of skill aspects into a purely chance event induces an illusion of control, "then the effects should be far greater when they are introduced into situations where there is already an element of control." This is exactly the kind of circumstances that managers often find themselves in. Experienced managers in particular seem to be less influenced by probability information, as they do not believe that these probabilities apply to them personally [56,p. 74]. Specifically, they think that they can beat the probability estimations. In essence, managers (as actors) become so used to having some control in situations that involve a mix of chance and skill that they may be more apt to develop an illusion of control. Given their role as observers, IT auditors will likely experience a lower level of control, leading to higher risk perceptions. Thus, we theorize that actor–observer asymmetry will moderate the relationship between risk probability and risk perception. From this reasoning, we offer the following hypothesis:

H4) *Consistent with the actor–observer asymmetry perspective, the relationship between risk probability and risk perception will be moderated by actor–observer role such that the relationship between risk probability and risk perception will be stronger for IT auditors than for IT managers.*

To summarize, our central hypotheses (H1 and H4) are that observers' perceptions of risk will be higher than actors' perceptions of risk (H1) and that as risk probability increases, the increase in perceived risk will be greater for observers (i.e., auditors) than it is for actors (i.e., managers) (H4).

4. Method

4.1. Experimental design

To test our hypotheses, we conducted a 3 × 3 × 2 mixed-design quasi-experiment. Risk impact and risk probability were treated as within-group factors (each with three levels: high, medium, and low), and actor–observer role was treated as a between-group factor. Rather than randomly assigning subjects to one of the two roles (actor or observer) in a laboratory setting, we recruited 32 IT managers and 44 IT auditors from a single Dutch banking organization to participate in the study. All participants worked in the bank's offices in both Amsterdam and London (splitting their time between the two offices) and were familiar with the organization's standards and procedures on risk assessments, either from an internal auditing perspective or from a management perspective. Given the prominent role of IT within the bank's strategy, infrastructure, and operations, all participants were also highly familiar with the implications of IT and IT risks.

Because we executed our study in an organizational field setting, we could maximize the benefits of having realistic conditions, while simultaneously achieving the internal validity of a quasi-experiment. For the within-group factors, we isolated specific risks that had meaning in this organization, constructed realistic scenarios for each risk, and then mapped each scenario to one of the nine levels of risk impact and risk probability according to the organization's standards and procedures for risk assessment. We chose this route because we were particularly interested in understanding role-based differences that can exist in actual organizational settings and wanted to make the risks (and the exposure each represented) as realistic as possible. Our risk scenarios were based on actual audit findings from previous reports filed by IT auditors within the organization. A small panel of experts was assembled to verify whether the text of each scenario was consistent with the presented probability and impact levels, thereby ensuring that our scenarios were realistic.

For the actual quasi-experiment, each participant was asked to respond to a sequence of nine different IT risk scenarios, each one labeled with a different combination of risk impact (low, medium, and high) and risk probability (low, medium, and high). Using a repeated-measures approach for this aspect of our quasi-experiment allowed us to control for personal differences and increased our statistical power so that fewer participants could be used [57]. The quasi-experiment covered all combinations of probability and impact levels (low, medium, and high). The actual scenarios used are shown in Appendix A.

Recruiting participants from a single organization allowed us to control for situational factors such as organization size, type, and culture, while also allowing us to compare IT auditors and IT managers on standardized criteria such as function level within the organization. Participants were invited by e-mail and joined the study voluntarily.

4.2. Postexperiment interviews

In our quasi-experiment, all respondents provided us with their personal contact information. This information enabled us to schedule follow-up interviews with 10 IT auditors who had participated in our study long after they had participated in the experiment. These interviews allowed us to check our assumption that whether IT auditors would consider themselves in the position of observers and to shed more light on how IT managers and IT auditors might differ in their perception of IT risks. Among the interviews conducted, we specifically selected four respondents who had switched between the role of IT manager and the role of IT auditor during their careers. In all interviews, we first probed whether respondents experienced differences in the perception of IT risks between IT managers and IT auditors, and if so, how they would explain such differences. We also asked our interviewees whether any differences in risk perception between IT managers and IT auditors might relate specifically to the probability and the impact associated with an IT risk. Next, we introduced the "actor versus observer" concept to our respondents, illustrating it with the car-driving example in which the driver is seen as the actor and the passenger is seen as the observer. We asked our respondents to tell us whether they saw IT auditors and IT managers as either actors or observers. To the four respondents who had performed both the roles of IT manager and IT auditor, we asked whether the switch between these

Table 1
Constructs and Measures.

Construct	Type of variable	Content	Measurement	Source
perceived risk	Dependent	Rated risk level according to the organization standards	Nine within-subject measurements with single-item, three-level scale (low, medium, high)	Organization's risk assessment and reporting standards
actor–observer role	Independent	Role as IT auditor (observer) or IT manager (actor)	Dichotomous variable (0 = actor; 1 = observer)	Provided by the company
risk prop	Control	Risk propensity in the domain of IT risks	Six 5-point Likert-type scale items	Adapted from Nicholsen et al.'s [58] Applied Risk Propensity Scale
vicepres	Control	Employee carried the title of Vice President	Dichotomous variable (0 = not a VP; 1 = VP)	Provided by the company
gender	Control	Participant's gender	Dichotomous variable (0 = female; 1 = male)	Self-reported
nationality	Control	Participant's nationality	Two dichotomous variables Dutch (0 = not Dutch; 1 = Dutch) British (0 = not British; 1 = British)	Self-reported
work experience	Control	Respondent's work experience with the organization	Years	Self-reported
function level	Control	Respondent's function level within the organization	Measured on a 5-point scale	Provided by the company

roles made them perceive risks differently. The interviews typically lasted from 20 to 25 min and were recorded and transcribed verbatim.

4.3. Constructs and measures

Table 1 provides a summary of our constructs and measures. Appendix A provides a detailed description of the individual measurement items used in our quasi-experiment. For context realism, we adopted the risk perception measure used by the organization in which we performed this study. Employees at the bank not only used this scale in their daily work but had also been formally trained on risk assessment using this approach.

5. Analysis and results

5.1. Descriptives and control variables

The participants' experience, gender, education, function level, and nationality are provided in Tables 2 and 3.

Before proceeding with our main analysis, we explored whether any of our control variables were significant in the model. This was performed by testing the control variables individually as between-subject variables in a series of mixed-design ANOVAs. We found no significant effect of either gender ($F = 0.907$; $p = 0.344$) or years of work experience ($F = 1.484$; $p = 0.172$) on perceived risk. Because all participants were selected from the same organization, we could compare participants across their function level, using the organization's HR framework. Tables 2 and 3 show that the IT managers who participated in our study had on average a higher function level than the IT auditors. We tested whether respondent's function level was significant in our research model and found no significant effect of function level on perceived risk ($F = 0.510$; $p = 0.728$). No significant between-subject effects were found for participants across the five function levels presented in Tables 2 and 3. Whether or not a participant held a vice president title within the organization was also not found to be a significant predictor of risk perception ($F = 0.002$; $p = 0.965$).

