



# Manifold Conceptions of the Internal Auditing of Risk Culture in the Financial Sector

Vikash Kumar Sinha<sup>1,2</sup> · Marika Arena<sup>2</sup>

Received: 20 November 2017 / Accepted: 4 July 2018  
© The Author(s) 2018

## Abstract

This exploratory study investigates the manifold conceptions of the internal auditing (IA) of risk culture prevalent among four influential actors of the financial sector—regulators, normalizers, consultants, and implementers. By inductive analysis of 20 interviews and 295 documents, we illustrate a two-step interpretive scheme utilized by the four actors in their IA approaches of risk culture: defining broad goals and designing visibility schemes. The visibility schemes were tied to the demarcation, measurement, as well as the IA data collection techniques of risk culture. Our results indicate two dichotomous interpretations among the four actors concerning the IA of risk culture. The first interpretation, prevalent among regulators and implementers, promotes the control of risk culture primarily through verification. The second interpretation, adopted by consultants and normalizers, promotes the control of risk culture by IA along with the empowerment of employees through training programs. Our results not only contribute to understanding IA expansions, specifically to non-tangible domains such as risk culture but also enrich the literature exploring the mechanisms different stakeholders utilize to shape weakly professionalized IA practices.

**Keywords** Internal audit · Risk culture · Auditability · Financial sector

## Introduction

Recent banking scandals and failures are often linked to rampant and inappropriate risk culture that allows excessive risk-taking in banks (Carretta et al. 2017; Palermo et al. 2016). As a reaction, regulators such as the Financial Stability Board (FSB), the Basel Committee on Banking Supervision (BCBS), and the European Banking Authority (EBA) issued broad guidelines on risk culture control, involving internal auditing (IA) processes (Ring et al. 2016). These regulatory initiatives stirred a controversial debate on the IA of risk culture among various stakeholders: the professional bodies—the Institute of Internal Auditors (IIA) and

the Institute of Risk Management (IRM)—hereby referred to as the normalizers, consultants, and practitioners/implementers (Palermo et al. 2016). While the debate provoked various stakeholders suggesting approaches on the IA of risk culture, it did not result in a shared understanding (Ring et al. 2016).

This lack of a shared understanding among the different stakeholders provided empirical motivation for this study to understand their viewpoints. Further motivation for the paper arose from the three underlying challenges in the application of IA to risk culture. First, unlike organizational processes such as risk management where specific protocols, process ownership, and departments provide tangible boundaries for IA (Hall et al. 2015; Mikes 2009, 2011), risk culture concerns the intangible domain of individual motivations and behaviors (Cornia et al. 2016). This raises ethical concerns on how far IA should colonize and control employees through the IA of risk culture (Ezzy 2001; McCabe 2014). Second, involvement of different stakeholders (Erasmus and Coetzee 2018; Roussy and Brivot 2016), application to a variety of processes (Hayne and Free 2014; Spira and Page 2003), heterogeneity (Arena and Jeppesen 2015; Jiang et al. 2018), and unclear ethical guidelines (Friedberg 1998) have

✉ Vikash Kumar Sinha  
vikashs@kth.se

Marika Arena  
marika.arena@polimi.it

<sup>1</sup> Industrial Economics and Management, KTH Royal Institute of Technology, Lindstedtsvägen 30, 100 44 Stockholm, Sweden

<sup>2</sup> Management, Economics and Industrial Engineering, Politecnico Di Milano, Via Lambruschini 4/b, Milan, Italy

sometimes challenged IA's abilities in achieving its ethical ideal of independence and objectivity (Everett and Tremblay 2014; Neu et al. 2013). The compromised nature of existing IA practices raises concern on how IA could assure risk culture (Christopher et al. 2009; Mihret 2014). Third, the problem of the IA of risk culture is exacerbated by an existing incoherent understanding of risk culture, its production, or alteration within organizations (Palermo et al. 2016), and its relationship with the organizational culture (Schein 1990, 2004).

In addition to the three challenges mentioned above, a paucity of literature on "how IA expands to new domains" (cf. Chambers and Odar 2015; Gramling et al. 2004; Parker and Johnson 2017) and "how different stakeholders conceive IA expansions" (cf. Erasmus and Coetzee 2018; Roussy and Brivot 2016) created a fertile ground to understand the manifold viewpoints on the IA expansion to assure on risk culture. Consequently, our investigation focused on analyzing (1) how different actors—regulators, normalizers, consultants, and implementers—conceive the IA of risk culture and (2) what type of approaches they embrace to audit risk culture.

Given the contextual ambiguities and contemporary nature of different stakeholders' approaches to the IA of risk culture (Palermo et al. 2016; Ring et al. 2016), we conducted a qualitative field study involving different stakeholders to explore their emergent ideas inductively (Power and Gendron 2015). Following Roussy and Brivot (2016), the inductive examination involved analysis of 20 interviews and 295 documents on the IA of risk culture by the four actor groups (regulators, normalizers, consultants, and implementers).

Our findings indicate that regulators and implementers promoted the control of risk culture based on "regular" IA activities. The regulators restricted themselves to high-level guidelines and promoted the IA of risk culture as a new check and balance to mitigate what they observed as widespread cultural problems within banks. The implementers were reluctant in implementing any new "costly" changes to their IA activities in what they claimed were strategy and business model matters and thus included some elements of verification in their existing IA activities. Consultants and normalizers, in contrast, promoted a cautious approach to risk culture "control" by IA along with empowerment of employees through training. Motivated to keep their thought leadership, the normalizers reconciled efforts from the regulators and the consultants to promote a library of toolkits and a bricolage of ideas to guide implementing organizations. The consultants utilized this as an opportunity to monetize new "value-adding" solutions by promoting "comprehensive" control frameworks (including IA) and widespread employee empowerment. Our results on the heterogeneity of viewpoints among different stakeholders may seem unsurprising given the ambiguity of the object of IA (risk culture

in our case) and variations in the current IA practices. However, our results posit three important implications.

