Risk Management Unveiling and Taming Danger: Exploratory Search Embedded in Legitimating Routines

By
Laurel Edwards Grassin-Drake

B.A., Art History
Swarthmore College, 1981

M.B.A.
University of Pennsylvania, 1983

M.A., Religion
Columbia University, 1992

SUBMITTED TO THE MIT SLOAN SCHOOL OF MANAGEMENT IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE IN MANAGEMENT RESEARCH
AT THE
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

FEBRUARY 2016

Signature of Author: Signature redacted
MIT Sloan School of Management
January 14, 2016

Certified by: Signature redacted
Ezra Zuckerman Sivan
Alvin J. Siteman (1948) Professor of Entrepreneurship and Strategy
Deputy Dean
Thesis Supervisor

Accepted by: Signature redacted
Catherine Tucker
Sloan Distinguished Professor of Management
Professor of Marketing
Chair MIT Sloan PhD Program

Risk Management Unveiling and Taming Danger: Exploratory Search Embedded in Legitimating Routines

by

Laurel Edwards Grassin-Drake

Submitted to the MIT Sloan School of Management
On January 14, 2016 in Partial Fulfillment of the Requirements for the
Degree of Master of Science in Management Research

ABSTRACT

This paper explores how contemporary organizations manage inherent tensions between productivity and legitimacy in the context of the "risk society." Interviews with executives in large organizations across a range of industries reveal that many risk managers echo this tension within their own work as they juxtapose two seemingly contradictory modes of search and action across five dimensions of risk management (identification, assessment, action, reassessment, and monitoring/reporting). On the one hand, they employ the routine procedures, measurement, tracking and reporting of audit processes designed to uphold legitimacy. On the other hand, though, they also use a radically different approach for risk identification, which they view as the substance of their work. Aware of risk's indeterminate nature, they adopt unscripted processes of exploration that question and undermine the taken-for-granted nature of measurement and routine, employing a collection of techniques I label "creative challenge."

Thesis supervisor: Ezra Zuckerman Sivan
Title: *Alvin J. Siteman (1948) Professor of Entrepreneurship and Strategy*
Deputy Dean

Introduction

> *"The conscious effort of managing risk where 'risk' is in the title of the meeting is a recent phenomenon in my experience...It was really in the latter years, maybe the last 10 years that we started to introduce the subject in a much more conscious way."*

(ex-CEO pharmaceutical company, past and present member of corporate and non-profit boards)

Risk management as an organizational practice has evolved rapidly over the past 20 years. Originally a term used to describe the work of a mid-level department that purchased insurance, managed security, or dealt with health and safety, risk management is becoming a senior executive function, which addresses a wide-range of risks across the organization, often reporting to the Board of Directors. Responding to diverse competitive and legal pressures, organizations have been increasingly forced to address risk in a formalized way. Demands for recursive awareness of risk emanating from our "risk society" (Beck 1992) are enacted and backed up by regulatory and quasi-regulatory rules to ensure the self-governance of risk with a clear expectation that organizations, from corporations to universities to charities, can and *should* manage risk.

The organizational literature on risk management, though, has not entirely kept up with these changes. Much of it specifically addresses 'safety and crisis management.' For obvious reasons scholars have focused primarily on the safe, 'reliable,' operation of technological systems whose failure can produce catastrophic results, but operational risk is only one type of risk needing to be addressed by today's organizations. Moreover, among the various recipes for managing risky technologies, prescriptions for mindfulness, based on a small universe of atypical high-hazard organizations, proliferate. A mindful organization rejects automatic information processing and orderly routines in order to maintain a continuous state of vigilance and adaptability. More precisely, it undermine routines and organizational structure by questioning, avoiding simplification, maintaining duplication, encouraging flexibility, and accepting reversals of hierarchical structure when necessary (Weick et al. 1999). There is general agreement, though, that achieving this model state of risk preparedness is costly since it comes at the expense both of efficiency, which relies on narrow attention and automatic information processing, and of

legitimacy, which relies on routines and structures which appear orderly to the external world (Weick et al 1999, Levinthal and Rerup 2006, Ray et al. 2011). Thus, much research on risk management has questionable utility for the vast majority of organizations, which struggle with an assemblage of conflicting objectives, limited resources and a variety of seemingly more mundane, but nonetheless non-trivial risks (Leveson et al. 2009).

More recently, though, another strand of work has looked beyond this restricted set of risks and organizations for models of risk management. This body of research describes how organizational risk management -- intermingled with audit and compliance processes -- is occupying an increasingly critical role in sustaining the legitimacy of organizational governance structures (Power 1999, Doyle and Ericson 2003, Heimer et al. 2005, Hutter and Power 2005, Power 2007). The claim of legitimacy must be visible and legible to those capable of bestowing it on the organization (Weber 1978): it requires a regularized language that allows stakeholders to perceive and interpret legitimating actions. Thus this form of risk management is secured by routinized, methodical processes of audit using supposedly transparent indicators and measures of organizational action which create trails of how things are done and provide acceptable evidence of conformity to the norms of legitimacy (Strathern 2000). These are the very types of actions that are theorized to promote organizational "mindlessness" and rigidity. From the audit perspective, then, risk management is viewed as a "ceremonial performance" (Meyer and Rowan 1977) to demonstrate responsible action to external audiences, and its fundamental value is suspect.

Hence, both lines of research agree that practices designed to promote the efficacy of risk management through mindfulness are at odds with practices that promote legitimacy and accountability through audit. Thus, the existing accounts of organizational risk management – mindful attentiveness to risk vs. systematic tracking of organizational processes – suggest fundamental incompatibility. Put another way, the pursuit of "unintegrated complexity," essential to achieve a mindful organization "runs the risk of appearing disorderly, messy, and unsafe, which could jeopardize legitimacy" (Weick et al. 1999:54). Organizations, thus, seem to be between a rock and a hard place when it comes to risk management. But is this really the case? Empirically, how are organizations actually approaching risk management? Are the

predictions of incompatibility correct? Are they indeed limited to an either/or of 'genuine' risk management which reduces risk vs. the ceremonial show of risk management which answers external expectations of risk management?

With this question in mind, this study set out to explore the implementation of whole-organization risk management in a variety of industries beyond the limited world of complex technological systems by focusing on the practice of Enterprise Risk Management (ERM). Through an inductive analysis of interviews with senior risk managers, as well as executives and board members, in banking, manufacturing, pharmaceuticals, high tech, retailing, and education, I find that for many executives and board members, risk management does and should contain two seemingly contradictory modes of thought and action. The routine procedures, measurement, and tracking of organizational decisions through audit processes designed to sustain legitimacy work alongside unscripted processes of exploration which question and undermine the taken-for-granted nature of measurement and routine. Aware of risk's ambiguity, risk managers work to make the invisible visible by providing alternative perspectives and using relational skills to challenge routines and established ways of thinking). These exploratory techniques, which I call "creative challenge," are combined with audit routines not only within the same organization, but even within the same functional unit and/or person. Rather than being contingent on the industry, the organization or the individual, this research shows how these modes of action and interpretation are correlated with specific dimensions of the risk management process. Having identified five (at times overlapping) components of risk management -- identification, assessment, action, re-assessment, and monitoring/reporting – I find that when risk managers speak about using audit routines, these are strongly associated with assessment, reassessment, and monitoring/reporting, while risk identification is widely characterized by the perspective and techniques of creative challenge.

Following a review of the literature on risk and organizational risk management and a description of the data and research methods, I will focus on creative challenge as an exploratory mode for risk identification. I will then trace the five components of the risk management process, showing how the elements connect and overlap. In walking through this process, I demonstrate how the risk management role and techniques shift with respect to a risk object from

identification to monitoring. This happens as responsibility for action moves outward into the larger organization: the communication and transition having been facilitated by re-imaging the risk object through the common language of categories and probabilities in assessment. In parallel, the mode of risk management similarly transitions from exploratory 'creative challenge' to audit routines, with many risk managers continually oscillating between the two seemingly discordant modes in their responses. Having laid out the process, roles, and modes, I hypothesize that not only does risk management live out the organizational tension between productivity and legitimacy, but that it may also serve as a an organizational buffer against future threat (Thompson 2003), allowing the organization to engage with radical uncertainty, while still moving forward productively.

Risk in Theory and Management Theories of Risk and Risk Management

Risk

The concept of risk is located at the center of modern notions of rationality, science, commensuration, and control, emerging in the 17th century with the measurement of uncertainty through statistics (Hacking 2006). Initially, probability served to remove future events from supernatural control into a natural world of calculable chance (Bernstein 1998). However, the characterization of risk as categories and numbers quickly becomes the basis for making predictions and taking action (Porter 1996). Once uncertainty is processed into risk, the future is no longer unknown, but rather takes shape, becoming comprehensible, thereby encouraging if not demanding that we act to ensure a positive outcome (Adams 1995). Though risk management was futile for the ancients who saw destiny as set by the Gods; in a humanistic world of calculated chance, we have become responsible for our own fate (Turner 1969). Thus, as moral actors, it becomes incumbent on us to manage risk: we *should* act to prevent potential negative consequences.

Historians report that modern risk management also arose in the 17th century alongside risk pooling through marine underwriting at Lloyd's Coffee House in London (Hodgson 1984). The twentieth century knowledge base of risk and risk management, however, has rapidly moved out

of the traditional spaces of statistics and insurance into a wide range of disciplines and professions, each focusing on its own conceptualization and categorization of risk (e.g. insurance, engineering, finance, accounting, legal). Each type of risk is viewed as having a unique set of characteristics and associated modes of control and/or mitigation. As a result, rather than being a primary profession, risk management (including risk assessment), has remained a field of subsidiary expertise dependent on and emergent from a variety of disciplines and consequently often buried within the functions and business units of the organization.

In this melee even the very definition of risk itself is up for grabs, as two competing theories try to shape the discourse around risk. In each, risk is the probability of some future event or outcome. The first risk conception represents risk as the probability of hazard or danger. This is the dominant understanding of risk, appearing as the primary entry in the OED: "(Exposure to) the possibility of loss, injury, or other adverse or unwelcome circumstance." It is this construction of risk that has focused risk management on control, prevention and mitigation, leading to the proliferation of departments such as classical risk management (concentrating on insurance or self-insurance), compliance, health and safety, as well as audit. Risk is to be avoided and the risk officer's job is to say 'no'. It has also provided the foundation for most academic work on risk and risk management. The second major perspective comes out of economics, which defines risk as the probability of *any* future event (Knight 1921), whether threat or opportunity, often shifting the focus from the normative valence of outcomes to the volatility of potential outcomes, especially in finance (Markowitz 1959). Rather than danger, risk is closely associated with opportunity and offers potential rewards. Heavily connected to ideas about shareholder value and economic growth, the risk-taking entrepreneurial spirit has become a management ideal (March and Shapira 1994) to be embraced (Baker and Simon 2002). Thus in one narrative risk has a negative valence, while in the other it is a positive value. Both conceptions of risk are voiced and managed within contemporary organizations that struggle to balance legitimacy and productivity/efficacy.

Risk Management

Within organizational and sociological scholarship on risk management there is, however, another divide, between those who promote the efficacy of particular practices of risk

management, and those who suggest that risk management is largely a ceremonial act of organizational legitimation. On the one hand, case studies of low or zero accident organizations have led to claims that successful risk management is possible when an organization establishes an overarching "safety culture" (Reason 1997): placing safety as a first priority, developing an alert awareness of the environment and anomalies within it, and focusing on potential failure. On the other hand, though, sociological analysis of risk management has gone beyond safety management, linking risk management to broader social and institutional changes, and concluding that risk management is an exercise in legitimacy, rather than an efficacious practice.

Organizational work in 'risk management' has tended to focus narrowly on safety management (physical, material failures being only one type of organizational risk), reflecting concerns about the potential for catastrophic failure caused by the interaction of engineering systems and organizational dynamics in high-hazard industries. Though some early work argued that accidents are inevitable, therefore normal, in complex and tightly-coupled systems (Perrow 1984, Sagan 1993), others have challenged this, pointing to high-risk organizations that have avoided or minimized accidents. The prescriptive answer is a good "safety culture." Though its definition and mechanisms are debated, it generally encompasses a holistic 'safety first' organizational mindset, undergird by collective practices designed to notice and act on the unexpected, and to actively learn from failure (Guldenmund 2000; Zhang et al 2002). One subset of this work has focused on high-risk organizations such as nuclear power plants, air traffic control and naval aircraft carriers and submarines (dubbed "high reliability organizations" or HROs), emphasizing the learning culture (rather than safety culture per se) of such organizations. Mindfulness, a constant state of active organizational self-awareness, is recommended as the source of safe, reliable management in high-hazard organizations (Roberts 1990, Schulman 1993, Weick and Roberts 1993, Weick et al. 1999, Weick and Sutcliffe 2001). The mindful state is more specifically supported by a collection of organizational practices which include: reluctance to simplify interpretations; sensitivity to operations; commitment to resilience; and underspecification of structures" (Weick et al. 1999). Thus a mindful organization rejects automatic information processing and orderly routines in favor of non-automatic information processing in its quest to maintain a constant state of vigilance and adaptability.