As indicated in Tables 2 and 3, most participants were either Dutch or British. We tested whether participants' nationality was significant in our research model and found no significant effects for British compared to non-British participants ($F = 0.085$; $p = 0.772$) or for Dutch compared to non-Dutch participants ($F = 0.137$; $p = 0.712$). One explanation for this may be that our Dutch and UK participants worked for the same company, and prior to Brexit, they were encouraged to spend time in both locations. Thus, the common corporate culture and the high mobility of personnel may have swamped any differences relating to national culture. Finally, we tested whether participants' risk propensity was significant in our model and found that it was marginally significant ($F = 1.640$; $p = 0.084$). On the basis of these results, we retained only risk propensity as a control variable, retaining it as a covariate in our subsequent analysis.

5.2. Reliability and validity

Before proceeding further with our analysis and hypothesis testing, we explored the reliability and validity of our measures. An initial principal component analysis (PCA) revealed that one of our risk propensity items (RiskProp 6) cross-loaded with observer role; therefore, this item was dropped from our measurement model. A subsequent PCA with our independent variable measures reveals a clean factor structure as shown in Table 4.

As the measurement items correlate higher with their own "construct" (factor) than with others, and the cross-loadings are quite low; Table 4 suggests that our measures have adequate convergent and discriminant validity [57]. We also examined the reliability of our measurement items for risk propensity and obtained a Cronbach's alpha of 0.84, which exceeds the threshold of 0.7 [59].

Table 2
Descriptive Statistics for the IT auditors.

IT Audit experience			Gender			IT Audit education			Function level within HR framework			Nationality		
< 3 years	1	2%	Male	39	89%	Certified IT auditor	36	82%	1. IT auditor	13	30%	Dutch	27	61%
3–5 years	11	25%	Female	5	11%	Not (yet) certified IT auditor			2. Senior IT auditor	17	39%	British	14	32%
5–10 years	22	50%					8	18%	3. IT-audit manager (VP)	12	27%	Other	3	7%
10–15 years	10	23%							4. Head IT-audit (SVP)	1	2%			
> 15 years	0	0%							5. Director IT-audit (EVP)	1	2%			
Totals	44	100%		44	100%		44	100%		44	100%		44	100%

Table 3
Descriptive Statistics for the IT managers.

IT management experience			Gender			Highest education			Function level within HR framework			Nationality		
< 3 years	0	0%	Male	28	87%	Msc/MBA	19	60%	1. Project mgr equiv	1	3%	Dutch	9	28%
3–5 years	1	3%	Female	4	13%	Bachelor	5	16%	2. Sr. Project mgr equiv	10	31%	British	22	69%
6–10 years	7	22%				A-level	3	9%	3. Progmgr/IT-mgr (VP)	6	19%	US	1	3%
11–15 years	10	31%				Secondary	2	6%	4. Progmgr/IT-head (SVP)	8	25%			
> 15 years	13	41%				Unknown	3	9%	5. IT-Director (EVP)	7	22%			
Unknown	1	3%												
Totals	32	100%		32	100%		32	100%		32	100%		32	100%

Table 4
Principal Component Analysis.

Component			
	1	2	3
RiskProp1	**0.807**	0.210	0.038
RiskProp2	**0.802**	0.113	0.027
RiskProp3	**0.756**	−0.240	0.079
RiskProp4	**0.762**	−0.247	0.024
RiskProp5	**0.817**	0.029	−0.089
Gender	0.020	−0.005	**0.996**
Actor–ObserverRole	−0.006	**0.951**	−0.004

Rotation Method: Varimax with Kaiser Normalization.

5.3. Analytical approach

We used a single-item, three-level scale (low, medium, and high) for measuring perceived risk because this was the approach used in the bank where we conducted the study, and we treated this as an interval scale.[3] Before proceeding further with our main analysis, we explored whether risk propensity was a function of observer role and whether there was homogeneity of variance between the two groups (IT managers and IT auditors). An independent sample *t*-test showed that there was no significant difference in risk propensity between the IT auditors and IT managers who participated in our study ($t = -0.792$; $p = 0.431$). In addition, Levene's test for homogeneity of variance indicated that there was no significant difference in variance between the two groups ($F = 1.515$; $p = 0.222$).

Given these results, we proceeded with our main analysis and ran a 3 × 3 × 2 mixed-design ANOVA to test our hypotheses. This design is an extension of the two-way repeated-measures ANOVA, and it is typically used for the analysis of within-subject treatments across multiple groups of respondents. The within-subject dependent variable *perceived risk*$_{prob,impact}$ was measured in the following sequence: *perceived risk*$_{high,high}$; *perceived risk*$_{high,low}$; *perceived risk*$_{high,medium}$; *perceived risk*$_{medium,low}$; *perceived risk*$_{low,low}$; *perceived risk*$_{medium,high}$; *perceived risk*$_{low,high}$; *perceived risk*$_{medium,medium}$, and *perceived risk*$_{low,medium}$. The between-subject factor was *actor–observer role*, and we introduced *risk propensity* as a covariate.

ANOVA assumes that the scores obtained under different conditions are independent. Because this assumption cannot be met in a repeated-measures design, an additional assumption of sphericity is added, which means that the relationship between pairs of experimental conditions is similar. To confirm that this assumption was met, we performed Mauchly's test, which tests the hypothesis that variances of the differences are equal between treatment levels [61]. Our results indicated that the assumption of sphericity had not been violated for the main effect of probability, $\chi^2(2) = 4.45$, $p = 0.11$, and impact, $\chi^2(2) = 0.272$, $p = 0.873$. As such, it is reasonable to conclude that the variances of the differences are roughly equal and that the F-ratios in our ANOVA are valid.

5.4. Hypothesis testing

As noted earlier, a 3 × 3 × 2 mixed-design ANOVA was conducted to test our hypotheses. The test of between-subject effects showed that actor–observer role was significant ($F = 10.81$; $p = 0.002$) and in the expected direction with a partial eta-squared effect size statistic of 0.129, indicating a medium effect following Cohen's thresholds. Specifically, our results confirm that IT managers and IT auditors have different risk perceptions regarding the same underlying risk scenarios and that consistent with the actor–observer asymmetry perspective, IT managers' risk perceptions are lower than IT auditors' risk perceptions, thus supporting H1.

From the analysis of within-subject effects, we identified a significant main effect of risk impact on perceived risk ($F = 517.68$; $p < 0.001$) having a partial eta-squared effect size statistic of 0.876, indicating a large effect following Cohen's thresholds. Specifically, consistent with prior research, we found that increased risk impact is positively associated with risk perception, thus supporting H2. The analysis of within-subject effects also showed a significant main effect of risk probability on perceived risk ($F = 33.94$; $p < 0.001$) with a partial eta-squared effect size statistic of 0.317, indicating a large effect following Cohen's thresholds. Specifically, we found that increased risk probability is positively associated with risk perception, thus supporting H3.

Finally, we also found a significant interaction effect of *probability x actor–observer role* on perceived risk ($F = 3.46$; $p = 0.034$) with a partial eta-squared effect size statistic of 0.045, indicating a small effect following Cohen's thresholds. This result shows that there is a moderation effect due to actor–observer role and that consistent with the actor–observer asymmetry perspective, the relationship between risk probability and risk perception is stronger for IT auditors than for IT managers, thus supporting H4.