First, the absence of implementers' support or coercive regulation on changing the conventional notions and techniques raises doubt on whether IA would be able to successfully transition from its current paradigm of assuring tangible processes to the paradigm of assuring intangibles, such as risk culture and ethical values. There is a danger that a direct transfer of knowledge, without critical considerations on the intangibility of risk culture, could lead to mere ritualistic thinking among implementers promoting a tick-box-based verification approach rendering IA of risk culture inefficient or ineffective (Erasmus and Coetzee 2018; McCabe 2014; Power 1999). Second, the control and governance approach, if extended to employees' behavior, raises ethical concerns where excessive controls might rob employees of their individuality and dissociate them from critical and moral decision-making (leading to the colonization of employees' emotional self) (Ezzy 2001; McCabe 2014). Third, approaches from normalizers and consultants to the implementation of IA as a control mechanism balanced by the empowerment of employees through training seems theoretically plausible but pragmatically challenging to attain (McCabe 2014; Simons 1995). In practice, while empowered employees might use their entrepreneurial flair to contribute to value creation using their innovative/critical ideas, they might be difficult to control and could harm organizational well-being (Simons 1995).

The rest of the paper is structured as follows: "IA Expansions to New Domains" problematizes the IA literature; "Research Approach" addresses the methodology; "Results" presents the findings; "Discussion" and "Conclusion" present discussion and conclusions, respectively.

## IA Expansions to New Domains

Waves of corporate and banking scandals in the last three decades have punctured trust in firms' behavior (Neu et al. 2013; Parker and Johnson 2017) and explicated employees' dissociation from the moral and ethical compass (Arel et al. 2012; MacLean et al. 2015). The trust-deficit in corporations, coupled with a societal trust-deficit (Power 1997), has spurred regulatory demands for tighter control (Baud and Chiapello 2016; Chambers 2014; Collier and Zaman 2005). As a result, ethics and risk culture have been included in the ambit of IA (Palermo et al. 2016; Ring et al. 2016). However, the inclusion of risk culture poses several paradigmatic challenges to the IA expansions. The most prominent being the non-tangible and unbounded nature of risk culture compared to existing IA applications to tangible processes (check introduction, paragraph 2 for details).

Consequently, to understand the paradigmatic challenges of IA expansions to risk culture, we inductively examined (1) how different actors—regulators, normalizers, consultants, and implementers—conceive the IA of risk culture and (2) what type of approaches they embrace to this aim. We informed our inductive investigation of the IA of risk culture by categorizing the extant literature on the expansion of IA into three distinct approaches and distilling knowledge from them.

The first approach, focusing on what internal auditors do (Roussy 2015), revealed problems with normative and ethical expectations of IA as an independent and objective assurance and consultancy provider (Christopher et al. 2009). Commentators in this stream blamed the non-objectivity and non-independence of internal auditors on their role conflicts (Morgan 1980) and inter-role conflict in negotiations (Cohen et al. 2002; Roussy 2015; Roussy and Brivot 2016). For example, Roussy (2013) and Roussy and Rodrigue (2016) find that internal auditors team up with the auditee managers instead of with the audit committees and the boards. This siding with the auditee managers makes it comfortable for internal auditors in accessing data and information from the auditees (Fanning and David Piercey 2014; Goodwin and Yeo 2001). Norman et al. (2010) demonstrate that internal auditors *perceive more personal threats when they report high levels of risk directly to the audit committee* and thus mild down the reporting of high-level risks. Teaming up with auditee managers or threat perception results in comfort provision by internal auditors to the control committees and the board of organizations in their reporting (Sarens et al. 2009). While these studies teach us to understand IA practices by examining what internal auditors do and how they carry out their work, they only tell a one-sided story of IA work.

In contrast to the first approach, the second approach investigates varying goals, configuration, competence, ethics, and techniques of IA in different contexts, especially risk management (Arena et al. 2010, 2017; Castanheira et al. 2009; de Zwaan et al. 2011; Vinnari and Skærbæk 2014) and corporate governance (Arena and Jeppesen 2015; Roussy and Rodrigue 2016). For example, Sarens and Lamboglia (2014) suggest varying competence and knowledge requirements for internal auditors in different domains. In this regard, some scholars suggest the rotation of employees to enrichen the knowledge of internal auditors (Burton et al. 2015; Christ et al. 2015). While rotation might improve the quality of reporting (Christ et al. 2015), it could discourage employees and newcomers from joining IA teams by pointing to the general nature of the IA work (Bartlett et al. 2016). In a similar vein, studies exploring outsourcing of IA to third parties suggest that outsourcing improves the independence and objectivity of IA, but discourages auditee managers from sharing information, resulting in lower audit quality (Abdolmohammadi 2013; Caplan et al.

2000; Prawitt et al. 2012; Spekél et al. 2007). Overall, these studies reveal that due to lack of content knowledge on the heterogeneity of processes (including risk management, corporate governance, and internal control), IA has developed its techniques to merely verify the process of decision-making (Pentland 2000; Power 1999). While these studies teach us to look at rationales and approaches of IA, they ignore the interactions and expectations of different stakeholders on IA rationales and approaches.

The third approach explains IA by studying involvement and expectations of different stakeholders (Erasmus and Coetzee 2018; Roussy and Brivot 2016). Studying differing expectations of the major stakeholders and their influence on IA becomes essential considering the influence of a variety of stakeholders on IA practices (Arena and Jeppesen 2009; Covaleski et al. 2003), as repeatedly shown through its historical development (Hayne and Free 2014; Parker and Johnson 2017; Spira and Page 2003). Scholars promoting this approach study influence of the auditee managers (Sarens and De Beelde 2006), external auditors (Brody et al. 1998; Felix et al. 2001; Mat Zain et al. 2015), audit committees (Goodwin 2003), and regulators (Chambers 2014) in making IA indispensable. Furthermore, this emerging stream of research explores “interaction,” “influence,” “power asymmetry,” and “control” along with typical contract-based relationships to explain IA practices (Mihret 2014), e.g., oversight or closeness of audit committees to IA functions has been shown to enhance the independence of IA functions (Abbott et al. 2010). Goodwin (2003) goes a step further and demonstrates that the accounting experience of audit committee members enables them to assess the work of internal auditors, thereby promoting the independence of the IA function. Sarens and De Beelde (2006) show how the expectations of senior managers from IA on monitoring risk management, internal control, and corporate culture positively influence their work. Some studies within this approach cover historical contingencies and different rationales of IA expansions (Chambers and Odar 2015; Parker and Johnson 2017; Spira and Page 2003). This stream teaches us to identify key stakeholders and include their views in understanding IA expansions. However, like the other two approaches, the questioning has been limited to exploring IA as a control and governance mechanism (Mihret 2014) or an independence and objective function (Christopher et al. 2009; Stewart and Subramaniam 2010) within the purview of its application to processes.