The HRO universe, though, is limited and unique, and it is not obvious that lessons learned from HRO theory can be effectively applied to the general universe of organizations. Many HROs are public entities, with singular missions where safety is essential to the mission; some could even be argued to be total institutions (e.g. air traffic control or a navy air craft carrier). HRO theory treats mindfulness as a holistic state which must be operative across the relevant organization; it doesn't work piecemeal. It cannot be partially implemented, neither by process nor by a portion of the organization. While it may be possible to establish mindfulness throughout a focused disciplined, authoritarian organization, where large resources are devoted to risk management and to institutionalizing a deeply-ingrained and unified culture, trying to implement such a culture across an extensive, diverse organization dependent upon creativity and discretion at all levels of the organization, such as today's complex design, research, educational and service corporations is problematic. There is even some question as to whether the concept of organizational mindfulness works at all given its basis in an instrumental (rather than emergent) understanding of culture (Silbey 2009, Sagan 1993). Assuming it is achievable, though, mindfulness would be costly on multiple levels. Attention is a scarce resource which bureaucracy husbands by using routines to facilitate information processing (March and Simon 1958/1993, Cyert and March 1963) and distributes through differentiated roles and activities in the organization (Ocasio 1997). In addition, legitimacy claims require visibly regularized actions and structures which can be 'read' by important external stakeholders as demonstrations of appropriate conduct. Mindfulness, then, comes at the expense of efficiency and legitimacy (Weick et al. 1999, Levinthal and Rerup 2006, Ray et al. 2011). Thus, by using this very particular set of high reliability organizations as data, the conclusions have questionable utility for the much larger universe of organizations that struggle with conflicting objectives, limited resources and seemingly more mundane, but nonetheless non-trivial risks (Leveson et al. 2009).

In fact, outside the narrow confines of HROs, organizational scholars remain skeptical about the role and efficacy of risk management in light of significant evidence that risk management is more about 'showing' rather than 'doing.' This second line of analysis emphasizes the subjective and socially constructed nature of risk (Ewald 1991, Garland 2003). Drawing from an infinite universe of potentialities rather than objective realities, we pick and choose what to focus on as risk or danger, and the list of acknowledged dangers and their respective valences vary by

culture (Douglas and Wildavsky 1982, Wildavsky and Drake 1990, Douglas 1994,) as well as by individual (Kahneman et al. 1982, Slovic 1987). In this context, our modern age finds us surrounded by external, manufactured risks (Giddens 1990), and we have become a "risk society" as "a systematic way of dealing with hazards and insecurities induced and introduced by modernisation itself" (Beck 1992:21). Moreover, social trust in institutions has deteriorated as society becomes increasingly vulnerable to the failure of "socially consequential actors… to carry out their duties with the full degree of competence and responsibility that fellow citizens need to expect." (Freudenberg 1993:927) Thus, chance is no longer an acceptable excuse. Ironically, while chance as part of the humanist project should have severed the putative causality between sinfulness and suffering, risk has re-instituted the connection. Today's sin is poor management, and bad outcomes make visible organizational sin for the community to blame and punish via our present-day after disaster fact-finding, commission reports and lawsuits. This move is amplified by the shift away from hard regulation (governmentally imposed rules and procedures and/or outcomes) to soft governance (voluntarily adopted standards and metrics of organizational performance promoted by non-governmental institutions and organizations), with a resultant "responsibilization" of the market (Shamir 2008), ascribing moral imperatives to organizations. Overcome by the purposively and inadvertently manufactured risks of the modern age, society makes increasing demands for the reflexive performance of risk by government and private organizations (Giddens 1999), leading to an explosion of 'risk management' in organizations in an attempt to rebuild trust and a sense of control.

This "quite extraordinary" demand for "failure free" organizations, though, seems unachievable in practicality (LaPorte and Consolini 1991) given the impossibility of anticipating all possible chains of failure in our complex, often tightly-coupled systems (Perrow 1984, Beck 1992, Taleb 2010); the understanding that even in loosely-coupled bureaucracies, mistakes are routine (Vaughan 1999); the knowledge that seemingly predictable risks can be hard to manage due to "risk reactivity" (Heimer 1985); and the fact that these demands are often at odds with the primary goals of organizations (Leveson et al. 2009) and impossible to meet with scarce resources (Rudolph and Repenning 2002, Lyneis 2012). Moreover, for anything other than statistics on the most routine and common perils, there is no way to reasonably measure whether

risk management is effective. Successful risk management is a non-event, or a reduced cost versus *what would have been* had there been no risk management in place. So there is an expectation that organizations should 'do something' about risk, but the demands are limitless and efforts indeterminate. Since operative, productive action is unfeasible, the most common approach is to produce a ceremonial performance (Meyer & Rowan 1977), based around rules and processes recognized as legitimate proof (DiMaggio & Powell 1983) of right action: i.e. audit.

Audit procedures have become the organizational response to demands made by external audiences for organizational self-governance, responsibility and transparency. Extending beyond its original financial remit, the audit function's focus on bureaucratic control processes and measurement has become the 'seal of approval' providing a rational representation of accountability and trustworthiness in multiple modes of organizational practice (Strathern 2000). Internally, audit procedures serve to implement the broad ideals embodied in regulatory regimes (whether statutory or voluntary), managing the 'gap' between regulation and practice (Huising and Silbey 2011) through the certification of processes and procedures and establishing a top-down mode of self-reflexive control through internal surveillance (Foucault 1995). Externally, audit certifications of 'best practice' allow organizations to demonstrate compliance with expectations through bureaucratic procedures rather than outcomes (Dobbin 2011, Shapiro 1987), while standardized measurements reduce varied and complex phenomena to a few reified numbers, providing the illusion of scientific rational expertise and control (Hacking 1990, Espeland and Vannebo 2007). These "rituals of verification" (Power 2007) help constitute the organization as a unitary moral actor in society (Gray and Silbey forthcoming), while at the same time creating trails of responsibility which allow the transfer of blame from the organization to individuals when something does go wrong (Russell 1996, Hood 2002, Shamir 2008, Jackall 2009).

The relationship of audit to risk management, though, is fundamental. The audit function doesn't just check on risk management; it is itself a form of risk management. Originally designed to protect owners from the financial malfeasance of agent managers by certifying that the financial statements "present fairly...the financial position of the company" (AICPA

1989:2151), internal audit has become a broad control function enacting "stewardship," by overseeing procedures which establish management actions as rational, sober and responsible, rather than foolhardy and risky.

As such, audit practices are the antithesis of mindfulness. Just as the questioning and unintegrated complexity of an HRO undermines the order and routine of audit, so do the processes of audit seem to trap reflection, analysis and critique within boxes of automatic thought. Good practices of risk management may be crowded-out in a legalized over-audited organization (Hutter and Power 2005), and evidence exists that such "technologies of control develop ritualistic properties with symbolic meanings" can actually increase risk (Vaughan 2005). Nonetheless, from the transformation of non-calculable uncertainties into calculable "risk objects" (Hilgartner 1992) to the creation of "fantasy" planning documents exhibiting management's readiness and control in the face of potential disaster (Clarke 2001), audit frameworks provide the tools to legitimize the organization's risk management efforts. Such rational visibility may be missing in mindful organizations which can paradoxically "appear disorderly, messy, and unsafe" (Weick et al. 1999). In sum then, risk management is becoming intertwined with audit, occupying an increasingly critical role in sustaining legitimacy as part of the structure of organizational governance, despite the fact that both lines of research agree that such audit practices are at odds with effective risk management. In other words, current theory on risk management contends that organizational risk management can aim to accomplish productivity or legitimacy, but it can't have both.

Enterprise Risk Management and this Study

To address this conundrum, I focus on the management practice of Enterprise Risk Management (ERM) both because it is widespread (especially in large organizations) and because it clearly embodies the intersection of audit and risk management. ERM is a 'new' vision of risk management which began to appear in the 1990's. Responding to corporate failures, litigation, calls for increased accountability (Power 2007) and new government regulation, ERM has gained significant traction in the past decade, post Sarbanes-Oxley (Bradford and Fox 2013, Beasley et al. 2014) As opposed to the traditional disciplinary risk management function found further down the organizational hierarchy, ERM is meant to provide a top-down, holistic view of

the organization. ERM documents (Lam 1994, COSO 2004, ISO 2009, University Business Executive Roundtable 2012) emphasize that this is ***whole*** enterprise risk management: integrated, aggregated, and cross-silo. Heads of ERM are usually found not more than 1-2 levels down from the CEO, and some have been given the title of "Chief Risk Officer," while risk reports produced by ERM are ultimately designed for Board review and approval. Charged with the oversight of all aspects of risk in the organization, from strategic and reputational to financial and technological, these executives come from a variety of backgrounds, including compliance/legal, systems and IT, insurance/actuarial, econometric modelling, etc. (interviews). But outside of banking (where regulations prevent the mixing of audit and risk functions), the large majority of ERM executives are auditors (Bradford and Fox 2013). ERM is presented as a pure expression of the audit model of risk management largely based on non-empirical work (Power 2007). Despite the fact that ERM has become ubiquitous, and is *the* dominant form of risk management in many large organizations, we know little about how it is actually practiced inside these entities.

Through interviews with senior and executive managers, and board members of organizations representing a variety of industries, supplemented by observations at meetings, this study provides an inside glimpse with surprising results. In fact, while all organizations used audit techniques for at least part of the risk management process, many informants also describe concurrent practices which are at odds with the logic of audit, suffused by exploratory search, self-reflection, critique and challenge. Moreover, analyzing the data across the 54 organizations represented by the 48 senior managers observed or interviewed, I model risk management as a five-phase process composed of risk identification, risk assessment, action to manage risk, risk re-assessment, and monitoring/reporting; and I find that these practices of exploration are primarily associated with a specific element of the risk management process – risk identification. Aware of risk's ambiguity, risk managers face the unknown, working to make the invisible visible by remaining open to alternative perspectives and using relational skills to challenge routines and established ways of thinking: a collection of exploratory techniques which I call "creative challenge."

Data and Methods

For this research, I conducted 36 interviews with 34 senior executives over 6 months (one Director of ERM was interviewed multiple times), and observed a two-day peer-network meeting of Enterprise Risk Managers, attended by 14 senior risk managers. Interviews were semi-structured, consisting of open-ended questions about risk and risk management. Interviews ranged from 30 minutes to 1 hour and 45 minutes, with the majority lasting about an hour. Most were face to face although 3 were conducted over the phone. In addition, archival material from professional organizations and the Enterprise Risk Management Initiative at North Carolina State University (including video interviews of ERM managers) was also consulted.

ERM generally resides towards the top of the organizational hierarchy and often reports to the Board of Directors. Outside of banking, these programs tend to be concentrated in the largest corporations. Thus empirical research on these risk managers required access to Board members, CEOs and other C-Suite executives, as well as the risk managers themselves (who might also be part of the C-Suite) in Fortune 250 companies. Because such access is very difficult to obtain, the study created a sample based on personal and professional connections, some snow-balling, and cold-call email requests, some few which received positive responses. Given the nature of the findings, though, the convenience sample should not propose problems for reliability or validity. This research documents the unexpected presence in risk management of a confluence of exploratory search and audit routines, rather than trying to prove how 'typical' these practices are. In other words, this research is not attempting to establish statistical generalizability. As Small (2009) notes (citing Glaser and Strauss 1967, and Lofland and Lofland 1995), "a well-executed single-case study can justifiably state that a particular process, phenomenon, mechanism, tendency, type, relationship, dynamic, or practice exists." Thus, this study goes further than Small anticipates by using multiple case studies to substantiate that this phenomenon exists in more than one company and across more than one industry.

The 34 interviewees were selected to provide variation in roles within organizations and across business sectors. Twenty-two interviewees came from two firms (a bank and a manufacturing

company). These in-depth inquiries in two firms constituted the core of the study, while the additional twelve interviews distributed across six sectors. (See Table 1) Additionally, many interview respondents had held past positions at other firms, and so were able to speak to experience in more than one organization and at more than one level (for instance, one CEO is also a current Board Member elsewhere and had past experience as CFO and risk manager at yet another firm). Thus these senior managers represented 38 companies (including 22 Fortune 250 at the time the respondent worked for the firm) in financial services, manufacturing, pharmaceuticals and high tech, as well as one major research institution. Adding observations from the peer network meeting and video interviews brought the total number of represented companies to 54 (30 of which were Fortune 250). (See Table 2) While risk managers dominated the group (18 interviewed and 14 observed at the conference), I also undertook to capture the views of Board members, CEOs, CFOs, and others who set risk policies or who interacted with the risk management function. Hierarchically, respondents were at most 3 reporting levels down from the CEO. 3 ERM 'experts' were also interviewed at professional and educational organizations who promulgate ERM and offer coursework.

Interviews consisted of questions about the meaning and values of risk and risk management (e.g. How do you personally define risk? What does it mean to 'manage' risk? What are the benefits of risk management? How would you describe the ideal senior risk manager?), as well as questions about risk management processes and relationships within the specific organization (e.g. Would you describe for me the structure and responsibilities of risk management at your organization? What types of resistance has there been to creating the ERM function? Can you think of a specific example where someone didn't want to co-operate?). In addition, I tried to tease out opinions about the interaction of audit and risk management, and any disciplinary bias/tension between these traditional roles. Many questions were also tailored to the role, organization, and professional history of the individual respondent; for instance, I might ask a respondent who had substantive experience in two organizations to compare the two. Overall, interviews were organized to go where the respondent led, with follow-up questions building on what had already been said.