Although we did not theorize that actor–observer role would moderate the effect of risk impact on risk perception, we tested for this as part of our analysis. We found no significant interaction effect of *impact x actor–observer role* ($F = 1.68$; $p = 0.189$). Thus, as expected, actor–observer asymmetry appears to only influence the relationship between risk probability and risk perception and not the relationship between risk impact and risk perception. For reasons of completeness and to facilitate future *meta*-analysis on role-based risk perceptions, we also calculated the less common generalized eta-squared statistics, as advised by Bakeman [62].[4]

[3] Although one could argue that this should be treated as an ordinal scale, Blumberg et al. [60,p.444] suggested that parametric test results in this type of situation do not differ from nonparametric test results in terms of significance and power. Therefore, we used a mixed-design ANOVA for our hypothesis testing. However, for the sake of robustness, we further explored the effect of actor–observer role on perceived risk by running a series of nine ordinal regressions (one for each combination of risk impact and risk probability) and compared the results using corresponding ANOVAs. The pattern of results obtained was fully consistent regardless of the method used.

[4] Therefore, we transferred our data from SPSS to R, recalculated the partial eta-squared statistics, and calculated the generalized eta-squared statistics following the guidelines and formula by Olejnik & Algina [63] and Bakeman [62] for the specific design of our study. For hypothesis 1, we used the formula $SS_a/(SS_a + SS_{s/a} + SS_{Pa} + SS_{Ps/}$

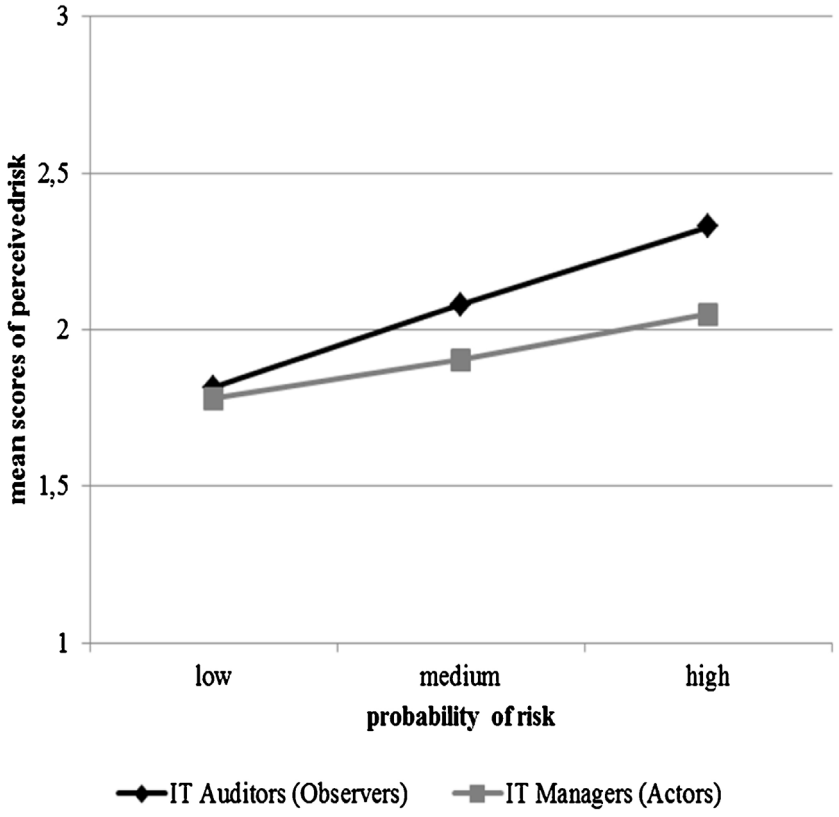

Fig. 2. Interaction between actor–observer role and risk probability.

Fig. 2 provides a visual representation of the interaction between risk probability and actor–observer role, which is consistent with Aiken and West [64,p. 123]. The x-axis distinguishes between three levels of risk probability (low, medium, and high). The y-axis represents the estimated marginal mean scores of perceived risk as calculated from our model. The gray line represents the "actors" (IT managers), whereas the black line depicts the "observers" (IT auditors) who participated in our quasi-experiment. The significance of the variable *probability x actor–observer role* is reflected in the different slopes of the lines. The black line is steeper than the gray line, which indicates that the actors (IT managers) in our study reacted less strongly to changes in risk probability than did the observers (IT auditors). Because the lines do not cross over within the range of possible values, the interaction between probability and actor–observer role is classified as an ordinal interaction [64,p. 22].

5.5. Ruling out some potential rival explanations

The assignment of subjects to treatments was driven by our choice to perform a quasi-experiment with actual practitioners who had significant work experience as a manager (in a position where they act on risks) or as an auditor (in a position where they observe and monitor risks). Therefore, our participants were not assigned randomly to treatment conditions, and thus, there is a potential for nonequivalence between the groups and threat of selection bias. For example, the differences that we observed between managers and auditors could have been caused by diffences between the two groups that did not relate to job role. By examining the two groups, however, we could rule out the possibility that the effects we observed were due to differences in gender distribution, work experience, function level, or nationality. We also considered and could rule out another rival explanation, namely that IT auditors and IT managers exhibit different risk perceptions because of the underlying differences in risk propensity. If IT auditors had significantly lower risk propensity as a group than IT managers, this might explain the pattern of results that we obtained in our quasi-experiment, as risk propensity is inversely related to risk perception. However, we can rule out this particular rival explanation with a high degree of confidence because we measured risk propensity and found no significant differences between IT auditors and IT managers.

Another type of randomization issue pertains to possible order effects associated with the repeated-measures aspect of our design. Specifically, although the nine cases to which participants were exposed were arranged in a random fashion with regard to the impact and probability manipulations, all participants were exposed to the nine scenarios in the same order. We do not, however, believe that this posed a significant threat to the validity of our findings for several reasons. Two common causes of order effects are fatigue and time-oriented learning [65]. With regard to fatigue, our pilot tests indicated that participants could easily complete the quasi-experiment in 10–15 min, and no one stopped in the middle or complained about the length of the quasi-experiment. This suggests that there was relatively little risk of order effects due to fatigue.

(*footnote continued*)
$a + SS_{Qa} + SS_{Qs/a} + SS_{PQa} + SS_{PQs/a}$) for the generalized eta squares and the formula $SS_a/(SS_a + SS_{s/a})$ for the partial eta squares, where *a*, *P*, and *Q* refer to our variables *actor–observer role*, *probability*, and *impact*, respectively, and *s* represents the subject factor. For hypothesis 2, we used the formula $SS_Q/(SS_Q + SS_a + SS_{s/a} + SS_{Pa} + SS_{Ps/a} + SS_{Qa} + SS_{Qs/a} + SS_{PQa} + SS_{PQs/a})$ for the generalized eta squares and the formula $SS_Q/(SS_Q + SS_{Qs/a})$ for the partial eta squares. For hypothesis 3, we used the formula $SS_P/(SS_P + SS_a + SS_{s/a} + SS_{Pa} + SS_{Ps/a} + SS_{Qa} + SS_{Qs/a} + SS_{PQa} + SS_{PQs/a})$ for the generalized eta squares and the formula $SS_P/(SS_P + SS_{Ps/a})$ for the partial eta squares. For hypothesis 4, we used the formula $SS_{Pa}/(SS_{Pa} + SS_a + SS_{s/a} + SS_{Ps/a} + SS_{Qa} + SS_{Qs/a} + SS_{PQa} + SS_{PQs/a})$ for the generalized eta squares and the formula $SS_{Pa}/(SS_{Pa} + SS_{Ps/a})$ for the partial eta squares. As expected from these formulas, the generalized eta squares offer lower values than the partial eta squares presented in our paper, resulting in recalculated effect size of 0.024 (with $p = 0.002$) for hypothesis 1, an effect size of 0.596 (with $p < 0.001$) for hypothesis 2, an effect size of 0.090 (with $p < 0.001$) for hypothesis 3, and an effect size of 0.010 (with $p = 0.034$) for hypothesis 4.