## Research Approach

### Research Strategy

We conducted a qualitative, explorative field study to inductively examine the different stakeholders’ approaches to

**Table 1** Interviews

No.	Organization	Informant
<b>Implementers</b>		
1	Interest organization-1	Chief analyst, risk and audit
2	Interest organization-1	Chief jurist, risk and compliance
3	Interest organization-2	Senior legal advisor, risk and compliance
4	Large bank-1	Audit and compliance head
5	Large bank-1	Risk head
6	Large bank-2	Internal auditor
7	Large bank-2	Internal auditor
8	Large bank-2	Chief credit risk officer
9	Large bank-3	Internal auditor
10	Large bank-3	Internal auditor
<b>Consultants</b>		
11	Big-4	Partner, financial services (risk and compliance)
12	Big-4	Director, IFRS services
13	Big-4	Director, financial services (risk and compliance)
14	Big-4	Manager, risk and IA services
15	Protiviti	Director, financial services (internal audit)
16	Protiviti	Manager, financial services (internal audit)
<b>Regulators</b>		
17	BCBS	Member secretariat
18	FSB	Member secretariat
<b>Normalizers</b>		
19	IIA	Technical manager, Italy
20	IIA	Global director, financial services audit

the IA of risk culture (Power and Gendron 2015; Roussy and Rodrigue 2016). In doing so, we adopted a social constructivist approach, accepting that knowledge resides in a group of actors who share a practice or a set of problems (Berger and Luckmann 1966; Wahlström 2009). The inductive approach informed the theoretically understudied IA expansion approaches with insights from the new empirical context of the IA of risk culture (Gioia et al. 2013; Power and Gendron 2015).

## Data Collection

We focused on the European context by relying on two data sources—interviews and documents on the IA of risk culture by the four actors (i.e., regulators, normalizers, consultants, and implementers).

## Semi-structured Interviews

Twenty semi-structured and explorative interviews, lasting from 30 to 120 min, with key informants were conducted (see Table 1). The informants from the regulators, normalizers, and consulting organizations were selected to discuss their ideas on the IA of risk culture and collect information and documents authored/promoted by them on the IA of

risk culture. The informants from the implementers such as risk managers, internal auditors, and members of the interest organizations were selected opportunistically, as we had access to these informants through our prior engagements with them. The interviews focused on understanding the conceptions of the IA of risk culture, its linkages to other control systems, and broad IA techniques. Informants were asked to freely draw from their experience with control systems within organizations, such as internal control, risk management, and corporate governance on the IA of risk culture.

## Documents

Overall, 295 documents<sup>1</sup> detailing the views of the four actors (i.e., regulators, normalizers, consultants, and implementers) concerning IA of risk culture were selected. Hundred-and-eighty-five of these documents belonged to the regulators—the Financial Stability Board (FSB), the Basel Committee on Banking Supervision (BCBS), and the European Banking Authority (EBA). These

<sup>1</sup> Private documents provided by the informants are marked in the relevant tables.

**Table 2** Documents from regulators

Actors	No. of documents	Comments
BCBS	52	(Standards and guideline: 11, news: 3, lobbying responses to standards and guidelines: 38 <sup>a</sup> )
FSB	73	(Standards and guideline: 5, news: 4, lobbying responses to standards and guidelines: 60 <sup>b</sup> , reports: 4)
EBA	60	(Standards and guideline: 5, news and other: 55)
Total	185	

<sup>a</sup>38 Lobbying responses on 2011 consultation on internal audit function (regulators: 1, normalizers: 8, banks: 8, interest organizations: 15, consultants: 6)

<sup>b</sup>32 Lobbying responses on risk appetite consultation in 2013 (regulators: 0, normalizers: 3, banks: 1, interest organizations: 22, consultants: 6); 28 Lobbying responses on risk culture consultation in 2013 (regulators: 4, normalizers: 3, banks: 3, interest organizations: 13, consultants: 5)

documents comprise standards, guidelines, and the lobbying responses (from other regulators, normalizers, consultants, and implementers) on IA, risk culture, risk appetite, risk governance, and corporate governance (see Table 2 for details).

Another 47 documents from the Institute of Internal Auditors (IIA), the Committee of Sponsoring Organizations of the Treadway Commission (COSO), and the Institute of Risk Management (IRM) were collected to understand the perspectives of the normalizers (see Table 3 for details).

Additionally, 58 documents issued after the financial crisis by the big four consulting firms (PWC, E&Y, Deloitte, KPMG) and Protiviti<sup>2</sup> on risk culture including IA approaches were analyzed. We also collected 5 documents from the implementers for the analysis (see Table 4 for details).

### Data Analysis

Following guidelines of naturalistic inquiry (Lincoln and Guba 1985) and constant comparison techniques (Corbin and Strauss 1990), we continuously analyzed the data during collection. This continuous analysis proved useful in assessing areas that needed more data points. Our analysis included several steps. First, relevant data points were selected and analyzed separately for the four actors: regulators, normalizers, consultants, and implementers. Second, key historical events were identified. Third, open in vivo coding of the empirical data, using simple text codes in the

<sup>2</sup> Protiviti was included because the IIA and the IRM indicated their collaboration with Protiviti on the issue. Protiviti also consists of the remnants of the IA business of the previous large firm Arthur Andersen.