Findings were derived through inductive analysis using grounded theory (Glazer and Strauss 1967, Charmaz 2006). Interviews were recorded and transcripts coded initially by hand, and then using Atlas.ti. Recording was not permitted at the peer-group meeting, so for this I relied on detailed field notes, written during the meetings and elaborate immediately afterward. Initial deductive codes were drawn from the risk management literature and concepts of audit. These included items such as: categories of risk, quantification, modes of control, routine processes, board reporting. But at the same time, I developed codes from the respondents' own language. As the concepts which eventually came together as creative challenge emerged, I began to build inductive codes. As Gray and Silbey (2014) note, "the virtue of...using the model of grounded theory is the opportunity for surprises the researcher did not anticipate." With "creative" and "out-of-the-box" thinking as an early descriptor of the ideal risk manager, and accounts of risk's ambiguity appearing in the transcripts, I turned to the literature on organizational sensemaking (Weick 1999, Weick et al. 2005, Sandberg and Tsoukas 2014) to ensure that I was paying attention to respondents' unscripted attempts to "make the world orderly" in the face of a chaotic future through "creation, interpretation and enactment." Similarly, an emphasis on relational skills, which was surprising in a control function, became an unexpected new coding category. Eventually it became clear that the use of relational skills was not only about control, but was intimately connected to the critical inquiry and questioning that respondents believed necessary for effective risk identification (see below).

As interviews progressed, analysis through studying the transcripts and memo-writing proceeded simultaneously. Eventually, axial coding (Strauss and Corbin 1998) was performed using Ewick and Silbey's (1998, 2003, 2014) four dimensions of social action (normativity, capacity, constraint and time/space). However, this study contained two focal objects -- risk management (a form of social action) and ideas about risk (meaning which interacts with risk management) -- so two additional axial codes were introduced covering the perceived nature of risk and sources of risk objects. In studying these results, patterns surfaced across the dimensions which coalesced into two core categories representing two modes of risk management action: creative challenge and measured routines. Taking these findings and returning to transcripts and memos revealed that ideas around creative challenge were associated with risk identification and the use

of relational skills, while routines were most commonly associated with other stages of the risk management process.

Findings

In interviews of auditors, controllers, and IT managers turned senior risk manager, as well as bank risk officers acting as the go-between with the Federal Reserve regulators, audit routines were not hard to find. Complex and uncertain risks were sorted into categories and reified into one or two standardized measurements of potential hazard and probability. "Ownership" was assigned; providing clear lines of responsibility and blame. Owners were held accountable for developing appropriate plans of action, and actions were "measured" against plans. Monitoring and reporting provided documented trails of the overall process, and the final formal reporting to the board represented in brief schematics (e.g. lists of top X risks, "heat maps," and XXX) the broad universe of complex risk faced by the organization, providing proof that management had paid attention to risk and was doing something about it.

However, alongside processes of audit something else emerged. Rooted in the understanding that risk represents uncertain ambiguity, many managers spoke of using a creative, exploratory mode of inquiry. Further, this inquiry was associated with a collection of practices designed to uncover organizational risk through punctuated questioning and challenge of taken-for-granted ways of seeing and doing. This combination of inquiry and practice, I term creative challenge.

Creative Challenge

Out-of-the-Box Thinking

Q: What would your ideal senior risk manager or officer look like?

A: "*A good risk manager is someone who can look at things in many different ways and someone who never settles on one thing, as* ***the*** *way to look at something.*" (CRO, bank)

"Having a risk professional at the table helps: someone who thinks a bit differently. I can say that because my past colleagues said that to me: that I looked at things differently." (ERM Expert for Professional Organization and past head of ERM for consulting firm.)

"*The brain kind of works crosswise.*" (Chief Model Risk Officer, bank)

"almost a free-form type thinker....kind of out-of-the-box." (CRO, bank)

ERM is the prototypical example of risk management enmeshed in standardized audit routines of measurement, control and tracking, and used to demonstrate good organizational governance to external audiences. In this context, the image of risk officer as a creative and unconventional thinker was completely unexpected. It certainly doesn't look like the role description for either the typical auditor or compliance officer: occupations which thrive on convention, rules and procedures. Yet senior risk manager as out-of-the-box thinker emerged as a common trope in these interviews.

According to many senior managers and executives, effective risk management requires a unique point of view: one which itself is open-ended, and holistic. Perhaps more appropriately, this vision might be characterized as one of multiple perspectives. To avoid reifying a single view of the world, respondents spoke of looking at a question, problem, situation, context, etc. from a variety of angles. For many, it was not professional risk expertise which separated risk management from the rest of management, rather it was this ability to think "crosswise." In fact risk expertise, including quantitative skills, was dismissed by many. In addition, for those embracing this ideal, if risk management has any value, it derives from this creative capability, *"'When you have an impact on me it's gonna be when you can help me think about a different way to view my business or my world.'"* (Senior business unit executive speaking to the CRO, as recounted by the CRO, manufacturer) Whether this is an in-born trait (as many hinted), or the result of diverse experience (which was visible in the backgrounds of several senior risk officers), or the effect of specializing in the alternative futures of risk is unclear, but as the quotes above suggest it seems that some executives actively look for this in a risk officer.

Risk as ambiguity

At first glance, one might conclude that the use of 'out-of-the-box' thinking is a management cliché, representing a professional play for status (Abbott 1988) as part of the "creative class" (Florida 2014); however, the associated discussion of risk from these respondents suggests something more fundamental. The very same respondents who described the ideal risk manager as unconventional and creative, spoke of risk as amorphous and emergent elsewhere in their accounts: *"I suppose it all depends on how you define risk management....I mean a nebulous term or at least an open-ended one."* (Treasurer, Manufacturer) These managers didn't reify risk; rather they recognized that risk arises out of ambiguity. To them risk represents an invisible, uncertain future. So they struggle to grasp this object which initially has no clear shape: *"So there is this mix of people trying to solve a problem that is not written anywhere. What is the problem? Nobody knows what the problem is, but we're all trying to solve something."* (Operational Risk Manager, bank) Worse, this undefined problem has no fixed solution: "*Risk is very different from finance. In finance there's an answer for everything, there's a right answer. It's math, right? In risk there is no answer."* (CRO, Bank) A few respondents even recognized the socially-constructed nature of risk, particularly those at the highest level of the organizational hierarchy. The CEO of a pharmaceutical company spoke of risk as perception, noting that, *"There are people who have different views on these risks."* Further, for him, risk was about falling short of expectations: unstable expectations which change over time. Speaking of the evolution in risk awareness another CEO (of a bank) noted that, *"...that's why I say [risk is] a social sort of deal...these are all risks that society has decided they're worried about and they wanna do something about."* Thus risk is not absolute; it morphs as the society which defines it shifts. It is not surprising, then, that these respondents believed that exploratory inquiry (Dewey 2009) was the key to unlocking this "terra incognita" (Stark 2009:4). Just as "the product developer frequently starts out without really knowing what she is trying to create" (Lester and Piore 2004:41), so the risk manager starts out without really knowing what she is trying to find. In this context, out of the box thinking has a very practical component.

Making the Invisible, Visible

In problematizing risk, though, risk management itself is no longer straightforward. For these same respondents, risk management was not just about control and tracking -- it also represented

a process of discovery. Though vague and indefinite, risk was also objectified as something which exists independently where we can't see. *"Unknown"* or *"invisible,"* risk was described as something to be *"discovered,"* or pulled out of some fixed universe of 'risk,' such that one can speak of *"every risk"* or *"all risks."* Seeing themselves as uniquely capable of such exploratory work these managers focused heavily on risk identification in their accounts and clearly saw their primary contribution as unveiling these hidden risks to the organization, or making the invisible risk, visible.

In these accounts, invisibility is often more about our process of knowing and perception than it is about the risk object as such existing beyond our horizon. Respondents voiced this in multiple ways. Risk is indiscernible because we think it impossible. This is sometimes the result of a failure in imagination, as groups of people fail to envision a future which is noticeably different than the past, as in the financial crisis. At other times, though, risk is inconceivable despite evidence to the contrary. In other words, the organization *could* see the risk, but it has implicitly assigned a probability of 0 to the event. The CEO of a pharmaceutical firm, speaking about a virus which closed down a manufacturing plant reasoned this way, *"We had NEVER had a virus. It was not a part of our vocabulary. [Competitor A] had a virus; [competitor B] had a virus. We'd never had a virus. We had a different approach, and when it hit, of course, it hit us between the eyes at our most vulnerable."* (CEO, Pharmaceutical firm)

Managers also spoke of risk hiding in customary practices. Several respondents suggested that taken-for-granted routines blind people to risk, because in following patterns without thought, they stop questioning. A good risk manager looks behind the veil of habit, then, to probe and examine: *"Risk would be either not knowing, being unaware of, an actual practice that can cause adverse impacts to the firm....I'm always trying to dig to get to the answer because they always say, 'Oh, we do it this way.' And then, it's the way it's just been done."* (Risk manager, Bank) Another reason that risk is so readily concealed in routine processes is that it comes disguised. In particular, many pointed out how potentially catastrophic risks start small, suggesting that risks become real through complex paths which transform the trivial into disaster. Additionally, categories themselves become a source of risk, because the organization isn't structured to perceive and comprehend objects which don't fit the classifications. The dominant

categories are those that constitute the organization itself: the business and functional units, or "silos." ERM literature is replete with discussions of 'cross-silo risk,' and a key argumentation for implementing ERM is to integrate and aggregate risk to a level of the organization which transcends these divisions. In this, the study respondents were right on board. The large majority spoke about people within silos, being unable to see over the walls. More than one risk manager shared personal stories demonstrating the need for cross-category vision (and their personal ability to provide that vision).

Finally, and most tellingly, risk is invisible because managers refuse to look at it. Many narratives (including that of the pharmaceutical CEO above), suggested that executives are actually at some level afraid of significant risks. Metaphors of dying appear again and again. Interviews are sprinkled with phrases about risk that will *"sink," "kill," "destroy,"* or lead to the *"death"* of the company. This sense of fear was beautifully summed up by the senior risk manager at a manufacturer as he spoke about some of the advantages of the risk management function. Faced with the possibility of a Euro collapse, he organized a meeting with relevant senior executives to discuss more informally what might happen and what could be the potential effects:

> *"And the ability to convene a [meeting]: that would have been hard to get done without this kind of function.... There is a strong desire that this not be a big issue, okay? And so, until it becomes an issue, it's such a scary prospect, that there is this tendency to say, 'I haven't seen it yet, therefore, it's not a risk.' And so the ability to ask these questions without having to say, 'Yes, it's better than 50% chance that this is gonna happen' or, 'This is now our forecast,' that this will happen."*

Even in these rational, bureaucratic environments, risk is danger: a taboo which should not to be touched (Mary Douglas 1984, 1994). Like Voldemort's name in the Harry Potter series (Rowling 1999), speaking risk by attaching a probability or placing it in a formal report is seen as performative (Austin 1975), bringing the threat out of the shadows and actualizing it.

Effective Challenge

Creative challenge, then, is rooted in the belief that risk is invisible, amorphous and has no single answer; that the fundamental role of the risk manager is to make this invisible risk visible; and that the ideal risk manager is therefore someone who can operate effectively in ambiguity as an out-of-the box thinker. But in addition, creative challenge also emerged as a collection of practices for finding and unveiling risk. At the heart of the practice of creative challenge is asking questions, or "effective challenge."

Questions are the risk manager's tool both for uncovering risk as well as for revealing it to others in the organization (Miller and Lessard 2008). Questions facilitate exposing the 'unknown unknowns,' delineating their existence and shape. Questions also help expose malfeasance, where people have deliberately covered up risk for personal or political reasons, and some risk managers spoke of *"sleuthing"* or *"playing Columbo."* But questions are particularly valuable in addressing risk from "taken-for-granted" institutions.

Routines establish a single way of seeing the world, an automatic answer, whose underlying assumptions and shades of grey have vanished: they are blinders which support focus and afford consistent, efficient action. From a risk perspective, though, they can be screens obscuring risk. Questions help pierce this screen. It is the Head of ERM at a bank who labelled this process "effective challenge," using the Federal Reserve's terminology for model validation:

> *"My career, it's been an effective challenge function... As soon as you start getting comfortable with something, you start questioning it. What isn't it seeing? What's not in it? So it requires a breadth. It requires a way of thinking that is constantly challenging; it's never accepting an answer as being right...To me, that's getting at the core of how I see risk management."*

Much of this is about peeling back layers to get to the core assumptions. Hence while the perspective is broad, the thought process is narrow, disciplined and focused, or as one respondent put it, *"laser sharp,"* so as to cut through the clutter. The goal is to prompt people to step-back from routines and to reflect consciously about what they are taking for granted. The debate and resultant heightened awareness is meant to create a more disciplined decision process leading to

improved outcomes. This critical eye is not only turned outwards to the larger organization, but inwards as well, as even the very routines which have been designed by risk managers to control risk are suspect.