With regard to time-oriented learning, we performed two additional analyses to test for any learning effects that may have occurred due to order of presentation. First, we examined the standard deviations associated with IT auditors' and IT managers' risk perceptions for each of the nine individual cases presented. If there had been learning effects, we would expect that the standard deviations would decrease as our participants went through the nine risk assessments. The standard deviations were tightly centered, ranging from 0.21 to 0.59 for the IT auditors and from 0.42 to 0.72 for the IT managers, and did not show any decreasing trend as participants moved through the case. Second, we performed an analysis in which we examined only the first risk scenario that a participant received, thus removing the possibility of order effects. Our findings were consistent with what we obtained when we aggregated across the nine risk scenarios. This suggests that if any order effects were present, they did not materially affect our results. Taken together, the above analyses indicate that we can be confident that order effects do not pose a threat to the validity of our findings.

The actor–observer perspective that we draw upon provides the theoretical logic for the hypotheses tested in our quasi-experiment; however, we did not measure whether respondents actually saw themselves as actors or observers at the time the quasi-experiment was conducted. The results of 10 follow-up interviews with the IT auditors, who had participated in our quasi-experiment, however, showed that all the IT auditors associated the role of the IT manager with that of an actor (i.e., one who is sitting in the driver seat in a position to manage IT risks) and that all of them associated the role of the IT auditor with that of an observer (i.e., one who is sitting in the passenger seat having a position to observe and issue risk warnings). This was illustrated by one of the respondents who said "the observer position is inherent to the role as an IT auditor and IT managers consider themselves in the position as actors sitting at the driver seat. An IT manager once said to me (i.e. the IT auditor): 'this is *my* department and it is *my* responsibility to take actions and *you* are not in the position to do my job', so these roles are clearly divided." Thus, the results of our interviews lend support for the theoretical logic underpinning our study.

The interviews also provided evidence that IT auditors tend to perceive risks to be greater than IT managers do, and this is something that was frequently observed in audit engagements. The interviews also illustrated that these differences between IT managers and IT auditors mainly focus on the probability of IT risks to occur. This was illustrated by one of the respondents who told us: "In my twenty years of practice as an IT auditor I hardly ever argued with an IT manager about the *severity* of consequences of an IT risk to occur. They know damn well themselves the impact when an event would occur, especially since such would have consequences to them personally. On the other hand, I very often argue with IT managers about the *chance* of an IT risk to occur. Managers often say that such an IT risk had never occurred to them in the past and that they don't believe this will happen to them in future either. They say we [IT auditors] are overstating chances since we are not actively involved in daily operations and because we observe from a distance."

The four respondents who had switched between the role of IT auditor and IT manager in their career reported that their perception of IT risks changed as a function of role. This was illustrated by one of our respondents who had moved from the IT auditor role to the IT manager role and back: "My role had a huge effect on how I perceived IT risks. In the position as an IT manager I knew for myself what actions I would take if an event would occur. If I had the idea that I could actually take these actions myself in case this was needed, I perceived risks to be much lower than I did when I was in the role as an IT auditor and was not in the position to take actions myself." These findings are consistent with what one would expect based on the actor–observer asymmetry perspective. Thus, the results from our postexperiment interviews are consistent with the results of our quasi-experiment and lend additional support for the notion that IT managers and IT auditors perceive IT risks differently and that the actor–observer asymmetry perspective provides a plausible theoretical explanation for this.

6. Discussion and implications

In the introduction of our paper, we showed that the movement toward IT auditing is based on the premise that IT auditors will improve an organization's capacity to identify and manage IT risks, but we pointed out that such a premise hinges on whether IT auditors differ from IT managers in terms of risk perceptions. The aim of our study was therefore to probe for possible differences in risk perception between IT auditors and IT managers. The results of our study suggest that the emphasis now being placed on IT auditing may indeed have value in that IT auditors do exhibit heightened risk perceptions relative to IT managers.

6.1. Implications for research

Prior research has established that different stakeholders can have varying perceptions of IT risk [1,39], but this is the first study that has specifically compared the risk perceptions of IT managers and IT auditors. Given the increasing emphasis on IT auditing, it is important to know whether IT auditors differ from IT managers in terms of risk perceptions. Drawing on the actor–observer asymmetry perspective, we theorized that IT auditors would have heightened risk perceptions relative to IT managers. Consistent with our theorizing, we found that when exposed to the same underlying risks, IT auditors' perceived risk was greater than IT managers' perceived risk.

Our results also indicated that actor–observer role moderated the relationship between risk probability and risk perception such that the relationship was stronger for observers (i.e., IT auditors) than for actors (i.e., IT managers). In other words, our study provides empirical evidence that as risk probability increases, the increase in perceived risk will be greater for observers (i.e., IT auditors) than it is for actors (i.e., IT managers). This moderating effect applied to the probability aspect of risks and not to the impact aspect of risks and was consistent with the predictions that we made based on the actor–observer asymmetry perspective.

Our study also contributes to existing knowledge by testing expectations from the actor–observer perspective with working professionals and realistic business scenarios as opposed to prior research that relied on experiments with student subjects and somewhat artificial tasks (such as coin tosses). In doing so, we show that the actor–observer perspective helps us to understand differences in IT auditors' vs. IT managers' risk perceptions.

6.2. Implications for practice

Identifying and managing IT risks has become ever more important, and this has led to an increased interest in IT auditing [41,p. 6]. To justify the additional investment in IT auditing, it is therefore important to know whether IT auditors perceive risks differently than IT managers. Our study has important implications for practice because it is the first to provide concrete evidence on this point. The results of our work clearly show that when exposed to the same set of IT risks, IT auditors' risk perceptions are higher than those of IT managers. If practitioners want to create an early warning system for detecting IT risks, then the increased emphasis on IT auditing may indeed be one way to achieve this as our work shows that IT auditors react more strongly than IT managers to increases in risk probability. As such, auditors can add value by serving as devil's advocates. If, as our results suggest, auditors' perceptions of risk differ systematically from managers' perceptions of risk, they (i.e., auditors) should be in a good position to challenge managers' perceptions of risk.