**Table 3** Documents on Normalizers

Actors	No. of documents	Comments
IIA	21	14 public (reports: 8, survey:1, webpages:3, standards:2) and 7 private (reports: 4, surveys: 2, workshop power point:1)
IRM	6	3 public reports, 3 public web pages
COSO	20	17 public reports, 2 public web pages, 1 public power point
Total	47	

**Table 4** Documents on Consultants and Implementers

Actors	No. of documents	Comments
<b>Consultants</b>		
Deloitte	17	(16 public reports; 1 privately shared)
E&Y	12	(10 public reports; 2 privately shared by the IIA)
KPMG	16	(16 public reports)
Protiviti	3	(2 public reports, 1 privately shared)
PwC	10	(9 public reports, 1 privately shared)
Total	58	(53 publicly available and 5 privately shared)
<b>Implementers</b>		
	5	(3 public; 2 private – 1 shared by the IIA and 1 by the implementer)

language of the informants, was performed. Fourth, axial coding allowed the grouping of different in vivo empirical codes into second-order theoretical themes (Corbin and Strauss 1990; Gioia et al. 2013). Finally, the relationship between the emergent second-order themes connected the empirical data to our emergent theoretical framework.

### Theoretical Constructs

The approach of identifying theoretical constructs in an inductive rather than a deductive manner was inspired by Gioia et al. (2013). Gioia et al. (2013) suggest focusing on the language of informants while investigating new empirical phenomena (in our case the IA of “non-tangible” risk culture) that differ paradigmatically from existing phenomena (in our case the IA of any tangible process—risk management or corporate governance). Gioia et al. (2013) argue that ignoring the language of informants and focusing on an *a priori* theoretical construct in such cases could result in a confirmation bias towards existing theoretical understanding and missed opportunity on construct refinement and theory building through new empirical paradigms. The table below

**Table 5** Constructs

Empirical language	Theoretical meaning	Theoretical construct
Making the object of audit visible and auditable		
What is included	Demarcation of things inside or outside (A. Abbott 1995; Bowker and Star 1996)	Boundaries
What is not included		
Areas of concern	Qualitative assessment (Callon and Law 2005; Callon and Muniesa 2005; Cochoy 2008)	Calculation
Index and metrics		
Quantitative data: recorded and calculated metrics	Concrete tasks and routines which allow IA to collect information (Power 1999)	Techniques
Qualitative field study: interview, survey, questionnaire		
Documental evidence: steering, management system and process document		
Broad goals of IA		
Objective, purpose, or aim of IA of risk culture either spoken or found in documents	Rationale (Power 1999)	Broad goals

details the ways we formulated the two theoretical constructs inductively (Table 5).

The first theoretical construct that we identified concerned visibility and auditability scheme of the object of audit. It comprised three sub-constructs: boundary identification, calculation, and adaptation of the techniques of the IA. Boundary identification was the first step towards making the object of audit visible. The boundary identification was mostly linked to understanding what to include and what to exclude (Abbott 1995; Bowker and Star 1996; Mikes 2009). Here, more specifically, we found the idea of “demarcating the object of audit” (Power 1997, 1999). The second step that emerged was calculation linked to the aspiration of rendering “organizational spaces knowable and governable” (Miller and O’Leary 1987; Miller and Power 2013; Vaivio 1999, 2006). Here, we found the use of both quantitative measures (calculations) (Mikes 2011; Power 2004) and qualitative areas of assessment (qualculations) (Callon and Law 2005; Callon and Muniesa 2005; Cochoy 2008). Third, we found techniques of IA aimed at collecting data for calculations/qualculations (Power 1999). In this study, we limited our focus to broad techniques used in collecting the information about the object of audit. Consequently, we mainly focused on field techniques of interviews, surveys, questionnaires, and internal company data sources on processes and steering documents informing opinions on behavior and risk calculations. To keep the findings of this study comprehensible, we excluded data collection and theorization on auditor judgment techniques.

In the process of theorizing on making the object of audit visible and auditable, we also found that the visibility and auditability schemes were tied to another theoretical construct that we name as broad goals (Power 1999) and mostly represented a ‘style of thinking’ (Dean 1999; Foucault

1988a; Miller and Rose 2008; Rose and Miller 1992). This style of thinking was either explicated by the informants or mentioned in the documents. We found different broad goals among different actors (Dean 1999, pp. 17, 40).

### Trustworthiness of Data and Analysis

We followed several tactics to enhance the trustworthiness of our data collection (Gioia et al. 2013). First, guaranteed anonymity allowed informants to speak their minds and present their viewpoints freely. Second, semi-structured interviews reduced the interviewer bias by limiting interviewer interference. Third, paraphrasing and confirming our interpretations and claims with the interviewees during the interviews reduced interviewer bias. Fourth, talking about recent events, helped counter the recall biases in the interviewees’ accounts.

We also followed several steps to ensure trustworthiness of our data analysis. First, use of a computer program rendered transparency, traceability, and replicability to our analysis. Second, triangulation of information and fact checking during data analysis imparted credibility and validity to the constructs. Third, historical analysis allowed for a better grasp of the contextual factors, enhancing the quality of theorization. Fourth, input from the scholars in accounting and management conferences enhanced the rigor of our results and analysis. Finally, the exposure of our process on the relationship between the empirical material and theoretical constructs in the previous sections imparts additional transparency and trustworthiness.

## Results

### Regulators: Framing Self-Control, Blaming Practices

The European Union (EU) has a multilevel regulatory environment: national, European, and international. While the national regulators (central banks, supervisory authorities or both) drive national standards/policies, the national parliaments legalize national regulations/laws. On the European level, the European Banking Authority (EBA) (a European-level supervisory authority of banks) influences standards/policies; the European Parliament, the European Commission and the Council of Ministers drive the actual laws and regulations (including directives) binding member states. The European-level standards/policies, in turn, are affected by international regulators, most notably the Basel Committee on Banking Supervision (BCBS) and the Financial Stability Board (FSB) (Baud and Chiapello 2016; Palermo et al. 2016). Here, we restrict our analysis to the views of the three regulators, the FSB, the BCBS, and the EBA, as these regulators have shown recent interest in the IA of risk culture. The idea of the IA of risk culture among regulators is tied to two concerns: culture as a factor of financial crises and the need to address cultural problems by detailing additional guidelines on self-control.