In a sense, the risk managers who use creative challenge are playing organizational devil's advocate (Mason 1969; Cosier 1978), and free-form questions emerging from out-of-the-box thinking facilitate this. Simple questions can be one of the most important tools in a risk manager's arsenal, *"I think there's value to having a mechanism that helps people think...that probes on, 'Have you thought about this or not thought about that?'"* (CFO, manufacturer) Intelligent questioning, though, requires expertise: not risk expertise, but a deep understanding of the business. Virtually no one listed expertise or a background in risk management as necessary for the ideal risk manager, but almost everyone stressed the need for the senior risk manager to be knowledgeable about the business, such that she can cut through unnecessary details and ask intelligent, insightful questions of senior and executive business and functional managers.

In addition, though, managers also turned to several formal practices for framing questions and challenging the organization. Scenario-planning, and the related stress-testing, forced business planners to make their assumptions explicit so that appropriate models can be built. Moreover, they revealed hidden connections across the organization. One risk manager at a bank, responsible for formal stress-testing said this, *"There has been a ton of rigor around this particular exercise...to get this line of sight on the granularity of how dynamic a company's results can be based on a couple of different factors and the ripple effects that occurred due to this."* Such stress-testing is mandated by the Federal Reserve, but several non-banks used scenario-planning to accomplish some of the same goals in a less resource-intensive fashion. At a manufacturer, managers were confronted with their own unrealistic assumptions through scenarios, *"When we developed our budget business plan this year, I mean we actually got some scenario plans, some upside/downside scenarios to incorporate into it. And the results were, we took some of our volume estimates down, our guys were too optimistic, and so we built what we think is a lot more realistic plan."* (CRO, manufacturer) This was an example of a decision which clearly the CRO (and executive managers) believed had been improved through effective challenge. Structured debates also served to test assumptions. One diversified corporation

arbitrarily assigns a group of managers to the *"red team or blue team"* to research and argue *"pro or con"* as they map futures to guide new technology, while a technology company encourages, *"constructive confrontation, creating active debate in all areas."* Finally, some organizations looked to external reviewers to question established ways of doing things and provide a fresh perspective. In some cases this was driven by certifications, for instance bank holding companies are subject to rotating expert teams from the Federal Reserve reviewing specific aspects of their operations and universities are periodically evaluated by a visiting committee of peers, but at other times organizations voluntarily seek outside input. As one Corporate Finance Controller, responsible for ERM at a technology company, said, *"We all get fascinated with drinking our own champagne. External people are not wedded to internal strategy."*

Relational Strategies

Whether in the form of free-form questions or accepted practices, though, effective challenge is always interactive and responsive – and it is discomfiting to the organization. Risk managers are pushing people to look hard at things they don't want to see. They make abstract possibilities real and visible, forcing the organization to confront danger. They cross inter-organizational boundaries, seeming to step on others' territories, sometime uncovering the *"uglies"* that others want to keep hidden. They are the devil's advocate which throws cold water on enthusiastic plans. Finally, they destabilize organizational institutions by questioning the taken-for-granted. Risk managers are keenly aware of this dynamic, and spoke at length about the relational skills needed to manage push-back from others in the organization and effectively do their work. Accordingly, these risk managers valued "people skills" over technical skills, and spoke of the need for communication and social skills to gain trust and credibility, to persuade and "sell" their ideas, and to encourage and facilitate divergent perspectives (Silbey et al. 2009).

Multiple risk managers spoke of the importance of trust, and the need to establish a connection with business managers, so as to open lines of communication. In fact, the auditor of a bank (not in the risk management department) said the most important question separating a good risk management function from a bad risk function was, *"How well does that group communicate with the line function, with the business function, and to what degree is there transparency between the two?"* Trust creates a two-way street that encourages business managers to talk --

"You have to be able to get their trust and get them to open up about what concerns them." (CRO manufacturer) – as well as taking the sting off the difficult questions risk managers ask.

Two key trust mechanisms reported by risk managers were spending time with business managers and positioning oneself has a helpmate. Aware that familiarity is the basis for a comfortable relationship of trust, some risk managers made a point of getting to know key business managers. For one risk manager at a bank, this even included social time after work, *"I mean half of our job is to get along with people...I actually do hang out with them. I actually do take them out."* Others would create trust and credibility by using the risk function to support business managers where possible, positioning themselves as a "partner" to management. Ironically, at times this included reassuring managers who fear responsibility and blame in the new risk management regime, *"'It's gonna take a little work, but we'll get it done.' Well, if you can feel the chip... everyone'll get a little bit more relaxed."* (Chief Compliance Officer, bank)

Though their formal role gave legitimacy to risk managers' questions, managers nonetheless stressed building credibility. Outside of banking, where the risk control function is mandated, ERM departments were not yet fully institutionalized. Feeling still vulnerable, more than one senior risk manager spoke of the need to create *"quick wins"* or *"small wins"* to ensure the function continued survival. Such wins also helped risk managers convince time-starved executives to actively engage with the risk management work. The key was persuading business unit heads that there's *"something in it for them,"* and that risk had practical implications rather than being *"too theoretical." "You have to kind of put some scenarios together where all of a sudden it becomes a bit more real to 'em and then they can say, 'Ah, you know something? Well, I guess, it's not an all or nothing thing. I could see where things start to happen and I have to figure out how am I gonna react to it,' not just, 'Well, a meteor is coming and we're all dead, so why bother to plan?'"* (CRO, manufacturer)

Mangers also looked for ways to downplay the challenge of risk management through asking cloaked questions, providing safe spaces and emphasizing the upside. Questions which challenge routine might be defused through seeming naiveté, and some respondents would argue that *"dumb questions"* are the best questions: *"I like to say I am a ninja clear thinker and a lot*

of my weapons in being a clear thinker are dumb questions, so one of my derailing questions [is]....'Stop. Sorry. Just one quick question: why are we doing this project?'" (Chief Info and Security Risk Officer, manufacturer) Moreover dumb questions helped lower defenses, leading to better information, *"It's like playing Colombo or something. You try to, say, 'I'm just not smart enough, I went to a state school, so I can't pick these things up as quickly as you can. So, can you repeat that one more time? How you get the data from here and transform it to ultimately put into this report?'"* (Risk manager, Bank) Creating safe spaces for exploring risk, as in the workshop on the Euro-zone break-up mentioned earlier, also eased the encounter with risk (Kellogg 2009). For some organizations, such exploratory workshops were an important tool for encouraging the organization to confront a major risk identified by the risk management department. Finally, risk managers spoke of persuading business managers to engage with risk management through focusing on the positives over the negatives. For instance, the CRO at a manufacturer argues that the question shouldn't just be *"What are we missing on?"* but *"Well, what are we doing good? And how can we do more of what we're doing good?"* This is the *"sugar"* that helps the *"medicine go along."* He believes this makes things a lot easier, *"'cause it really stinks to have to go work on stuff that you really don't like to do in the first place."*

Ultimately, relational strategies were used to some degree by all risk managers. Such strategies, though, were most visible in the accounts of risk managers using creative challenge, and appeared to be a an important component in creative challenge. Knowing that their risk discovery process represented a challenge and even a threat to the larger organization, risk managers looked to soften the blow and encourage open communication through these strategies.

Summary

At its heart, creative challenge is all about risk identification. While assessing, taking action and monitoring are rooted in the present, risk itself lives in an unknown future which is the stuff of inquiry rather than problem-solving (Dewey 2009). Creative challenge thus represents a complex approach to risk, at odds with an audit or control perspective.

At the same time, though, neither is creative challenge equivalent to mindfulness. There are some similarities between the organizational practices of mindfulness theorized as anticipatory

(i.e. preoccupation with failure, reluctance to simplify, and sensitivity to operations), but creative challenge is far from those of containment (i.e. commitment to resilience, and underspecification of structures) (Weick and Sutcliffe 2001); creative challenge is focused on the identification of risk rather than crisis management. In this sense creative challenge is less than mindfulness, but at the same time it is something more. Fundamentally, creative challenge is not limited to the risk of a technical/engineering system. Organizational mindfulness theory is derived from work on specific high-hazard systems, and the emphasis is on the recognition of anomalies, or deviations from the norm, which may signal an embryonic system failure. In other words, mindfulness looks for failure which is already in progress, and requires everyone's participation to keep an eye out. Creative challenge though, must consider a much wider and open-ended risk universe which can play out over years. In going beyond current anomalies, creative challenge does not require holistic continuous awareness of the present, but is instead intermittent. Moreover, the most distinctive aspect of creative challenge is that it stems from a strong sense of risk as ambiguous, amorphous, and hidden. It is notable that HRO theory does not even use the more subjective term 'risk,' instead choosing the more concrete engineering term 'failure.' In this creative challenge is closer to exploratory search, and like exploratory search in organizations, creative challenge is allocated to specialists. The most surprising aspect of creative challenge, though, for both risk management and exploration/innovation scholars, is that it is so closely intertwined with the routines of audit, as described below.

The Risk Management Process and Modes of Search and Practice

Creative challenge does not exist in a vacuum. Used for risk identification, creative challenge is embedded in routines and procedures of a larger risk management process, and it is this juxtaposition which is perhaps even more surprising given the predictions of current theory. It is therefore worth considering the process and more specifically how creative challenge interacts with audit routines and procedures.

The applied ERM literature is replete with frameworks and stages for risk management. Recommendations and instructions for good risk management revolve around a series of components meant to encompass the proper activities for the risk management function. The respondents in this study also voiced this understanding of risk management. Though one CRO

at a bank spoke of establishing the risk "framework," the dominant model was processual, rather than structural. While the basic outline of the process is the same across respondents and professional advocates, there is variation as to where lines should be drawn to distinguish one segment from another, and the number of phases might be as few as three and as many as six, with some activities overlapping others.

Based on interviews in this study, I model risk management as a five-part process, consisting of: (1) risk identification; (2) risk assessment; (3) action to mitigate, control, or avoid risk; (4) re-assessment of the net risk after action taken; and (5) monitoring/reporting. As will be seen below, these elements represent differences in the interaction between the risk management function and the wider organization, in what is done to and with the risk object, and in the balance between modes of audit and exploratory creative challenge. After detailing each phase and presenting how the process flows across them, I will then discuss how creative challenge is embedded in this process.

Risk Identification: risk management in the lead

Before a risk can be assessed, controlled or monitored it must first be identified. Audit theories of risk management largely assume away this step, focusing instead on the latter processes, but how one actually goes about 'discovering' a potential hazard amongst infinite possible futures is not obvious, and in this study many risk managers placed risk identification at the heart of the risk manager role. Moreover, despite the fact that there was universal reliance on the routines and measurements of audit processes for the other stages, audit was largely missing from these accounts when it came to risk identification.

Given the nature of risk, what might an audit version of identification look like? Such techniques did turn up. In particular, a few companies performed risk identification through surveys and questionnaires. One healthcare company performs company-wide surveys asking employees at all levels what they perceive to be the major risks faced by the company. These responses are then collated and aggregated to present to executive management for review (NCSU video). Similarly, a risk manager at a smaller tech company reported conducting an annual full company survey *"to capture emerging risks bubbling up from the bottom."* Other

companies survey only managers above a specific hierarchical level in order to avoid a long list of minor local risks, assuming that only more senior managers would have a broader, corporate perspective. Such surveys can be open-ended, or might include a list of categories or already identified risks as prompts. At more than one company, follow-up annual surveys are sent out to employees with the prior year's list of risks attached, making it easy for the process to turn into one of thoughtless 'ticking boxes' after the initial go-round. These are annual, generally at budget time, further emphasizing the link with audit routines and encouraging a rote performance. Finally, computerization can facilitate the company-wide practice by providing an automated link between survey results and the overall risk management framework.

However, the large majority of managers recognized the complex nature of risk identification, and rejected the automated procedures of audit for carrying it out. Instead, risk identification was synonymous with the exploratory inquiry of creative challenge. For those respondents, quality risk management required being willing to look at the present through the lens of multiple future possibilities and probing through careful interactive questioning of the status quo in order to reveal, or identify risk, for the organization.

Risk Assessment: risk in transition

Following identification (and sometimes overlapping with it) named hazard is converted into bounded risk using categorization and commensuration. In 1921 the economist Frank Knight famously made a careful distinction between risk as random events whose probability distribution is measurable and known, and uncertainty as random events whose probability distribution is not measurable or known. Effectively the first steps of risk management are designed to move potential dangers up the Knightian ladder, transforming unknown uncertainties into risk which can then be managed and readily tracked. Risk assessment, therefore, is fundamental to risk management. Moreover, just as risk assessment transitions risk objects from uncertain threats to manageable risks, it also distributes them out from the risk management function into the larger organization for action. It does this by: assigning categories which will determine who will receive the risk object (i.e. be responsible for the risk); translating risk into a common language so as to facilitate communication and ease of transfer; providing the

information which allows for efficient management using existing routines from past analogous risks.