Our study also provides key insight into the differences in IT auditors' vs. IT managers' risk perceptions. Specifically, the actor–ob-

server asymmetry perspective suggests that IT managers are apt to have lower risk perceptions than IT auditors as IT managers (as actors) are closer to the activity and may develop illusions of control that exert a downward bias on their risk perceptions relative to that of IT auditors who play the observer role. This has important implications for practice, as many organizations wrestle with the challenge of how to deploy their IT auditors in the most effective manner possible.[5]

In some cases, organizations have found that the traditional IT auditor role as watchdog can create friction and lead to distrust between IT managers and IT auditors [66]. In extreme cases, IT auditors are regarded as obstructionists who add little or no value to systems and processes treated as "the enemy" by IT managers. When this occurs, dysfunctional behaviors can ensue whereby individuals cease to cooperate with the auditors or actively hide information from them. To avoid this problem, some organizations have tried to position their IT auditors as internal consultants who are there to help, not to be obstructionists. One way of accomplishing this is to embed IT auditors in work teams, thereby making them more of a participant rather than a detached observer. Our work, however, suggests that this strategy can backfire if IT auditors lose their ability to play the observer role and become no more adept at perceiving risk than those who they are monitoring.

Thus, another implication of our study is related to the communication between IT auditors and IT managers, which is key to IT auditors' effectiveness. It is important that IT auditors and IT managers develop a better mutual understanding that their respective roles can lead to actor–observer asymmetry when they assess IT risks. It is our hope that this will contribute to better communication of the unique perspective that each party brings to the table.

6.3. Limitations and directions for future research

Although our research hypotheses and results are consistent with the actor–observer asymmetry perspective, we did not actually measure the extent to which our IT manager participants viewed themselves as actors, or the extent to which our IT auditor participants viewed themselves as observers. Thus, even though we gathered additional evidence through interviews that lends support for the actor–observer asymmetry perspective, we cannot rule out the possibility that there might be other theoretically plausible explanations for the pattern of results we observed. One such possibility is that IT auditors and IT managers exhibit different risk perceptions because of the selective perception that is grounded in expertise or training associated with a functional role (rather than one party being an actor and the other party being an observer). Dearborn and Simon [67] claimed that managers selectively perceive information according to their functional background, and Beyer et al. [68] suggest that functional background can also cause managers to ignore certain stimuli. Although one could argue that selective perception in this instance is driven by actor–observer asymmetry, we cannot rule out the possibility that the differences in risk perceptions that we observed are because of the selective perception that is grounded in functional background or training, but which is not necessarily due to actor–observer asymmetry. Further research on the effects of functional background and training is warranted.

A second limitation of our study involves the use of a single-item measure for risk perception. Although single-item measures are generally to be avoided because they cannot be assessed for reliability, we employed a single-item measure in this study because we wanted to employ the same measure that was normally used within the organization. Further, since each participant was asked to respond to nine different cases, it would not have been practical for length reasons to use multiple measurement items. Moreover, we reasoned that the repeated-measures component of our design created a situation in which participants were recording their risk perceptions multiple times across nine different scenarios, thereby strengthening the confidence that we can have in our findings.

A third limitation of our study is that there were very few women in our pool of participants. Thus, our findings are based on a participant pool that was largely comprised of male participants, and the fact that we did not find any gender effects, given the small number of women in our study, is not surprising. Further research would need to be conducted to determine whether our results generalize to a participant pool comprised of women.

Fourth, although our research design has distinct strengths, it did not allow us to include all the contextual aspects of organizational life. Thus, our study does not account for the social interactions that may occur in the workplace related to IT risks. Prior research [69] shows that social interaction may strongly polarize existing risk perceptions and bring either a shift toward lower levels of perceived risk—a risky shift [70]—or toward higher levels of perceived risk—a cautious shift [71]. The social interactions between IT auditors and IT managers and the consequences of these interactions represent an interesting avenue for further research. The effectiveness of social interactions between internal auditors and managers has thus far received little attention in the auditing research [72], even though it has been highlighted as critically important to the internal audit effectiveness in organizations [73].

Fifth, risk is multifaceted, and it would be fruitful to conduct further research to investigate how factors other than probability and impact may affect risk perceptions. One such factor is national culture. Although we did not observe significant differences between the Dutch and U.K. employees of the bank in which we conducted our research, we expect that with Brexit and the recent movement toward populism, the differences in national culture between auditors and managers may become more salient in the future as compared to what we observed in this study. The implication that such shifts will have on the auditing profession and how this will affect risk assessments in multinational corporations is another area for future research.

Finally, given the increased role that IT auditors are playing in many organizations, there is a need for additional research on the ways in which auditors and IT managers can jointly or separately evaluate IT system risks. Some experimentation around the inclusion of IT auditors in project teams and its effect on risk assessments and team behavior may be beneficial and could help establish interdisciplinary guidelines that would advance practice.

7. Conclusion

Drawing upon the actor–observer asymmetry perspective, this study provides insight into differences between IT managers' and IT auditors' risk perceptions and strong empirical evidence that such differences in perception do exist. Through a quasi-experiment with 76 employees of a financial institution, we found that IT auditors' perceived risks were higher than their IT management colleagues. Additionally, IT auditors reacted more strongly than IT managers to increases in risk probability. An improved understanding of the differences in IT managers' vs. IT auditors' risk perceptions can be very helpful to organizations as they wrestle with the challenge of how to assess and monitor IT risks. Based on our study, it is quite clear that perceptions of IT risks are shaped by the roles that people play in organizations. Given this, we believe that further research is warranted to explore the accuracy of risk perceptions held by IT managers and IT auditors and to find the best way to leverage IT auditors in practice.

Acknowledgments

We thank Mr. Bert Zwiers for his very important role during the

[5] On the basis of a 2013 KPMG survey across 400 organizations in Europe, Africa, and the Middle East, "fewer than half of the survey participants said that they were satisfied with the IT Internal Audit service they receive" [41,p. 8].

initial stages of this study, more specifically, in the preparation of the cases and in data collection.

Appendix A. Cases

The participants were asked to read the following case material. It consists of nine different hypothetical situations concerning IT risks. They are shown here including their respective probability and impact indicators as they were presented to the participants. The participants were asked to provide the risk ratings themselves. The cases correspond with the varying input of probability and impact, according to the company's risk framework.

Finding 1 – Lack of antivirus controls **Impact: High** **Probability: High**

To protect against the negative impact of malicious software such as computer viruses, an anti-virus strategy should be in place. This strategy should detail how the company's infrastructure and computer systems are to be protected by anti-virus software, firewalls, or other measures. During the audit, the following came to our attention: (1) no anti-virus strategy is in place, (2) approximately 40% of the workstations contain no virus scanner, and (3) the virus scanners on servers are from different suppliers, a long time out of date, and not maintained. The risk posed by the lack of these controls is compounded by the fact that users have full access to their workstations and may install software that is not inspected, verified, and controlled by the network administration team. The severity of this situation is exemplified by the frequent downtime of both servers and workstations due to the effects of viruses, as reported by the network infrastructure team. The risk exists that downtime increases and information is compromised if no further action is taken, leading to significant operational losses due to inoperable computer systems. Besides operational effects, a reputational risk exists because of the deteriorated service levels.

Finding 2 – Insufficient helpdesk capacity **Impact: Low** **Probability: High**

Users of computer systems in large companies frequently face problems that they cannot solve themselves. This includes software problems, obtaining password resets, or requesting new hardware or software. For this reason, a helpdesk should be available to these users that can assist them quickly and efficiently with their requests. It was noted that the current helpdesk is understaffed. The average waiting time was measured to be 15 min, and a resolution for nonurgent requests took 3 days on average, rather than the 1 day as mentioned in the service-level agreement. The risk exists that users are not assisted adequately or quickly enough with their problems because of the lack of resources. This may lead to frustration in system users and to operational losses by unnecessary time spent on the phone with the helpdesk or waiting for resolution of a problem.