Culture at financial institutions was one of the highlighted factors identified as an important factor contributing to the financial crisis (Informant 18)

IA is there to bridge the asymmetry of information between the principle and the agent. [...] That already has been an issue [with IA] in some banks. The independence of IA was not sufficient [during the crisis]. (Informant 17)

At FSB, the discussion on culture started with concern about the governance of *risk management culture* and originated in an October 2011 progress-report of the FSB to the G20. The progress report identified risk governance as critical to ensuring a strong risk management culture. Strengthening of the risk governance was advocated by identifying a well-defined risk appetite framework and having strong chief risk officers (CRO), chief executive officer (CEO), and audit committee (a top-down approach). The discussion was boosted further in April 2012, when the FSB sought opinions from different national supervisors during its thematic review on risk governance. The paper and consultation documents on the thematic review of risk governance mainly linked IA to a *risk control framework* without offering details on control or IA approaches of risk management culture.

The discussion at the FSB on the governance of *risk management culture* later changed to the governance of

*risk culture* in November 2012, when the FSB progress-report to the G20 promoted a more detailed understanding on the governance of risk culture. The document identified strong risk culture as an essential element of good governance. The document recommended supervisors to *explicitly assess risk culture at firms*. Several qualitative areas for the assessment of good risk culture such as, “tone from the top,” “monitoring by senior managers and board,” “appropriate risk appetite definition and implementation,” “remuneration practices,” and “escalation practices and policies” were propounded. The link of culture to the strategy and business model of banks and the strong top-down approach through a strong board, CEO, and CRO were further promoted. In this document, IA is posited as a control function and the third line of defense that in tandem with risk management and compliance is considered crucial for risk culture control. IA’s *sufficient authority, stature, independence, resources, and access to the Board* are posited as crucial for its usefulness in control of risk culture. This document recognizes the problem with the IA function in banks: *The financial crisis, and more importantly recent events, demonstrates that internal audit functions should be empowered to constitute an effective third line of defense.*

Concrete quantitative indicators such as “number of audit findings not being closed,” “number of risk limits breached and their cause,” “the manner in which problems identified in IA reports are addressed,” “the preexisting awareness of the problems by the board,” and “employee survey results” were promoted as reliable indicators for indirect monitoring and control of culture. The document also related risk culture to operational risk management culture.

Risk culture is also related to operational risk in part because operational risk includes people risk: (i) inadequate training; (ii) insufficient personnel needed to perform required tasks adequately; (iii) dependency on a limited number of qualified persons (e.g., key person dependency); (iv) misalignment of business objectives and compensation programs; and (v) inadequate mindset of control teams.

It was not until February 2013, when the thematic review on risk governance was finalized that a clear line of thought linking risk culture control to risk governance appeared. The board, top management, and control systems (risk management, IA, compliance, and corporate governance) and failure of banks during the financial crisis motivated this document.

The idea of firms controlling risk culture took root through the efforts of the FSB when, after several round tables with the industry experts (informant 18), the FSB published a consultation document on controlling risk

culture in 2013. This document catapulted the FSB as the opinion builder among the regulators.

In its contemporary debates, the FSB acknowledges the non-measurability and intangibility of risk culture. On the issue of the calculability of risk culture, the informant 18 bluntly said, *We do not measure risk culture. You should talk to firms – culture is very firm driven. We issue guidance to help authorities assess risk culture.* The non-measurability of risk culture was translated into propounding qualitative assessment areas: tone from the top, accountability of employees, effective communication from the board, and incentive check in organizations.

It is hard to quantify [culture] right. Therefore, what we are saying is to look into the culture and conduct related aspect in risk appetite framework, assessment, and incentive plans. And to look at what the tone at the top is? (Informant 18)

Although informant 18 refrained from the quantitative reductionism of culture, upon further queries on what quantitative indicators could be suitable, the informant suggested, *No. of complaints to the managers, response of managers to the complaints. Customer feedback and things like that. These indicators could give a gauge on culture in a more quantitative way.* The avoidance of the quantitative reduction of risk culture was promoted on two grounds: (a) the policy-driven mandate of the FSB

We are at the ten thousand [feet] level. We issue the guidance and how it is implemented varies across the jurisdictions. [...] The work we are doing is very policy driven. (Informant 18)

And (b) the non-intervention in banking business models

We are not in the business of getting involved with banks' business model and trying to shape them. We recognize that this has to be driven by management (Informant 18)

Although direct involvement of the FSB on IA matters of risk culture was not highlighted, the broad goal for the IA of risk culture indicated IA as a control and governance mechanism.

I do not know if FSB will go into too many details on internal audit. But I mean there will be a useful role of control for internal audit in this space. [...] However, the Guidelines on culture and toolkits [including IA] to assess them are very important for aligning the behavior of the employees (Informant 18)

The FSB informant (18) also highlighted the currently undergoing projects to look deeper into *the misconduct issues, scientific view on culture*, and proposal of a *toolkit* to assess culture. Informant 18 further stated, *the next*

*phase of culture work will begin next year (referring to 2018) and hesitantly disclosed we will not only look at risk culture but overall culture.* On what kind of assessment tools will be included, informant 18 suggested that there will be *no direct way to the measurement on culture* but emphasized qualitative areas of assessment on *non-financial incentives and escalation policy.*

In contrast to the risk appetite and risk governance led context of the FSB, the IA of risk culture at the BCBS evolved from discussions of internal control, IA, and corporate governance. The first standalone internal control guideline of 1998 by the BCBS recognized boards' importance in creating a control culture to curb excessive risk-taking. The high-level guidelines of the BCBS on IA (consultation in 2011 and finalization in 2012) did not even mention risk culture or culture once.

The first standalone corporate governance guideline by the BCBS in 1999 only mentioned "culture" to caution banks' board to draft their compensation and remuneration policies in accordance with the culture. This rhetoric continued in the consultations and guidelines on corporate governance proposed by the BCBS until 2010. The new high-level guidelines on corporate governance (consultation in 2014 and finalization in 2015) by the BCBS mentioned for the first time the risk culture concept and its audit and control.