Once a risk object has been identified, it is immediately classified. In fact, respondents found it difficult to speak of risk without categories. Nearly every respondent at some point referenced risk categories, and for some this was the first characterization they gave when asked their personal definition of 'risk.' Grouping risks immediately makes risk more manageable. Through analogy, the risk object is made equivalent to risks which have already been processed or hazards which have already been experienced. In this way, established routines can be extended to control this risk object, rather than having to start from scratch. Generally these categories have to do with the perceived 'source of risk' (i.e. the type of potential hazard). Frequently the borders tend to be set in reference to the organizational structure, so that the source of risk also serves to define the risk 'owner', i.e. the manager/department who is responsible for managing the risk (e.g. finance vs. human resource vs. IT risk) and by implication, the disciplinary model which will be applied. It is worth noting that these categorizations fly in the face of ERM's claimed goal of viewing risk cross-silo (Protiviti 2006), since for the most part they serve to accentuate, rather than dissolve boundaries between divisions and functions. Nonetheless, these categories make risk malleable: giving shape to an amorphous uncertainty through a legitimated structure, marking the first step towards commensuration and the ability to aggregate and report at an organizational level, and helping to apportion accountability and potential blame.

Next is quantification. Across the board, all respondents calculated the probability of a negative event and its expected cost. For some, the measures remained a rough mapping of high, medium or low, while others adopted much more sophisticated methods, with the banks in particular relying on complex computer risk models. These assessments provided critical commensuration which ranked and sorted risks (Espeland and Sauder 2009, Espeland and Stevens 1998), determining which risks would get Board and executive attention (and therefore risk management's attention), and what would be ignored at this level of the organization. Several companies produced cut-offs, reporting only the 'top X risks' or 'risks above $X million' to the Board. Moreover, some went so far as to argue that risks which can't be quantified shouldn't be taken because, "*taking unquantifiable risks runs the risk that you die.*" (CEO, bank).

Even "quantitative sceptics" (Mikes 2011), acknowledged the criticality of quantification. The Head of ERM at a bank, who repeatedly voiced concerns about relying too heavily on quantification, nonetheless found himself at the vanguard of a group pushing for implementing quantitative methodologies, because, *"Only the model kind of approaches aggregate well."* More strikingly, at another financial services firm, the CRO on the one hand opined that Federal reserve requirements for operational risks were *"abstruse quantification approaches"* and noted that *"we do a very poor job at measuring [tail risks]...You know almost all risk modelers got that wrong;"* while at the same time asserting, *"So, I would argue that to really be able to say that we understand a risk, we have to be able to quantify it on some basis. That simply talking about it isn't enough, right? ...* ***If you believe that risk was not quantifiable on any basis... You're kind of a nihilist when it comes to risk management..."*** Note that for him, quantification is risk management: the opposite of just talking about it isn't action; it is quantification.

Though assessment is rooted in the audit culture of measurement and tracking, it begins in creative challenge. While the assessment process seems to advance uncertainty into a fixed and defined risk, in actual fact it remains uncertain; it is part of an unknown future. Categories, probabilities, potential losses and appetites are social facts depending on the individual's perspective, and subject to disagreements. They are not 'givens.' Classifying risk is approximate, especially if it falls between or across established category boundaries. For instance the Human Resources risk officer at a manufacturer was responsible for tracking *"culture,"* but pointed out that, *"you think about HR from a change management perspective and they don't really own that but they're guardians of that with the business partners,"* and numerous respondents noted the slippery all-encompassing nature of 'reputational risk.' Assessment modes are often chosen to align with external demands rather than internal efficacy, with the result that the mode of quantification might not 'fit' *"IT doesn't know about dollars. They know about their processes, their systems and if you ask them how much is it gonna cost?...It's almost impossible to think of that level. So that is the problem with dollars."* (Head of Operational Risk, bank). Even the most sophisticated models require *"expert judgment"* (Head of Model Validation, bank) to work, and such judgment is a political process of negotiation. Once agreed,

though, the assumptions which created the labels disappear and the category and numbers become a reified foundation for action (Espeland and Sauder 2007). A bank CRO, though a quantitative sceptic who acknowledged the imperfect process of arriving at measures, still spoke of the numbers in absolute terms, when describing action: *"So, within this category of operational risk and a certain category of operational risk is, I really don't think we should lose another $500,000 from this type of risk."* The result is 'transparency' in that the risk object can be seen and grasped internally by both those who are accountable and those who control, while being represented externally in legitimate terms to outside stakeholders.

Action: business managers as owners

While assessment is a shared responsibility between the risk management unit and the larger organization, by the time assessment is agreed, risk management shifts to a monitoring and reporting role, and the business manager/unit now 'owns' the risk. Ownership is responsibility, and the business manager is tasked with taking action to manage the risk. Ownership and responsibility also represent potential blame -- blame being part of the mechanism which enforces action. The great concern in having an independent risk management group, both in the risk management literature and amongst respondents in this study, is that business managers will feel 'absolved' of risk, and therefore ignore risk in their day-to-day business decisions. The CFO of a manufacturer, for instance, was most emphatic that it is a mistake to move responsibility for risk out of the businesses, because *"you end-up with misalignment....As soon as someone has the impression that someone else is worrying about that[risk] for them, they'll stop worrying about it."* If business units don't own the risk, then the result is *"that we'll lose control of it even more."*

In fact, outside of the banks, ERM operations were small and largely populated with part-time risk managers who had other key duties (such as audit, financial control, compliance, and strategic planning). These departments also had less direct authority or their authority emanated from their primary job rather than the risk management role per se. Nominal resources and only indirect power meant that, by construction and by necessity, these risk managers did not decide, but instead advised and provided oversight. Ownership rested squarely with the larger organization.

Though philosophically underpinned by agency theory (pushing responsibility down so that the manager's interest is aligned with the larger corporate interest), it is hard to know to what degree these decisions to minimize the risk function are actually representative of a ceremonial performance: establishing visible executive-level risk oversight at the lowest possible cost. But it is worth noting that the concerns voiced above also emerged in the bank holding companies, where the Federal Reserve mandates large, heavily resourced risk departments, with CROs reporting to a designated board risk committee. Despite having a powerful risk management unit, there is still a concern that the business management unit should also care about risk, so responsibility is shared: *"The basic philosophy is that the first line of defense, in terms of risk management, are the businesses themselves... They have to make good risk/return trade-offs; that's their job. And the risk function is the second line of defense...So, I absolutely believe that the businesses own the risk."* (CEO, Bank)

Because this first line of action was outside their remit, interviewed risk managers said little about the actual action taken to reduce risk. Broadly, there were four types of possible actions. First, some types of risk could be controlled through establishing limits capping the volume or nature of a productive activity that produces risk. These constraints were enacted through audit-type processes or computer systems, and were most common in banks (e.g. credit controls, or limits to volumes of particular types of trades). More commonly, though, risks were mitigated, or reduced, through action taken to lessen the potential impact. This could take a wide variety of forms, from buying insurance or hedging instruments, to crisis planning and creating redundancies which would soften the impact of the risk should it materialize. A small set of risks were avoided altogether. For instance, at one bank legal compliance was a *"no-fly"* zone. Finally, a few respondents made a point of saying that accepting a risk by taking no action was also an option. Risks that were tied to decisions which were strategically important to the organization, but which were too costly to substantively mitigate (e.g. business entry into China) seemed to fall into this category.

The picture that emerges is one of using routines to manage risk. The categorization within risk assessment determines the *"bucket"* into which the risk object will be placed. Now that the risk

is clearly defined by type and importance, the business manager knows what to do. Routines are selected by analogy with similar risk objects, somewhat customized, and applied to the new risk object. This allows business unit managers in the larger organization to deal with risk in an efficient manner.

In addition, most of these routines use audit control processes which are traceable and transparent, providing acceptable evidence of proper risk management to the organization's top executives and external stakeholders, including the Board. In fact, it may be the risk managers, in their role as monitor and reporter, who encourage the use of such routines. The use of institutionalized procedures both facilitates risk management oversight, as well as disengaging actions to manage risk from individual capabilities and whims. Risk management without process is dangerous both because it is dependent on a person who can leave and because it creates space for malfeasance.

Re-assessment: business managers calculate

As the term suggests, re-assessment echoes assessment, though now business managers are fully responsible. Re-assessment also adds a layer of complexity. Re-assessment calculates the outstanding probability-weighted cost of the risk object *net of the effect of action.* In other words, if the original potential hazard was estimated to cost $100 million, and $80 million is now insured, then the re-assessed risk outstanding is $20 million. But just as most of the original estimates of probability and cost are subjective, educated guesses cloaked in the guise of objective standardized measurement, so too the effects of mitigation are only occasionally as well-defined as an insurance policy. In addition, ERM goes a step further, expecting organizations to quantify a nebulous "risk appetite." Defining how much risk an organization is willing to take, the agreed risk appetite is to be used as a gauge to decide whether a given risk (or set of risks) is acceptable or unacceptable. Thus re-assessment is problematic on multiple levels.

Monitoring/Reporting: risk management operating in parallel

As soon as a risk is identified, the risk manager begins to shift out of exploratory mode (with respect to a specific risk object), and by the time the risk is assessed, the risk manager's role has been transformed. From that point onward, business management takes ownership, acts and

reassesses, and risk management observes and records from above, as the representative of executive management and the board. Often this shades into control. Control might be through influence (using some of the relational skills of creative challenge), or by directly building *"second-level defenses"* (especially in banking), and as monitor, the risk manager is encouraging management to use the very routines and processes which are suspect when identifying risk.

Across the interviews there were regular references to risk management as an administrative "control function," often associated with audit and compliance. The goal is a controlled environment, which resembles a self-contained cybernetic system through linked processes. For many, a controlled environment was protected by a process devoid of gaps: *"...making sure that there's no breaks in the process chain...you continue to refine this...we have a picture of a little set of arrows that go around in a circle. OK? And you have different inputs around your risks, so you'll have audit feedback, testing feedback, the examiner's feedback, which all informs your control environment."* (Chief Compliance Officer, bank) It is notable that though the language is the scientific language of engineering and systems, the circle described evokes a wagon-train circle, a closed fence keeping the organization safe from the dangers lurking outside. Coverage and sealing gaps were important themes, and in some narratives, gaps were particularly dangerous, *"A lot of times people focus here just on vulnerabilities, right? Let's find all the holes and let's patch all the holes....one way of prioritizing is understanding the threats and understanding the holes they're going after....the geeky side of my team, my security ninjas, right? are looking for bad guys, building firewalls, making sure all the technical things are in place"* (IT risk officer, manufacturer).

Often the *"second-line defenses"* of risk management were exactly as implied by the nomenclature: redundant processes designed to ensure that any cracks that open up at the lower level are still covered. In banking, regulation and self-governance took this philosophy to an extreme, creating surprising hierarchies of surveillance, through the overlapping of multiple control processes to ensure that hazards are kept at bay. For example, in the bank, credit risk is initially evaluated through models developed by the business unit selling loans. These quantitative models are checked and monitored annually by the model validation group within risk management. The internal audit function must then independently verify the models and the

work of the model validation group. Since audit does not have the quantitative modeling expertise to do this, they hire outside consultants. Finally, the Federal Reserve periodically sends in a team of expert specialists to again review the entire process.

Processes, though, are not simply fences. Sometimes they also serve to turn individual personalities into an organizational entity, and the lack of processes is itself a risk. The compliance officer quoted above echoed the regulator in saying that when he arrived at the bank it was *"disjointed"* and required plans and processes with well-defined lines of accountability to fix the company; that is to say, traceable audit processes make the organization whole. At another firm, the CRO and Chief Auditor of a manufacturer was not comfortable with the crisis team which operated on an ad-hoc basis because *"a lot of the plans, a lot of the contingency actions were informal, based on personalities, as opposed to being based on process. That person goes, now all of a sudden, that's the one person who knew how we were gonna react to this thing...you're placing an awful lot of risk in two legs that's walking around with that information in their head if you don't have a process to be able to work it through."* Thus process as a codification of organizational knowledge served to take risk management from a chaotic atomistic level to something integrated and unitary, as well as providing the paper trail necessary for transparency.

Standardized process and commensuration also directly facilitate monitoring and reporting, creating audit trails of accountability. Together, they produce the visibility requisite for central surveillance and tracking. Like audit and compliance, risk management is part of a system of self-reflexive control linked to Board oversight. These systems are designed to construct a singular organizational actor from disparate and far-flung groups of individuals, to provide a bird's eye-view for senior executives to centrally control the organization, and to demonstrate good governance to external audiences. The CRO for a financial services company summed up his responsibilities as: *"I'm responsible for our risk framework...making sure that* [risks] *are within the guard rails that we and our board, and their regulators and investors and everyone else, have set for risk-taking, and that we operate the firm in a safe and sound manner."* From a somewhat different perspective, the Chairman of the Board of a University put it this way, *"So,*

our [the Board's] *duty of oversight would include feeling comfortable that people are managing the risks that are around in a reasonable fashion."*

In performing this "duty," risk managers rely on multiple audit tools. In addition to processes that can be tracked, risk managers produce standardized reports which give a snapshot of the organization's risk profile, and benchmark both to what other organizations are doing. As the reports move up the hierarchy, information about risks is integrated and fine details lost, while processes and their output are distilled into abbreviated summary accounts. By the time it reaches the Board, it has become a shallow and abstract representation of the organization's 'risk profile' limited to a few pages. In deciding what to include and how to format the information, risk managers (and those they reported to) were concerned with meeting external norms. At the ERM peer-group meeting, there was an entire session devoted to *"Best Practices in Board and Audit Committee Reporting Formats"* In fact, though the peer group was intended to be a support structure, "benchmarking" was a constant refrain from all corners. Risk managers were continually comparing each other's practices, trying to surmise the group norm and to ensure that they met or exceeded the norm. In other words, benchmarking is the ultimate mimetic institutionalization (DiMaggio and Powell 1983), and benchmarks have become a key legitimizing tool in modern audit culture (Strathern 2000).