Finding 3 – Inadequate system capacity **Impact: Medium** **Probability: High**

Computer systems require different resources. These may vary from processing capacity to storage capacity and from response time to network bandwidth. To ensure that the right resources are available to all systems, a capacity management plan should be in place for all systems. The storage capacity of the logistic planning tool was found to be within its limit. More than 98% of the disk storage space was utilized, and the system administrator reported weekly outages because of this. Although a system is considered important rather than critical, continued malfunction of the system will lead to further interruptions in the planning process. This has led to increased delivery times and overstocked storage rooms. In a few instances, service-level agreements with clients have not been met and complaints may increase if these problems are not solved.

Finding 4 – Lack of back-up facility for labeling system **Impact: Low** **Probability: Medium**

When employing computer systems in the daily workflow of a company, continued operation without disturbance is necessary for effective production. For this reason, it is a best practice to ensure that for an automated system, a disaster recovery procedure is written and implemented. This would include the means to quickly restore a system in case of problems by creating back-ups of the system. It was noted that the mail labeling system is old and that the hardware is at the end of its expected lifetime. This has already led to the replacement of system parts last year causing a temporary unavailability of the system. When the system is not available, the mail room must return to manually producing the labels for posting, which as in the past will require overtime of the employees finish their work until the system is restored. The risk exists that mail is not delivered timely to customers.

Finding 5 – Lack of business continuity for audit department **Impact: Low** **Probability: Low**

To ensure continued operation in case of a disaster or emergency, businesses require a business continuity plan that will enable them to pick up normal operations as quickly as possible, should such a situation occur. It was noted that for the audit department, such a plan was not available at the time of the audit. Neither was a call tree, containing the details of all staff available as a minimum communication plan. The risk exists that in case of an emergency or disaster, the audit department cannot quickly resume normal operations, and reports will not be delivered when they are due.

Finding 6 – Inadequate client acceptance policy **Impact: High** **Probability: Medium**

It is in the long-term interest of a company to set up relationships with reputable and trustworthy clients. To this end, a proper client acceptance policy should be in place to ensure that no dealings take place with criminal, financially unsound, or otherwise unwanted clients. A client acceptance policy was not present at the time of our review. Neither were files available to store important information on clients such as chamber of commerce and lists of authorized signatories. Although the client relationship managers of the company are very experienced and have taken anti-money laundering courses, the risk of attracting unwanted customers remains. This may lead to defaulted payments or reputational damage when the company is connected to criminal customers in the media or the loss of an operational license when regulatory bodies judge the client take-on process as inadequate.

Finding 7 – Single point of failure in company network **Impact: High** **Probability: Low**

When company processes cross borders because of an international client base, reliable network connectivity is of the utmost importance. For this reason, these network connections should be redundant; if one connection fails, the other can take over so that operational processes may continue uninterrupted. The current company network infrastructure is based on a star topology. This means that all network traffic comes through one location and all other geographic locations are connected to it. All these connections are redundant, this means two network lines, owned by different network operators, connect all remote locations to the central location. Despite the redundancy of the network, there remains a single point of failure in the central location. If the network connection in this location is lost, none of the other locations can communicate with each other. The risk therefore exists that productivity comes to a full standstill when problems arise in the central location.

Finding 8 – Inadequate change management process **Impact: Medium** **Probability: Medium**

To ensure that changes to the company's IT systems are implemented without problems, a change management process should exist. This process should ensure that changes are well planned, proper approvals are obtained, and the impact on other systems is acceptable. It was noted that the current change management process is inadequate. The only evidence of control over changes in the IT systems was a list of changes to be performed in the coming period. It was not noted how large the change is, what impact the changes have, when they should occur, and what the dependencies are. The systems in use are not highly complex, but changes are implemented regularly. Additionally, the systems are not essential for continuous production, but they will cause delays and ineffective processing when unavailable.

Finding 9 – Inadequate service-level agreement **Impact: Medium** **Probability: Low**

To ensure that applications are serviced in line with requirements, service-level agreements should be drawn up between the service provider and the client. These agreements contain service windows, maximum time between failures, response times, etc. It was noted that for several nonessential but important systems that are hosted by an external service provider, no service-level agreement was available, but that support was given on a best effort basis. In the current situation, when problems arise at the providers' side, it is up to them to prioritize what customer to service as a matter of priority. At present, this will have to be accepted with no contractual means of ensuring that the required level of service is maintained. This risk is mitigated by the fact that the provider is recognized as a large professional party with a good reputation.

Appendix B. Invitation

The invitation to participate and answer the questionnaire was as follows:

'Dear participant,

You've been sent the questionnaire below as part of research conducted for the Erasmus University Rotterdam. All results will be treated confidentially and only generalised results will be published.

We would kindly ask you to complete the questionnaire by assigning the fictitious issues below a risk rating of high, medium, or low and by also answering the first set of questions. A definition of risk is included with this questionnaire to assist with assigning these ratings. Please note that the fictional issues are shortened and explicitly written for the purpose of this research. Whenever the risk rating is not clear from the issue, please select the risk rating that is nearest to the probable actual rating. In any case, you must pick one.

When the questionnaire is completed you are asked to answer the following open questions:

- Please describe why you were able or unable to assess the risk in the issues.
- Please indicate what factors influence the risk rating you have assigned to the issues. Name at least five factors.
- Please provide any other comments you might have.'

Appendix C. Risk Definitions [Company Name]

Low Risk: Audit finding, the solution to which may lead to improvement in the quality and/or efficiency of the organizational entity or process being audited. Risks of damage to the organization are limited. Routine management attention is warranted.

Medium Risk: Audit finding that may lead to (1) financial losses; (2) loss of controls within the organizational entity or process being audited; (3) reputation damage; and/or (4) adverse regulatory impact. Timely management attention is warranted.

High Risk: Serious audit finding that may lead to (1) substantial losses, possibly in conjunction with other weaknesses in the control framework of the organizational entity or process being audited; (2) serious violation of industry best practice; (3) serious reputation damage; and/or (4) significant adverse regulatory impact. Immediate management attention is required.

Appendix D. Measurement Items for Risk Propensity

The risk propensity questionnaire presented to both auditors and managers is as follows:

We are interested in everyday risk-taking. Please could you tell whether you would expose yourself to the following risks.