One of the primary objectives of this revision is to explicitly reinforce the collective oversight and risk governance responsibilities of the board. Another important objective is to emphasize key components of risk governance such as risk culture, risk appetite and their relationship to a bank's risk capacity. (Corporate governance final document 2015, page 4)

This document referred to the FSB documents, which had started appearing in parallel. Our informant suggested that the corporate governance of the BCBS was profoundly influenced by the risk governance framework of the FSB.

Our [many] recommendations on the risk governance framework has been embedded in the Basel Committee corporate-governance framework. (Informant 18)

As exemplified in the quotes below, the BCBS also linked the culture audit to the secondary system of risk governance and risk appetite and promoted audit as an independent internal control mechanism whose primary aim was to monitor and control the issues:

The third line of defense consists of an independent and effective IA function. Among other things, it provides independent review and assurance on the quality and effectiveness of the bank's risk governance framework including links to organizational culture, as well

as strategic and business planning, compensation and decision-making processes. Internal auditors must be competent and appropriately trained and not involved in developing, implementing or operating the risk management function. (Corporate governance consultation document 2014, page 10; Corporate governance final document 2015, page 11)

This was emphasized by the BCBS informant (17) when he linked IA to the “culture of control” discussion: *IA is before all internal. And the competence of internal auditors is to understand the controls and then you also need the bank to understand the controls and the existence of a culture of control.* On risk culture audit, informant 17 suggested that it should include the entire universe of a bank: *In addition, as we know, the scope of internal audit that is the audit universe is all the units in a bank. Therefore, nothing should be left unaudited [concerning risk culture] ranging from trading desk to the compliance department to the risk management function, procurement, HR including payrolls—you name it.* The informant also suggested looking at the psychological and organizational aspects to assess culture:

You also want to take into account some other aspects. [...] the psychology of the different actors and behavioral science and organizational aspects (Informant 17)

However, on quantification, the BCBS informant raised a word of caution by saying,

I think it would be dangerous in such a field [referring to risk culture] with internal audit, internal control, corporate governance to limit to view through quantitative analysis (Informant 17)

In the European context, the EBA’s predecessor—the Committee of European Banking Supervisors—issued consultation paper CP24<sup>3</sup> (in July 2009 and finalized as CP25 in 2010) focusing on the “High-level principles for risk management” and included the control of risk culture. These documents loosely coupled risk culture with risk governance and communication issues.

Institutions must implement a consistent risk culture and establish sound risk governance supported by an appropriate communication policy (CP 24, page 3; CP 25, page 3)

The IA of risk culture approach was further refined in detail in the governance frameworks of CP44 and GL44 in October 2010 and September 2011, respectively, by pushing IA as a control function. Moving from the traditional broad

principles on IA, in 2016, the EBA followed the FSB and tightly linked the IA of risk culture with the risk appetite and risk governance type secondary systems in its new consultation on governance. Here, again IA is conceived as a control mechanism that monitors deviations through metrics.

In particular, the institution should ensure that qualification of the IA function and its resources, in particular the monitoring tools and risk analysis methods, are in adequacy with its size, locations and the nature, scale and complexity of the risks associated with the institution’s model and business activities and risk culture and risk appetite. (EBA/CP/2016/16, Page 49)

### Normalizers: Balancing Control and Empowerment with Assemblages of Ideas and Toolkits

To understand the normalizers’ viewpoints on the IA of risk culture, we focused on the three normalizers: the Institute of Internal Auditors (IIA), the Committee of Sponsoring Organizations of the Treadway Commission (COSO), and the Institute of Risk Management (IRM). The reason behind the selection of these normalizers was twofold: first, their strong presence and influence and second, their recent interest in the IA of risk culture to keep their “thought leadership.”

The IIA approaches on the IA of risk culture focus on risk appetite as the first system for identifying how to audit risk culture:

First thing to look at is to make sure that financial services firms have a risk appetite framework on how much risk are they going to expose their capital to, which actually is other people’s money. (Informant 20)

However, in so doing, the IIA warns against applying the traditional models of IA as a control mechanism to guide the conduct of employees.

There are many models that look at the components of organizational culture. It is, however, dangerous to reduce work on culture and behavior into one set of indicators based on a particular model. There is no one-size-fits-all solution to auditing culture as organizations can be very different, even if they are producing the same or similar outputs.” Chief Executive of Chartered Institute of Internal Auditors, UK (Chartered Institute of Internal Auditors 2014)

The IIA also identified challenges with techniques of IA applied to risk culture, namely, the inadequacy of surveys and interviews in gathering evidence and the requirement of judgment as a subjective element on the part of the auditors.

I think with the soft aspects; you should aim to get a lot of answers. In this, survey and questionnaires can support you if you define these instruments in a simi-

<sup>3</sup> This consultation was mandated by the G-20 leaders’ declaration of 15 November 2008.

lar way. Thus, these instruments reduce the collection bias. Whereas interviews have collection biases that you ask different interviewees differently and are difficult to scale. (Informant 19)

You cannot rely merely on data and examination of documents. The soft aspects highlighted from interviews and surveys along with judgment by the auditor plays an important role in the effective assessment of risk culture (Informant 19)

Remedies by embedding risk culture in all audits were suggested. Informant 20 suggested, *There is a choice to be made on whether to carry out IA of risk culture separately or not. The risk culture survey and interview responses could be biased if conducted separately since people can twist behavioral and cultural survey and interview responses purposefully. However, if risk culture audit is embedded in every audit, you could remove some of these biases.*

Although the IIA approaches were cautionary, they did not provide concrete examples of how to be cautious. The risk culture manual shared by the IIA did not suggest any specific behavioral approach until organizations become mature and simply enumerated the FSB's indicators. Here, the informants and the documents suggested that IA should assume a consulting role in organizations starting risk culture implementations but an assurance role in organizations with growing maturity of implementations. Furthermore, apart from the traditional approaches of IA as a control mechanism, the IIA suggested the self-guidance of conduct by empowered employees.