While board reporting was a major concern for risk managers and at times appeared to be the ultimate goal, many were conscious of the ceremonial nature of such reporting; even questioning its productive value and hinting that it gets in the way of 'real' risk management. More than one risk manager spoke of Board members as unable or unwilling to digest too much information, and the need to simplify the material and keep it short, ideally utilizing summary graphs and charts:

> *"And if I show them 10 potential areas where you can lose 10 million, they have the attention span of four-and-half-year-old, you know, and for some reason it's a norm, it's accepted that all our reports are crammed down to that one-pager where they should know everything. I think that's how the world is, and I do the same thing, but the point is, you can't say much in that one page that's really useful."* (Risk Manager, Bank)

Ultimately, board reporting supported the risk management function, endowing risk management with legitimate authority and purpose to its work. However, while all risk managers treated reports to the board as an important task which had to be done well, for those who spoke of creative challenge, it did not define risk management. Rather, reporting was peripheral to efficacious risk management which is founded on creative challenge.

Creative Challenge in the Risk Management Process

Across the process then, risk is transformed. Emerging from the unformed chaos of future uncertainty, it takes shape through naming and measurement. Once delineated, the now concrete risk object can be dealt with and made safe through management routines. What distinguished risk managers who used creative challenge was that they consciously perceived the subjective nature of risk and the socially constructed character of the process of transformation and management. This understanding problematized audit routines for risk identification, so these managers turned to the more open-ended exploratory search of creative challenge.

Paradoxically, though, they also accepted the results of that metamorphosis, at times reifying the risk object, allowing it to be incorporated into routines of audit. As risk moved from being unknown to known -- and from risk management to the larger organization -- risk management itself shifted from identification to monitoring and reporting. Risk was now manageable and reportable, so exploratory search was no longer needed.

Yet monitoring and reporting reflects an odd dual role. Within categories, routines and processes lies a fundamental tension for risk management; they represent a form of protection against risk as well as a resource for legitimacy, yet at the same time they can become a source of risk. As controller and monitor, the risk management function is the archetypal administrative auditor, acting as keeper of the standards, routines and processes which create a transparent control system. But at the same time monitoring represents an opportunity for risk identification. It is in the role of monitor that risk managers often use effective challenge, as they oversee (and sometimes control) assessment, action, and re-assessment. Monitoring for these risk managers wasn't just about 'ticking boxes,' but periodically involved bringing alternative perspectives to

bear and asking questions about the decisions made, data provided, and processes observed. And successful questioning -- questioning that breaks through business managers' defenses, and changes their perspectives and/or actions -- requires relational skills to overcome resistance. In other words, when monitoring, risk managers are constantly cycling between audit routines and creative challenge.

Sometimes such challenge is meant to encourage business managers to rethink the assumptions underlying assessment or action, usually before decisions were solidified and agreed. Such questioning was more likely when managers were seen to rely too heavily on the established nature of things: whether it be actions based on existing routines or assessments assuming that the future will replicate or follow the trajectory of the past. In this way, many managers reported that creative challenge pushed business managers to step aside from automatic thought and action, and to think consciously. Once agreed, though, assessments and action plans became fixed components of the audit process, while risk managers turned from creative challenge back to monitoring and reporting on the approved measures and processes.

In addition, several risk mangers used the phrase *"trust but verify,"* and verification also took the form of effective challenge using relational skills while acting as monitor. For those risk managers concerned with internal risks, individual employees were always a potential source of risk, not only through malfeasance, but through lack of transparency or even over-optimism. A business manager might cover-up or withhold information if it would lead to a negative personal outcome. One type of unreported data, for instance, is mistakes which might result in blame and punishment. The CRO of a manufacturer referred to this type of hidden risk as *"uglies."* Alternatively, business managers might massage or hide data to circumvent controls. Finally, business managers were reported to be over-optimistic in their assessment of the future, and their estimation of their capabilities. To counter all this, risk managers used a paradoxical combination of skeptical sleuthing and trust-building, combined with deep knowledge of the business and tools such as scenario analyses; thereby revealing these risks in the monitoring process.

Thus, paradoxically, monitoring and reporting, despite being at the heart of audit control, also acts as an important platform for risk identification through creative challenge. Generally such challenge is concentrated on the initial construction of standardized measurements and action to be taken to mitigate, when these decisions are still somewhat open-ended and in flux. But risk managers, still aware of the inexact assumptions underlying these categories, numbers and plans, continue to occasionally challenge routines even as they are reified so that the organization can move forward. The result is that the risk management function as monitor uses and maintains audit routines, while intermittently questioning them through creative challenge. Providing a bird's-eye view from which to identify new risks, monitoring loops back in a process which requires the risk manager to hold both audit and creative challenge in tension with one another.

Conclusion

Society's conception of and relationship with the future has radically shifted in the modern era. In earlier eras the future could be assumed to resemble the past within each generation, and to the extent it didn't, and fortune or catastrophe struck, the Gods were in control. Today, however, fast-changing advancements in science and technology have introduced potential future dangers for which the past provides no guidance. Furthermore, as our division of labor and communication networks become more intricate, and as complex and interconnected relationships extend across time and space, ripple effects can quickly escalate small hazards into major catastrophes should disaster strike. Moreover, these new "manufactured" risks are the result of human agency. Organizations and institutions, not the Gods, are to blame. Paradoxically, then, we are in control of the means by which the world seems out of control. As a result, society as a whole has become increasingly reflexive with regards to risk.

Organizational risk management has not been immune to this transformation. Whereas once risk management was left to the individual business managers as they made their day-to-day decisions, and the role of risk manager was limited to deciding which insurance policies to buy, a growing number of important stakeholders are demanding that organizations be similarly reflexive: consciously evaluating, managing and controlling risk across the organization. For

some organizations, such as HROs, it has come more naturally. Risk and crisis management is critical to their core mission (although even at NASA, safety was compromised in the face of the competing goal to launch on time (Vaughan 1997)), but for most organizations risk management easily takes a back seat to other primary goals. Stakeholders, therefore, don't trust business management to manage risk on their own, and instead are asking for specific risk oversight by the CEO and the board of directors, ideally supported by a corporate-level risk management function and visible, transparent processes of control. In response, a large majority of those organizations with sufficient resources have implemented Enterprise Risk Management practices.

At the heart of ERM is the concept of 'good governance,' demonstrated and legitimized through the generally recognized measurement and processes of audit. This much has been observed already by scholars skeptical of risk management, and interviews and observations in this study corroborate their findings. However, contrary to existing accounts that dismiss ERM as ceremonial show, this study demonstrates that at least some risk managers combine ERM's audit routines of legitimacy with the incongruous open and questioning mindset and techniques of creative challenge, believing the latter to be at the heart of efficacious risk management.

Because research on the empirical practices of risk management has been cabined in discrete and opposing streams, and because both streams have by-passed the risk management process per se, the simultaneous enactment of audit and creative challenge within the same organization has heretofore not been recognized. In spite of widespread self-representations of risk management as a process which occurs in discrete stages, organizational scholars of risk management have failed to directly incorporate this into their analyses. This gap is significant in light of the degree to which practitioners organize their activities around discrete phases in a process. Safety culture and HRO literature has instead concentrated on how successful organizations manage crises, and prevent risks based on analyses of near-crises, and research rarely problematizes the potential hazard as such. Rather than focusing on the risk management process, safety culture theory views risk and crisis management holistically, and HRO mindfulness is presented as a constant state of attentiveness to safety and reliability on the part of the entire organization. Similarly, in the audit and governance approach, analyses cut across the process, emphasizing

routines which support legitimacy, such as the social construction of 'scientific' quantitative measures for qualitative uncertainty, the procedural nature of actions, and the ceremonial nature of risk reporting. The unintended result is that attention is directed at assessments and processes of control and monitoring, while skirting around how risks are identified in the first place. To the extent that identification is addressed, it is largely dismissed as undifferentiated 'list-making' (Huber 2010), which only amplifies the organization's perception of risk (Power), thereby undermining the organizational 'resilience' required to effectively deal with crisis (Wildavsky 1988).

Ethnographies and interviews of bank risk managers by Mikes (Mikes 2011, Hall et al. 2013) have turned up techniques akin to creative challenge that are used by "quantitative skeptic" risk managers (in contrast to "quantitative enthusiasts" who restrict their work to the quantitative modelling of risk). These studies, however, do not consider its combination with audit routines, because they use the organization as the level of analysis, focusing on comparing organizations which use exploratory, questioning, and relational techniques vs. those that stick to sophisticated, formalized computer models to manage risk. The conclusion is that differences are inter-organizational, and that each bank follows a single, coherent approach. Survey studies on ERM practices similarly suggest that ERM practice will be contingent on the dominant type of risk faced by the organization/industry (Mikes and Kaplan 2014).

By contrast, this study shows that these varied modes of inquiry and practice exist within the same organization, depending on which stage of the risk management process is operative. Many of the very same managers, who endorse audit techniques in risk assessment, management, and monitoring/reporting, turn to radically different methods when identifying risk, calling on the exploratory techniques of creative challenge. Significantly, though, risk managers who employ creative challenge for risk identification consider it to be the essential substance of their job, representing it as the critical task in accomplishing effective risk management which they uniquely provide. Yet at the same time, creative challenge puts into question the very audit measurements and routines which they must and do enact for continuing organizational legitimacy. In this, the risk management function echoes the ever-present organizational tension between productivity and legitimacy (Weber 1978, Crozier 2009, Blau 1956), as they juggle

these competing claims. But more than this, I hypothesize that the way risk managers combine these seemingly contradictory approaches across the risk management process helps the organization as a whole to enhance legitimacy *and* to confront risk productively by buffering the organizational encounter with risk.

Truly facing risk is difficult for people and organizations. The radical uncertainty of the modern age is overwhelming. It is impossible to even name all the potentialities which might destroy our goals or cause us harm, let alone act on them; yet society's mechanism is to demand protection from risk through a proliferating array of legal and organizational controls. Where do organizations even start? These ambiguous future possibilities have the potential for making the current goals and plans "unintelligible" thereby disrupting action (Weick et al. 2005) and freezing forward movement. Moreover, risk management is characterized by an unstable, subjective "non-goal" focused on avoidance of unspecified 'risk' (Roberts and Creed 1993) that is fundamentally at odds with the typical organizational goals that drive the organization by specifying singular objective outcomes (such as earning $X profits). The two are like oil and water. Thus confronting risk is itself risky for the organization as a whole.

Risk managers who emphasized creative challenge put risk identification at the heart of their productive role. In these accounts, the risk management function 'managed' the initial organizational encounter with risk. Though the larger organization clearly participated, such participation was not ongoing, and it was the risk management unit who took the brunt of the encounter. Risk management function seemed to lessen risk's impact on the rest of the organization by using relational skills to take the edge off unsettling questions and to establish themselves not just as overseers, but as helpmates, as well as by providing safe spaces for business managers to explore significant danger.

When, next, the identified danger needed to be distributed to the larger organization, it was first 'translated' into a well-defined and workable risk object through joint assessment. Speaking in the common language of agreed categories and expected value facilitated internal communication and transfer, as it is through such "'legitimate' estimates" that "all parts of the organization act on the same premises" (March and Simon 1958/1993:188). However,

translation was not just a matter of language, but also constituted a real conversion. Through assessment, risk was redefined from an abstract idea into an object which business managers could quickly grasp and incorporate into their existing activities. The non-goal became a clear, targeted and quantified goal to be efficiently addressed with known routines and processes. Thus for these risk managers, audit routines appeared to be multipurpose. Not only did they provide external legitimacy to stakeholders expecting evidence of good governance, but their wide acceptance afforded the internal legitimacy needed to transform raw danger into a manageable risk object. Finally, the common currency of audit and its routines potentially allowed for efficient action on the part of the larger organization. Based on this fixed understanding, the organization could proceed, only intermittently faced with the insecurity of risk through risk management's use of creative challenge. In this way, it may be that risk safely becomes part of the warp and weft of daily work.

In light of these findings, we may need to rethink our theoretical understanding of risk management. This study shows that exploratory modes of risk identification through creative challenge do exist alongside audit routines within ERM, and suggests that such routines may not be solely for legitimation but may also serve as shock absorbers between the initial encounter with risk within risk management and the larger organization, thus enhancing productivity. And, while this qualitative research makes no claim of generalizability, it is striking that several instances of creative challenge were visible in this small population of organizations and that both the manufacturer and the bank, subjected to more in-depth study, reported the dual approach to risk management. Further, ethnographic work in banks by Mikes also describes something similar, though the analysis is limited by the original framing of "quantitative cultures" specific to banks. By using the higher level classifications of exploratory creative challenge (non-automatic processing and action) vs. audit routines (automatic processing and action), this analysis frames the duality in broader terms, recognizing that the observed phenomena extends to the general organizational population. All this suggests that creative challenge might be found in many organizations.