Please use the scales as follows: 1: never, 2: rarely, 3: quite often, 4: often, 5: very often

a)	Business Continuity Risks	e.g., back-up system, disaster recovery procedures, business continuity planning	1 2 3 4 5
b)	Change Management Risks	e.g., full change documentation, formal approval, impact analysis	1 2 3 4 5
c)	Configuration Management Risks	e.g., inventory of configuration items, versioned software releases, asset inventory	1 2 3 4 5
d)	Testing Risks	e.g., presence test, acceptance, development, production environment, user acceptance testing	1 2 3 4 5
e)	Security Risks	e.g., system access, encryption of data, integrity of data	1 2 3 4 5
f)	Service-Level Risks	e.g., service-level agreements, definition of performance indicators, performance measurement	1 2 3 4 5

References

[1] S. Liu, J. Zhang, M. Keil, T. Chen, Comparing senior executive and project manager perceptions of IT project risk: a Chinese delphi study, Inf. Syst. J. 20 (4) (2010) 319–355.
[2] H. Drummond, Are we any closer to the end? Escalation and the case of Taurus, Int. J. Project Manage. 17 (1) (1999) 11–16.
[3] S.L. Pan, G.S.C. Pan, M. Newman, D. Flynn, Escalation and de-escalation of commitment to information systems projects: insights from a project evaluation model, Eur. J. Oper. Res. 173 (3) (2006) 1139–1160.
[4] D. Johnstone, S. Huff, B. Hope, IT projects: conflict, governance and systems thinking, 39th Hawaii International Conference on System Sciences, Hawai, 2007.
[5] M. Mähring, M. Keil, Information technology project escalation: a process model, Decision Sciences 39 (2) (2008) 239–272.
[6] J.J. Jiang, G. Klein, Supervisor support and career anchor impact on the career satisfaction of the entry-level information systems professional, J. Manage. Inf. Syst. 16 (3) (1999) 219–240.
[7] R. Baskerville, P. Spagnoletti, J. Kim, Incident-centered information security: managing a strategic balance between prevention and response, Inf. Manage. 51 (1) (2014) 138–151.
[8] S. Alter, M. Ginzberg, Managing uncertainty in MIS implementation, Sloan Manage. Rev. 20 (1) (1978) 23–31.
[9] M. Ginzberg, Early diagnosis of MIS implementation failure: promising results and unanswered questions, Manage. Sci. 27 (4) (1981) 459–478.
[10] F.W. McFarlan, Portfolio approach to information systems, Harv. Bus. Rev. 59 (5) (1981) 142–150.
[11] R.N. Charette, Software Engineering Risk Analysis and Management, Intertext Publications, New York, 1989.
[12] B.W. Boehm, Software risk management: principles and practices, IEEE Software 8 (1) (1991) 32–41.
[13] H. Barki, S. Rivard, J. Talbot, Toward an assessment of software development risk, J. Manage. Inf. Syst. 10 (2) (1993) 203–225.
[14] R. Schmidt, K. Lyytinen, M. Keil, P. Cule, Identifying software project risks: an international delphi study, J. Manage. Inf. Syst. 14 (4) (2001) 5–36.
[15] L. Wallace, M. Keil, A. Rai, How software project risk affects project performance: an investigation of the dimensions of risk and an exploratory model, Dec. Sci. 35 (2) (2004) 289–312.
[16] A. Bharadwaj, M. Keil, M. Mähring, Effects of information technology failures on the market value of firms, J. Strategic Inf. Syst. 18 (2) (2009) 66–79.
[17] J.S.-C. Hsu, S.-P. Shih, Y.W. Hung, P.B. Lowry, The role of extra-role behaviors and social controls in information security policy effectiveness, Inf. Syst. Res. 26 (2) (2015) 282–300.
[18] J.L. Spears, H. Barki, R.R. Barton, Theorizing the concept and role of assurance in information systems security, Inf. Manage. 50 (7) (2013) 598–605.
[19] IT-Governance-Institute, CobiT 4.1 – Control Objectives of Information and Related Technology Rolling Meadows, (2007).
[20] R.E. Cascarino, Auditor's Guide to IT Auditing, 2nd ed., Wiley, New Jersey, 2012.
[21] M. Siponen, M.A. Mahmood, S. Pahnila, Employees' adherence to information security policies: an exploratory field study, Inf. Manage. 51 (2) (2014) 217–224.
[22] H. Cavusoglu, H. Cavusoglu, J.-Y. Son, I. Benbasat, Institutional pressures in security management: direct and indirect influences on organizational investment in information security control resources, Inform. Manage. 52 (4) (2015) 385–536.
[23] S.V. Grabski, S.A. Leech, P.J. Schmidt, A Review of ERP research: a future agenda for accounting information systems, J. Inf. Syst. 25 (1) (2011) 37–78.
[24] R.S. Debreceny, Betwixt and between? bringing information systems and accounting systems research together, J. Inf. Syst. 25 (2) (2011) 1–9.
[25] M.L. Weidenmier, S. Ramamoorti, Research opportunities in information technology and internal auditing, J. Inf. Syst. 20 (1) (2006) 205–229.
[26] I. Solomon, K. Trotman, Experimental judgment and decision research in auditing: the first 25 years of AOS, Account. Organiz. Soc. 28 (4) (2003) 395–412.
[27] S.G. Sutton, The changing face of accounting in an information technology dominated world, Int. J. Account. Inf. Syst. 1 (1) (2000) 1–8.
[28] M.A. Vasarhelyi, Editor's letter, J. Emerging Technol. Account. 3 (1) (2006) i–vi.
[29] M. Gibbins, B. Pomeroy, Reflections on continuous reporting and auditing, Account. Perspect. 6 (3) (2007) 291–304.
[30] M. Jans, M. Alles, M. Vasarhelyi, A field study on the use of process mining of event logs as an analytical procedure in auditing, Account. Rev. 89 (5) (2014) 1751–1773.
[31] M.B. Curtis, J.G. Jenkins, J.C. Bedard, D.R. Deis, Auditors' training and proficiency in information systems: a research synthesis, J. Inf. Syst. 23 (1) (2009) 79–96.
[32] J. Blaskovich, N. Mintchik, Information technology outsourcing: a taxonomy of prior studies and directions for future research, J. Inf. Syst. 25 (1) (2011) 1–36.
[33] M.P. Neely, J.S. Cook, Fifteen years of data and information quality literature: developing a research agenda for accounting, J. Inf. Syst. 25 (1) (2011) 79–108.
[34] L. Wallace, H. Lin, M.A. Cefaratti, Information security and sarbanes-Oxley compliance: an exploratory study, J. Inf. Syst. 25 (1) (2011) 185–211.
[35] S.B. Sitkin, A.L. Pablo, Reconceptualizing the determinants of risk behavior, Acad. Manage. Rev. 17 (1) (1992) 9–38.
[36] P. Slovic, Perception of risk, Science 236 (4799) (1987) 280–285.
[37] C. Posey, T.L. Roberts, P.B. Lowry, R. Hightower, Bridging the divide: a qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders, Inf. Manage. 51 (5) (2014) 551–567.
[38] H. Mouratidis, H. Jahankhani, M.Z. Nkhoma, Management versus security specialists: an empirical study on security related perceptions, Inf. Manage. Comput. Secur. 16 (2) (2008) 187–205.
[39] M. Keil, A. Tiwana, A. Bush, Reconciling user and project manager perceptions of IT project risk: a delphi study, Inf. Syst. J. 12 (2) (2002) 103–119.
[40] T. Addison, E-commerce project development risks: evidence from a delphi survey, Int. J. Inf. Manage. 23 (1) (2003) 25–40.
[41] KPMG, KPMG's IT Internal Audit Survey, (2013) Published on 2013 November 6, http://www.kpmg.com/CH/en/Library/Articles-Publications/Documents/Advisory/pub-20131106-it-internal-audit-survey-en.pdf , Retrieved on 2014 January 7.
[42] D. Kahneman, A perspective on judgment and choice: mapping bounded rationality, Am. Psychol. 58 (9) (2003) 697–720.
[43] M.S. Horswill, F.P. McKenna, The effect of perceived control on risk taking, J. Appl. Soc. Psychol. 29 (2) (1999) 377–391.
[44] D. Fernandez-Duque, T. Wifall, Actor/Observer asymmetry in risky decision making, Judgm. Dec. Making 2 (1) (2007) 1–8.
[45] E.J. Langer, J. Roth, Heads i win, tails it's chance: the illusion of control as a function of the sequence of outcomes in a purely chance task, J. Pers. Soc. Psychol. 32 (6) (1975) 951–955.
[46] C. Helliar, A.A. Lonie, D.M. Power, C.D. Sinclair, Managerial attitudes to risk: a comparison of Scottish chartered accountants and U.K. managers, J. Int. Account. Auditing Taxation 11 (2) (2002) 165–190.
[47] B.A. Mellers, S. Chang, Representations of risk judgments, Organ. Behav. Hum. Decis. Process. 57 (2) (1994) 167–184.
[48] J.F. Yates, E.R. Stone, The Risk Construct in Risk-taking Behavior, Wiley, Chichester, 1992.
[49] S.A. Sherer, Measuring software failure risk: methodology and an example, J. Syst. Software 25 (3) (1994) 257–269.
[50] S.B. Sitkin, L.R. Weingart, Determinants of risky decision-making behavior: a test of the mediating role of risk perceptions and propensity, Acad. Manage. J. 38 (6) (1995) 1573–1592.
[51] E.J. Langer, The illusion of control, J. Pers. Soc. Psychol. 32 (2) (1975) 311–328.
[52] N.D. Weinstein, Unrealistic optimism about future life events, J. Pers. Soc. Psychol. 39 (5) (1980) 806–820.
[53] J.G. March, Z. Shapira, Managerial perspectives on risk and risk taking, Manage. Sci. 33 (11) (1987) 1404–1418.
[54] M. Keil, L. Wallace, D. Turk, G. Dixon-Randall, U. Nulden, An investigation of risk perception and risk propensity on the decision to continue a software development project, J. Syst. Software 53 (2) (2000) 145–157.
[55] K.R. MacCrimmon, D.A. Wehrung, Taking Risks: The Management of Uncertainty, The Free Press, New York, 1986.
[56] Z. Shapira, Risk Taking: A Managerial Perspective, Russel Sage Foundation, New York, 1995.
[57] W.R. Shadish, T.D. Cook, D.T. Campbell, Experimental and Quasi-experimental Designs for Generalized Causal Inference, Houghton Mifflin, 2002.
[58] N. Nicholson, E. Soane, M. Fenton-O'Creevy, P. Willman, Personality and domain-specific risk taking, J. Risk Res. 8 (2) (2005) 157–176.
[59] J.F. Hair, R.E. Anderson, R.L. Tatham, W.C. Black, Multivariate Data Analysis, Prentice Hall, Englewood Cliffs, 1998.
[60] B. Blumberg, D.R. Cooper, P.S. Schindler, Business Research Methods, 2nd european edition ed., McGraw-Hill, London, 2008.
[61] A. Field, Discovering Statistics Using SPSS, 3rd ed., Sage publications, London, 2009.
[62] R. Bakeman, Recommended effect size statistics for repeated measures designs, Behav. Res. Methods 37 (3) (2005) 379–384.
[63] S. Olejnik, J. Algina, Generalized eta and omega squared statistics: measures of effect size for some common research designs, Psychol. Methods 8 (4) (2003) 434–447.
[64] L.S. Aiken, S.G. West, Multiple Regression: Testing and Interpreting Interactions, Sage Publications, Thousand Oaks, 1991.
[65] P.C. Cozby, Methods of Behavioral Research, 10th ed., McGraw-Hill, New York, 2009.
[66] M. Keil, J. Smith, C.L. Iacovou, R.L. Thompson, The dynamics of IT project status reporting: a self-reinforcing cycle of distrust, J. Assoc. Inf. Syst. 15 (12) (2014) 879–912.
[67] D.C. Dearborn, H.A. Simon, Selective perception: a note on the departmental identification of executives, Sociometry 21 (2) (1958) 140–144.
[68] J.M. Beyer, P. Chattopadhyay, E. George, W.H. Glick, D. Ogilvie, D. Pugliese, The selective perception of managers revisited, Acad. Manage. J. 40 (3) (1997) 716–737.
[69] D.J. Isenberg, Group polarization: a critical review and meta-analysis, J. Pers. Soc. Psychol. 50 (6) (1986) 1141–1151.
[70] J.D. Rothwell, Risk-taking and polarization in small group communication, Commun. Educ. 35 (2) (1986) 182–185.
[71] D.M. Mackie, Social identification effects in group polarization, J. Pers. Soc. Psychol. 50 (4) (1986) 720–728.
[72] S. Ramamoorti, The psychology and sociology of fraud: integrating the behavioral sciences component Into fraud and forensic accounting curricula, Issues Account. Educ. 23 (4) (2008) 521–533.
[73] G. Sarens, M.J. Abdolmohammadi, Monitoring effects of the internal audit function: agency theory versus other explanatory variables, Int. J. Auditing 15 (1) (2011) 1–20.