We want to make sure that the first line of defense that is the managers and operational employees in the line are proactively evaluating all types of risk that they are exposed to. (Informant 20)

To foster employee self-guidance, the IIA promoted training and self-assessment on root cause analysis, cultural dissemination, and ethics (Chartered Institute of Internal Auditors 2014). Informant 20 further added, *We also encourage internal auditors to ask the question why do you think this problem happens? We do this so that they can get to the root cause when it comes to actual audit.* The IIA also promoted collaboration with compliance functions by using its report and verification as an additional cushion of control:

I do think that other areas could help with the risk culture. Compliance being the second line could help since risk culture is so much embedded in so many of the regulatory requirements. [...] IA could rely on the compliance function and its report. [...] While talking about using compliance report, we always promote internal auditors to ascertain the veracity of those reports. (Informant 20)

Furthermore, on compensation-related issues, the IIA promoted the involvement of human resource functions:

As part of a culture audit, IA could collaborate with the human resources in understanding the compensation and employee welfare and other aspects by introducing a few questions to the human resource surveys, which are already conducted within organizations. (Informant 20)

In summary, the IIA promoted both enhancements of IA as a control mechanism by utilizing behavioral indicators as well as training to empower employees in controlling their conduct. Inadequate skills of current internal auditors, problems with reporting integrity, and IA as a part of the risk culture itself were highlighted as problems with the risk culture audit approach (Chartered Institute of Internal Auditors 2014). Ethics were consequently highly promoted in the IIA general training programs:

We have not identified any specific training regarding business ethics and risk culture. We do talk about ethics in our beginner and advanced training and certification modules. (Informant 19)

The IIA informants' interviews and documents reveal their reliance on the COSO framework. Consequently, we also examined evolution of the risk culture concept in the COSO publications. The risk culture debate in the COSO framework is linked to the "control environment" element of their internal control framework of 1992. The framework of 1992 does not use culture as an explicit term but refers to five broad principles that cover aspects of risk culture indirectly.

[...] I would point back to the concept of control environment in the internal control framework of COSO [of 1992]. The internal control framework is old, but the risk culture term has gained popularity after the financial crisis of 2008. Within the five principles of the control environment of the COSO framework, we cover broadly the risk culture without using the term explicitly: commitment to integrity and ethical values, independence of the board of directors, transparent reporting lines, recruitment and nurturing employees to meet control environment objectives, accountability of individuals. (Informant 20)

Our analysis further indicates that the COSO internal control framework of 1992, its update in 2013, and subsequent clarification (e.g., the three lines of defense and regulations in 2015) continue the indirect discussion on risk culture by referring to the setting, evaluating, and monitoring of the appropriate level of risks (risk appetite) at the firm policy level. In line with the internal

control framework of 1992, the Enterprise Risk Management (ERM) framework of 2004 also supports risk appetite setting, evaluation, and monitoring. Starting in 2009, the COSO publications include a direct reference to risk culture in the discussions on policy setting and board oversight. A need for a *risk-aware culture* is promoted, citing the embeddedness of the risk management system in the organizational culture. Informant 20 ascribed this shift to the strong emergence of the risk culture discussion in regulatory circles. By 2010, risk oversight became embedded with qualitative indicators of assessment and monitoring culture, incentive, and tone of the top management on risk appetite and culture. From 2011 onwards, the ideas on organizational culture affecting key risk indicators (KRIs) and senior managers setting and disseminating policy on risk culture started emerging as part of risk appetite discussions. By 2012, the awareness of culture among employees as well as measuring and monitoring through workshops and surveys appeared as an important discussion of embracing risk management. All these efforts on risk oversight, KRIs, and risk appetite culminated in the 2017 COSO ERM framework linking enterprise risk management to culture and reinforcing the role of senior managers and boards in setting, disseminating, and monitoring culture.

In line with the COSO and the IIA development, the IRM's understanding on culture also emerges in their risk appetite framework of 2011 where advice on designing risk appetite (appropriate level of risk-taking) considering "risk management culture" and "control culture" of the organizations is propounded. Here, risk appetite is linked to the corporate governance (guidance and control from the board). Furthermore, in line with the IIA, the IRM directly proposed a behavioral approach to risk in 2012:

What is missing is the behavioral element: why do individuals, groups and organizations behave the way they do, and how does this affect all aspects of the management of risk? (IRM risk management framework, 2012)

This behavioral approach to risk was rendered concrete by indicating the use of personality tools to measure individuals' attitudes as indicators of risk culture.

It is possible to measure predisposition to risk by use of personality assessment tools. Their basic rationale is that, with regard to risk-taking, people vary enormously. (IRM risk management framework, 2012)

The IRM did not propound a direct approach to the IA of risk culture but noted that a mere culture of control would be unable to encourage employees to behave appropriately, and it thus promoted personality assessment to help empower employees to make appropriate decisions:

Taxi drivers and airline pilots are routinely given personality tests to determine how effectively they can exhibit self-control under stress – we should be ready to look at other key staff, managers and board members in the same way. (IRM risk management framework, 2012)

Furthermore, while promoting the control of risk culture, the IRM proposed verifying not only the "tone at the top" but also the "tone at the bottom" and "at the individual level." Although the IRM emphasized "well-engineered" culture, it was not restricted to the idea that dysfunctionality or deviation from norms results in problems within organizations. The IRM recognized risk culture as a complex issue and emphasized that too tight control of behavior could also fail within organizations.

### Consultants: Comprehensive Control, Employee Empowerment

Our analysis suggests that the consultants identified the issue of risk culture in the last decade and promoted a variety of branded approaches, e.g., Deloitte's intelligent risk culture model, E&Y's behavioral model, and KPMG's and PwC's risk culture models. Most of these approaches recognized risk appetite and governance as crucial for risk culture control and typically proposed a comprehensive control framework, promoting the involvement of the entire organization.

It is about [all] people and how do they manage risks. It is not only about spreadsheets, modeling, and mathematical issues." (Informant 14)

A robust and pervasive risk culture throughout the firm is essential. This risk culture should be embedded in the way the firm operates and should cover all areas and activities, with particular care not to limit risk management to specific business areas or to have it operate only as an audit or control function." (Deloitte 2015)

This comprehensive control framework relied on self-assessment, tracking tools, risk controls, and various indicators.

What we have done in these cases are tracking, having risk controls, a report regarding different indicators and propose self-assessment from board level and so on." (Informant 13)

The proposed control frameworks were fluid, and their implementation allowed accommodating the bank's internal worldviews as well as that of regulations.