Like March's (1991) exploratory search or Stark's (2009) reflective cognition, encountering risk is about searching the unknown, especially the unknown future, and it is notable that the duality

of creative challenge and audit mirrors the contrast between exploration and exploitation. Just as organizations struggle to balance productivity and legitimacy, so too do they find it difficult to balance exploration and exploitation (March 1991, Chen and Katila 2008). Corporations are found to pursue both by separating the two modes sequentially (cycling over time) or spatially (by role or unit) (Gupta et al. 2006, Chen and Katila 2008). Accounts in this study of risk managers using creative challenge, suggest that while risk management itself must be "ambidextrous," it creates an environment of "punctuated equilibrium" (Gupta et al. 2006) for the organization as a whole, allowing for productive efficiency much of the time. Ambidexterity, though, assumes "differentiated subunits or individuals" while here the same individuals are doing both. This study documents the duality, but does not contain the micro-observations necessary to answer how individuals practically accomplish this. It is conceivable that closer study of risk management in organizations which employ creative challenge might both inform and be informed by research on exploration/exploitation.

Limitations and Future Research

The results here suggest several interesting lines of research, many of which would require going beyond interviews to micro-observations of risk managers who describe using creative challenge techniques. The first question to answer is whether risk managers actually 'do' what they 'say.' A particular understanding of risk seems to undergird out of the box thinking and techniques of creative challenge, thereby making the picture logical and believable, nonetheless, it would be important to observe how this actually plays out in daily practice. And if indeed, risk managers toggle between exploratory creative challenge and audit routines, how is this specifically accomplished? Careful observation of such ambidexterity has the potential to contribute to theory and help explain phenomena beyond risk management.

Other questions take research to a broader scale. How typical is the use of creative challenge? This non-random sample suggests that it might be widespread, but it remains uncertain. More importantly, does creative challenge actually make a difference? And if so, what kind of difference? Risk theories argue that such an open, questioning approach is more efficacious, while risk managers who described creative challenge, believed that it was critical for successful risk management, but is it? Performance measurement of risk management efforts is problematic

(one is trying to measure the counterfactual, 'What could have happened but didn't?'), but such measurements will be critical to determining more definitively whether creative challenge 'works.'

Finally, studies of ERM practice across time would have the potential to demonstrate more specifically how larger processes of institutionalization happen in the present, rather than through looking into the past, after the fact. For most of these organizations ERM is relatively new and still in the process of development. Research on the diffusion of new management practices has shown that early adopters tend to customize as they address real problems, while later adopters are more likely to choose normative standards for legitimacy's sake (Westphal, Gulati and Shortell 1997). Likewise, research on exploration and exploitation has shown that over time "a natural organizational tendency exists towards exploitation [over exploration]." (Chen and Katila 2008) Moreover, many of these senior risk managers felt that their creative perspective was the result of diverse personal experience, yet risk management shows all the hallmarks of moving towards a profession supported by certification and a formalized career path (Abbott 1988). All this suggests that creative challenge may disappear within risk management, subsumed by the routines of audit. In other words, will creative challenge last?

Table 1:

Respondents by current position(s) and industry, based on 2-digit NAICS code[1]

NAICS Codes	Head of Risk Mgmt	Other Risk Manager	Board Member	CEO[2]	C-Suite	Other
21 Oil & gas extraction	P = 1					
31 Mfg: Food, tobacco, textile, apparel	P = 2		I = 1			
32 Mfg: printing, chemical, pharma	P = 1		I = 3	I = 1		
33 Mfg: equipment and machinery (incl tech)	I = 1 P = 6	I = 3 P = 1	I = 3		I = 1	I = 3
44 Retail		P = 1	I = 1		P = 1	
48 Transportation						
51 Finance	I = 2	I = 10	I = 2	I = 2	I = 2	
54 Prof Services						I = 2
61 Education	I = 1		I = 5			I = 1
92 Public Admin						I = 2

[1] Some respondents held positions at more than one company, especially board members. These are coded as multiple entries.

[2] CEOs can be assumed to also be the Chairman of the Board, but since it is for the same company, they are coded only as CEO.

I = interviewee

P = participant at peer network meeting

Table 2:

All relevant roles and industries represented by respondents (includes past experience)[1]

NAICS Codes	Head of Risk Mgmt	Other Risk Manager	Board Member	CEO[2]	C-Suite	Other
21 Oil & gas extraction	P = 1					
31 Mfg: Food, tobacco, textile, apparel	P = 2		I = 1			I = 1
32 Mfg: printing, chemical, pharma	P = 1		I = 3	I = 1		I = 1
33 Mfg: equipment and machinery (incl tech)	I = 1 P = 6	I = 4 P = 1	I = 3		I = 1	I = 4
44 Retail		P = 1	I = 1		P = 1	
48 Transportation						
51 Information Services	I = 1					
52 Finance	I = 2	I = 10	I = 4	I = 2	I = 2	I = 1
54 Prof Services						I = 3
56 Admin & Waste Services	I = 2					
61 Education	I = 1		I = 5			I = 1
92 Public Admin		I = 2	I = 1			I = 2

[1] Some respondents held positions at more than one company, especially board members. These are coded as multiple entries.

[2] CEOs can be assumed to also be the Chairman of the Board, but since it is for the same company, they are coded only as CEO.

I = interviewee

P = participant at peer network meeting

References

Abbott, Andrew. 1988. *The System of Professions: An Essay on the Division of Expert Labor.* Chicago: University Of Chicago Press.

Adams, John. 1995. *Risk.* London England : Bristol, PA: Routledge.

American Institute of Certified Public Accountants. 2013. "AU Section 508: Reports on Audited Financial Statements." *AICPA.* Retrieved June 20, 2014 (http://www.aicpa.org/Research/Standards/AuditAttest/DownloadableDocuments/AU-00508.pdf).

Austin, J. L., J. O. Urmson, and Marina Sbisà. 1975. *How to Do Things with Words.* 2nd ed. Cambridge, Mass.: Harvard University Press.

Baker, Tom, and Jonathan Simon. 2002. *Embracing Risk: The Changing Culture of Insurance and Responsibility.* Chicago: University Of Chicago Press.

Beck, Ulrich. 1992. *Risk Society: Towards a New Modernity.* Newbury Park, CA: SAGE.

Beasley, Mark, Bruce Branson, and Bonnie Hancock. 2014. *Report on the Current State of Enterprise Risk Oversight: Opportunities to Strengthen Integration with Strategy.* ERM Initiative, North Carolina State University.

Bernstein, Peter L. 1998. *Against the Gods: The Remarkable Story of Risk.* New York: Wiley.

Bigley, Gregory A., and Karlene H. Roberts. 2001. "The Incident Command System: High-Reliability Organizing for Complex and Volatile Task Environments." *The Academy of Management Journal* 44(6):1281–99.

Blau, Peter Michael. 1956. *Bureaucracy in Modern Society.* New York: Random House.

Bradford, Josh and Carol Fox, eds. RIMS. 2013. *ERM Is Here to Stay: 2013 RIMS Enterprise Risk Management Survey.*

Charmaz, Kathy. 2006. *Constructing Grounded Theory: A Practical Guide through Qualitative Analysis.* Newbury Park: SAGE.

Chen, Eric, and Riitta Katila. 2008. "Rival Interpretations of Balancing Exploration and Exploitation: Simultaneous or Sequential?" Pp. 197–214 in *The Handbook of Technology and Innovation Management*, edited by Scott Shane. Chichester, Hoboken, NJ: Wiley-Blackwell.

Clarke, Lee. 2001. *Mission Improbable: Using Fantasy Documents to Tame Disaster.* Chicago: University Of Chicago Press.

Corbin, Juliet M. 1998. *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory.* 2nd ed. Thousand Oaks, CA: SAGE.

Cosier, Richard A. 1978. "The Effects of Three Potential Aids for Making Strategic Decisions on Prediction Accuracy." *Organizational Behavior and Human Performance* 22(2):295–306.

Crozier, Michel. 2009. *The Bureaucratic Phenomenon*. New Brunswick, NJ: Transaction Publishers.

Cyert, Richard Michael, and James G. March. 1963. *A Behavioral Theory of the Firm*. Cambridge, MA: Basil Blackwell.

Dewey, John. 2009. *The Essential Dewey, Vol. 2: Ethics, Logic, Psychology*. edited by Thomas M. Alexander. Bloomington: Indiana University Press.

DiMaggio, Paul J., and Walter W. Powell. 1983. "The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields." *American Sociological Review* 48(2):147–60.

Dobbin, Frank. 2011. *Inventing Equal Opportunity*. Princeton: Princeton University Press.

Douglas, Mary. 1984. *Purity and Danger: An Analysis of the Concepts of Pollution and Taboo*. New Ed edition. London: Routledge.

Douglas, Mary. 1994. *Risk and Blame: Essays in Cultural Theory*. New Ed edition. New York: Routledge.

Douglas, Mary, and Aaron Wildavsky. 1982. *Risk and Culture: An Essay on the Selection of Technological and Environmental Dangers*. Berkeley: University of California Press.

Doyle, Aaron, and Richard V. Ericson. 2003. *Risk and Morality*. Toronto: University of Toronto Press, Scholarly Publishing Division.

Espeland, Wendy Nelson, and Michael Sauder. 2007. "Rankings and Reactivity: How Public Measures Recreate Social Worlds." *American Journal of Sociology* 113(1):1–40.

Espeland, Wendy Nelson, and Mitchell L. Stevens. 1998. "Commensuration as a Social Process." *Annual Review of Sociology* 24:313–43.

Espeland, Wendy Nelson, and Berit Irene Vannebo. 2007. "Accountability, Quantification, and Law." *Annual Review of Law and Social Science* 3(1):21–43.

Ewald, Francois. 1991. "Insurance and Risk." Pp. 197–210 in *The Foucault Effect: Studies in Governmentality*, edited by Michel Foucault, Graham Burchell, Collin Gordon, and Peter Miller. London: Harvester Wheatsheaf.

Ewick, Patricia. 1998. *The Common Place of Law: Stories from Everyday Life*. Chicago: University Of Chicago Press.

Ewick, Patricia, and Susan Silbey. 2003. "Narrating Social Structure: Stories of Resistance to Legal Authority." *American Journal of Sociology* 108(6):1328–72.

Florida, Richard. 2014. *The Rise of the Creative Class--Revisited: Revised and Expanded.* New York: Basic Books.

Foucault, Michel. 1995. *Discipline & Punish: The Birth of the Prison.* 2nd ed. New York: Vintage Books.

Freudenburg, William R. 1993. "Risk and Recreancy: Weber, the Division of Labor, and the Rationality of Risk Perceptions." *Social Forces* 71(4):909–32.

Garland, David. 2003. "The Rise of Risk." Pp. 48–86 in *Risk and Morality*, edited by Richard V. Ericson and Aaron Doyle. Toronto: University of Toronto Press, Scholarly Publishing Division.

Giddens, Anthony. 1990. *The Consequences of Modernity.* Stanford: Stanford University Press.

Giddens, Anthony. 1999. "Risk and Responsibility." *The Modern Law Review* 62(1):1–10.

Glaser, Barney, and Anselm Strauss. 1967. *The Discovery of Grounded Theory: Strategies for Qualitative Research.* London: Weidenfield and Nicolson.

Gray, Garry, and Susan Silbey. forthcoming. "Governing Inside the Organization: Interpreting Regulation and Compliance." *American Journal of Sociology.*

Guldenmund, Frank W. 2000. "The Nature of Safety Culture: A Review of Theory and Research." *Safety Science* 34(1–3):215–57.

Gupta, Anil K., Ken G. Smith, and Christina E. Shalley. 2006. "The Interplay between Exploration and Exploitation." *The Academy of Management Journal* 49(4):693–706.

Hacking, Ian. 1990. *The Taming of Chance.* New York: Cambridge University Press.

Hacking, Ian. 2006. *The Emergence of Probability: A Philosophical Study of Early Ideas about Probability, Induction and Statistical Inference.* 2nd ed. New York: Cambridge University Press.

Hall, Matthew, Anette Mikes, and Yuval Millo. 2013a *How Do Risk Managers Become Influential? A Field Study in Two Financial Institutions.* Working Paper, Harvard Business School, October 17. Retrieved June 21, 2014 (http://www.hbs.edu/faculty/Publication%20Files/11-068_f1d5bd99-e47e-41a2-84ea-c4fd055e261d.pdf).

Heimer, Carol A. 1985. "Allocating Information Costs in a Negotiated Information Order: Interorganizational Constraints on Decision Making in Norwegian Oil Insurance." *Administrative Science Quarterly* 30(3):395–417.

Heimer, Carol A. 1989. *Reactive Risk and Rational Action: Managing Moral Hazard in Insurance Contracts.* Berkeley: University of California Press.