Dr. Arno L.P. Nuijten is currently the Academic Director of the IT Auditing & Advisory Program at the Erasmus School of Accounting and Assurance, the Erasmus University Rotterdam, the Netherlands. His research interests are in the area of IT auditing, internal auditing, and managerial decision-making on IT risks in general and IT projects in particular. For over 25 years, he has consulted with large companies throughout Europe

on various business problems. Arno has a PhD in Information Science from Erasmus University and MSc in Information Systems from Tilburg University.

Dr. Mark Keil is currently the John B. Zellars Professor of Computer Information Systems at the J. Mack Robinson College of Business, Georgia State University, Atlanta, United States. His research focuses on IT project management and includes work on preventing IT project escalation, identifying and managing IT project risks, and improving IT project status reporting. His interests also include IT implementation and use. He has published more than 100 refereed papers and served on the editorial boards of many academic journals. He holds BSE, SM, and DBA degrees from Princeton University, M.I.T. Sloan School, and Harvard Business School, respectively.

Dr. Gert J. van der Pijl is an emeritus professor of IT auditing & advisory and former Program Director of IT auditing & advisory at the Erasmus School of Accounting and Assurance, the Erasmus University Rotterdam, the Netherlands. His research focuses on business IT alignment and IT risk management. He has been in the program committee of several IT auditing-oriented conferences and has published his work in several peer-reviewed journals. He also acts as a Chief Editor of the professional journal of Dutch IT-auditors. He got his BSc and PhD from Tilburg University and MSc from Erasmus University.

Dr. Harry R. Commandeur is currently a full professor of industrial economics and business economics and holds the F.D.J Goldschmeding Chair of Economics and Humanities at the Erasmus School of Economics, Erasmus University Rotterdam, the Netherlands. His research focuses on the relationship between market structure, corporate strategy, and firm performance. He holds MSc and PhD degrees from Erasmus University Rotterdam.