Heimer, Carol A., Juleigh Coleman, Petty Culyba, and Rebecca Culyba. 2005. "Risk and Rules: The 'Legalization' of Medicine."Pp. 92–131 in *Organizational Encounters with Risk*, edited by Bridget Hutter and Michael Power. New York: Cambridge University Press.

Hilgartner, Stephen. 1992. "The Social Construction of Risk Objects: Or, How to Pry Open Networks of Risk." Pp. 39–53 in *Organizations, Uncertainties and Risks*, edited by James Short and Lee Clarke. Boulder, CO: Westview Press.

Hodgson, Godfrey. 1984. *Lloyd's of London*. New York: Viking.

Hood, Christopher. 2002. "The Risk Game and the Blame Game." *Government and Opposition* 37(01):15–37.

Huber, Michael. 2010. "Colonised by Risk - The Emergence of Academic Risks in British Higher Education." Pp. 114–36 in *Anticipating Risks and Organising Risk Regulation*, edited by Bridget M. Hutter. Cambridge: Cambridge University Press.

Huising, Ruthanne, and Susan Silbey. 2011. "Governing the Gap: Forging Safe Science through Relational Regulation." *Regulation & Governance* 5(1):14.

Hutter, Bridget M. 2010. *Anticipating Risks and Organising Risk Regulation*. Cambridge: Cambridge University Press.

Hutter, Bridget, and Michael Power. 2005. *Organizational Encounters with Risk*. Cambridge: Cambridge University Press.

Jackall, Robert. 2009. *Moral Mazes: The World of Corporate Managers*. Updated Edition. New York: Oxford University Press.

Kahneman, Daniel, Paul Slovic, and Amos Tversky, eds. 1982. *Judgment under Uncertainty: Heuristics and Biases*. New York: Cambridge University Press.

Kellogg, Katherine C. 2009. "Operating Room: Relational Spaces and Microinstitutional Change in Surgery." *American Journal of Sociology* 115(3):657–711.

Knight, Frank. 1921/1965. *Risk, Uncertainty, and Profit*. New York: Harper and Row.

LaPorte, Todd R., and Paula M. Consolini. 1991. "Working in Practice but Not in Theory: Theoretical Challenges of 'High-Reliability Organizations.'" *Journal of Public Administration Research and Theory: J-PART* 1(1):19–48.

Lavie, Dovev, Uriel Stettner, and Michael L. Tushman. 2010. "Exploration and Exploitation Within and Across Organizations." *Academy of Management Annals* 4(1):109–55.

Lester, Richard K., and Michael J. Piore. 2006. *Innovation--The Missing Dimension*. Cambridge, MA: Harvard University Press.

Leveson, Nancy, Nicolas Dulac, Karen Marais, and John Carroll. 2009. "Moving Beyond Normal Accidents and High Reliability Organizations: A Systems Approach to Safety in Complex Systems." *Organization Studies* 30(2-3):227–49.

Levinthal, Daniel A., and James G. March. 1993. "The Myopia of Learning." *Strategic Management Journal* 14(S2):95–112.

Levinthal, Daniel, and Claus Rerup. 2006. "Crossing an Apparent Chasm: Bridging Mindful and Less-Mindful Perspectives on Organizational Learning." *Organization Science* 17(4):502–13.

Lofland, John, and Lyn Lofland. 1995. *Analyzing Social Settings: A Guide to Qualitative Observation and Analysis*. Belmont, CA: Wadsworth.

Lyneis, John. 2012. "Resistance from Top to Bottom: The Dynamics of Risk Managment in Complex Organizations." Ph.D. Dissertation, Sloan School of Management, Massachusetts Institute of Technology, Cambridge, MA.

March, James G. 1991. "Exploration and Exploitation in Organizational Learning." *Organization Science* 2(1):71–87.

March, James G., and Zur Shapira. 1987. "Managerial Perspectives on Risk and Risk Taking." *Management Science* 33(11):1404–18.

March, James G., and Herbert Simon. 1958/1993. *Organizations*. New York: John Wiley & Sons.

Markowitz, Harry M. 1959. *Portfolio Selection: Efficient Diversification of Investments*. New York: John Wiley & Sons.

Mason, Richard O. 1969. "A Dialectical Approach to Strategic Planning." *Management Science* 15(8):B403–B414.

Meyer, John W., and Brian Rowan. 1977. "Institutionalized Organizations: Formal Structure as Myth and Ceremony." *American Journal of Sociology* 83(2):340–63.

Mikes, Anette. 2011. "From Counting Risk to Making Risk Count: Boundary-Work in Risk Management." *Accounting, Organizations and Society* 36(4–5):226–45.

Mikes, Anette, and Robert S. Kaplan. 2013. *Towards a Contingency Theory of Enterprise Risk Management*. Harvard Business School Working Paper 13-063. Retrieved June 21, 2014 (http://www.hec.unil.ch/documents/seminars/dcc/1102.pdf).

Miller, Roger, and Donald R. Lessard. 2008. "Evolving Strategy: Risk Managmeent and the Shaping of Mega-Projects." Pp. 145–72 in *Decision-Making On Mega-Projects: Cost-Benefit Analysis, Planning and Innovation*, edited by Hugo Priemus, Bent Flyvbjerg, and Bert van Wee. Northampton, MA: Edward Elgar.

Nelson, Robert L., and Laura Beth Nielsen. 2000. "Cops, Counsel, and Entrepreneurs: Constructing the Role of Inside Counsel in Large Corporations." *Law & Society Review* 34(2):457–94.

Ocasio, William. 1997. "Towards an Attention-Based View of the Firm." *Strategic Management Journal* 18(Summer Special Issue):187–206.

Ocasio, William. 2011. "Attention to Attention." *Organization Science* 22(5):1286–96.

Perrow, Charles. 1984. *Normal Accidents: Living with High-Risk Technologies*. New York: Basic Books.

Porter, Theodore M. 1996. *Trust in Numbers*. Princeton, N.J.: Princeton University Press.

Power, Michael. 1997. *The Audit Society: Rituals of Verification*. New York: Oxford University Press.

Power, Michael. 2007. *Organized Uncertainty: Designing a World of Risk Management*. New York: Oxford University Press.

Power, Michael, Tobias Scheytt, Kim Soin, and Kerstin Sahlin. 2009. "Reputational Risk as a Logic of Organizing in Late Modernity." *Organization Studies* 30(2-3):301–24.

Protiviti. 2006. *Guide to Enterprise Risk Management: Frequently Asked Questions*.

Ray, Joshua L., Lakami T. Baker, and Donde Ashmos Plowman. 2011. "Organizational Mindfulness in Business Schools." *Academy of Management Learning & Education* 10(2):188–203.

Reason, James T. 1997. *Managing the Risks of Organizational Accidents*. Aldershot, England: Ashgate.

Roberts, Karlene H. 1990. "Some Characteristics of High Reliability Organizations." *Organization Science* 1(2):160–77.

Roberts, Karlene H., and W. E. Douglas Creed. 1993. "Epilogues." Pp. 249–56 in *New Challenges to Understanding Organizations*, edited by Karlene Roberts. New York: Macmillan College Div.

Roger Miller, and Donald R. Lessard. 2008. "Evolving Strategy: Risk Management and the Shaping of Mega-Projects." Pp. 145–72 in *Decision-Making on Mega-Projects: Cost Benefit Analysis, Planning and Innovation, Tansport Economics, Management and Policy*, edited by Hugo Priemus, Bent Flyvbjerg, and Bert van Wee. Northampton, MA: Edward Elgar.

Rowling, J. K. 1999. *Harry Potter and the Sorcerer's Stone*. New York: Scholastic.

Rudolph, Jenny W., and Nelson P. Repenning. 2002. "Disaster Dynamics: Understanding the Role of Quantity in Organizational Collapse." *Administrative Science Quarterly* 47(1):1–30.

Russell, Pat. 1996. "Exercising Self-Control." *Accountancy* 117(1231):67.

Sagan, Scott Douglas. 1993. *The Limits of Safety: Organizations, Accidents, and Nuclear Weapons*. Princeton, N.J.: Princeton University Press.

Sauder, Michael, and Wendy Nelson Espeland. 2009. "The Discipline of Rankings: Tight Coupling and Organizational Change." *American Sociological Review* 74(1):63–82.

Schulman, Paul R. 1993. "The Analysis of High Reliability Organizations: A Comparative Framework."Pp. 33-53 in *New Challenges to Understanding Organizations*, edited by KH Roberts. New York: Macmillan 33–53.

Schwenk, Charles R. 1990. "Effects of Devil's Advocacy and Dialectical Inquiry on Decision Making: A Meta-Analysis." *Organizational Behavior and Human Decision Processes* 47(1):161–76.

Schwenk, Charles R., and Richard A. Cosier. 1980. "Effects of the Expert, Devil's Advocate, and Dialectical Inquiry Methods on Prediction Performance." *Organizational Behavior and Human Performance* 26(3):409–24.

Shamir, Ronen. 2008. "The Age of Responsibilization: On Market-Embedded Morality." *Economy and Society* 37(1):1–19.

Shapiro, Susan P. 1987. "The Social Control of Impersonal Trust." *American Journal of Sociology* 93(3):623–58.

Silbey, Susan S. 2009. "Taming Prometheus: Talk About Safety and Culture." *Annual Review of Sociology* 35(1):341–69.

Silbey, Susan S. 2011. "The Sociological Citizen: Pragmatic and Relational Regulation in Law and Organizations." *Regulation & Governance* 5(1):1.

Silbey, Susan, Ruthanne Huising, and Salo Vinocur Coslovsky. 2009. "The 'sociological citizen' relational interdependence in law and organizations." *L'Année sociologique* 59(1):201–29.

Simon, James G. March Herbert A. 1958. *Organizations*. New York: Wiley.

Slovic, Paul 1987. "Perception of Risk." *Science* 236(4799):280–85.

Small, Mario Luis. 2009. "'How Many Cases Do I Need?' On Science and the Logic of Case Selection in Field-Based Research." *Ethnography* 10(1):5–38.

Stark, David. 2011. *The Sense of Dissonance: Accounts of Worth in Economic Life*. Princeton: Princeton University Press.

Strathern, Marilyn. 2000. *Audit Cultures: Anthropological Studies in Accountability, Ethics and the Academy*. London: Routledge.

Taleb, Nassim Nicholas. 2010. *The Black Swan: The Impact of the Highly Improbable."* 2nd ed. New York: Random House Trade Paperbacks.

Thompson, James D. 2003. *Organizations in Action: Social Science Bases of Administrative Theory*. New Brunswick, NJ: Transaction Publishers.

Tsoukas, Haridimos, and Robert Chia. 2002. "On Organizational Becoming: Rethinking Organizational Change." *Organization Science* 13(5):567–82.

Turner, Ralph H. 1969. "The Theme of Contemporary Social Movements." *British Journal of Sociology* 2.

Vaughan, Diane. 1997. *The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA*. Chicago: University Of Chicago Press.

Vaughan, Diane. 1999. "The Dark Side of Organizations: Mistake, Misconduct, and Disaster." *Annual Review of Sociology* 25:271–305.

Vaughan, Diane. 2005a. "Organizational Rituals of Risk and Error." Pp. 33–66 in *Organizational Encounters with Risk*, edited by Bridget Hutter and Michael Power. Cambridge: Cambridge University Press.

Vaughan, Diane. 2005b. "System Effects: On Slippery Slopes, Repeating Negative Patterns, and Learning from Mistake?" Pp. 41–59 in *Organization at the Limit: Lessons from the Columbia Disaster*, edited by William Starbuck and Moshe Farjoun. Maldern, MA: Wiley-Blackwell.

Weber, Max. 1978. *Economy and Society: An Outline of Interpretive Sociology*. New Ed edition. Berkeley: University of California Press.

Weick, Karl E., and Karlene H. Roberts. 1993. "Collective Mind in Organizations: Heedful Interrelating on Flight Decks." *Administrative Science Quarterly* 38(3):357–81.

Weick, Karl E., Kathleen M. Sutcliffe, and David Obstfeld. 1999. "Organizing for High Reliability: Processes of Collective Mindfulness." Pp. 81–123 in *Research in Organizational Behavior*, vol. 1. Greenwich, CT: Jai Press.

Weick, Karl E., Kathleen M. Sutcliffe, and David Obstfeld. 2005. "Organizing and the Process of Sensemaking." *Organization Science* 16(4):409–21.

Weick, Karl, and Kathleen Sutcliffe. 2001. *Managing the Unexpected: Assuring High Performance in an Age of Uncertainty*. San Francisco: Wiley.

Westphal, James D., Ranjay Gulati, and Stephen M. Shortell. 1997. "Customization or Conformity? An Institutional and Network Perspective on the Content and Consequences of TQM Adoption." *Administrative Science Quarterly* 42(2):366–94.

Wildavsky, Aaron. 1988. *Searching for Safety*. 4th ed. New Brunswick, NJ: Transaction Publishers.

Wildavsky, Aaron, and Karl Drake. 1990. "Theories of Risk Perception: Who Fears What and Why?" *Daedalus* 119:41–60.

Zhang, Hui, D. A. Wiegmann, T. L. von Thaden, G. Sharma, and A. A. Mitchell. 2002. "Safety Culture: A Concept in Chaos?" *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 46(15):1404–8.