If you then take a step back and think about the different banks, they all have their own sort of ideal of what

the world looks like and that explains how they build up their internal control structure, how they build up their accounting framework and their own interpretation of what the original regulations meant and they are trying to reconcile it with a new set of regulations.” (Informant 12)

Although consultants suggested flexible approaches involving all employees, they consented that it is easier to get boards’ attention than that of the line managers.

It is not hard to get attention from the board level. But it is tougher to get attention from the line manager level. Because line managers, they have many things to manage.” (Informant 13)

This apathy from the line managers was blamed on the lack of a process view that permeates banking organizations.

There is a lack of process view. Big banks have been too much concerned about money here money there. They fail to have the process view.” (Informant 13)

Furthermore, consultants suggested that boards worry about having a “grip on the culture related things” and are keen to have “measures and risk indicators that can help evaluate, control and mitigate risks.” along with, “incentives” and “education” to align the employees to the broader vision (Informant 13).

To make line managers and employees aware of and accountable for their responsibilities, consultants suggested empowering them through training and self-assessment tests. Consultants rationalized training and self-assessment by arguing that employees make many decisions in organizations, and educated employees contribute to better risk culture through their independent behaviors on risk-related choices:

The institution provides and requires core training, professional development and assessment to ensure the bounds of acceptable and unacceptable behavior are understood. (E&Y 2014)

Employees have the skills necessary to complete what is asked of them, and feel comfortable to ask questions or pose challenge (KPMG 2016)

But without training, there is no basis for critical thinking and judgment around risk decision-making (KPMG 2014)

Regarding assessment of culture, the consultants proposed assessing tools on the individual level that measured *identity, belonging and behavior* (Informant 14). In fact, the consultants agreed that most of the metrics of culture were old and were linked to the application of *cultural tools* involving *organizational psychology* to measure

the *people dimension* of risks and *alignment of culture* endeavors (Informant 14).

At PwC, our approach is to reach below the surface of the traditional internal audit to shed some light on the culture and behaviors that underpin effective corporate controls. We include behavioral psychologists – and their methodologies – as an integral part of the team in a range of audits and reviews, providing both qualitative and quantitative risk culture feedback.” (PwC 2009)

In doing so, consultants recognized the delicate balance between control and empowerment:

Ensuring that people within an organization behave with integrity and in accord with the values and goals of the firm depends upon the balance between the firms’ stated rules and expectations, referred to as the entity-level instruments, and other factors that frame and condition an individual’s expectations of proper behavior, the cultural drivers. (KPMG 2016)

EY’s model incorporates the “tangible” elements of organizational structures and risk management systems (the culture mechanisms) with the more “intangible” elements of behavior. (E&Y 2015)

The measurement and reporting approaches of the consultants were also flexible and adaptable, where their clients could *define what they want to measure and what they want to report* (Informant 13). Consultants argued that *mere measurement, evaluation, and monitoring* could attract a senior manager’s attention *if the trends reveal something unusual* (Informant 13). Some consultants argued that mismatch between banks’ old models and language makes it difficult to implement changes in culture.

This causes quite a lot of work, quite a lot of worries I would say, because suddenly you’re going to get something that doesn’t fit in with your old model, with your old language so to speak. And I believe that the banks are really struggling with this because it’s at the core of their business model. (Informant 12)

One of the consultants went on to explain that the problem was not measuring culture instead of changing it. Informant 14 noted: *It is one thing to measure it [risk culture]. It could definitely be measured [to some extent]. But the problem is how to fix it.* The other consultant pointed to the judgment and flexibility required for the assessment of culture:

There’s also a lot of conceptual issues and a lot of judgment, and that’s the interesting part of it. (Informant 12)

Here, consultants specifically pointed to challenges with corporate governance, internal control, and IA. Consultants proposed that *creating procedures and level of checking* as well as *independence* were of utmost importance for all governance functions (Informant 13). Some consultants argued that internal auditors need to be independent enough to *challenge the risk control functions in their approach to control* (Informant 12).

Hence, consultants proposed *validation and check* from IA as well as external consultants (Informant 13). Some consultants proposed *pattern matching* and *big data analysis* to understand behavioral issues where such data were available (Informant 13). They argued that *it is subjective* and *requires appropriate judgment and education* of the board members and control functions (Informant 13). The consultants criticized the traditional IA practices of control as debilitating and recognized that the traditional notions of IA do not empower employees, and thus, employees do not take ownership of risks:

While we recognize that the 2013 FSB guidance has called on IA to report on effectiveness of risk appetite frameworks, it has not recognized the debilitating impact of regulators continuing to support the traditional IA paradigm [...] which promotes avoidance of risk ownership. – Risk Oversight responding to FSB risk culture paper

### Implementers: Control and Compliance

On the issue of risk culture, the implementers promoted the traditional “control of the control” model of IA and involvement with corporate governance. Informant 8 remarked, *We [risk control] are more involved in the development, check whether the model is compliant, and IA must verify whether what we do is correct in our work. So, they verify our process of validation, testing, and analysis.* Even audit manuals emphasized such views explicitly:

IA must control that the Bank has to adopt suitable devices for corporate governance and adequate mechanisms of management and control. (Large Bank-2 Audit Manual- referring to all IA work including risk culture)

The traditional “control of the control” model of IA by the implementers could be justified considering their demand concerning ambiguous guidance on the issue of risk culture audit:

There are no consistent standards, no consistent guidance, no tools, [...]. It's all new, uncharted territory. With Sarbanes-Oxley, there were defined steps sup-

ported by guidance. But with auditing culture, there is a lack of clear guidance from regulators about what they're looking for. (IIA workshop document quoting chief audit executive-1)

“Verification,” “identification of irregularities,” and “operational errors” were the buzzwords that implementers related quite frequently to IA approaches.

The auditors have to check if the main information given is correct or not. (Informant 7)

When we carry out an audit, and we identify irregularities in processes. (Informant 9)

“We have recently been discussing at work what happens. [...] if something goes wrong [at the fund companies]? If something is [...] calculated in a wrong way and some people have sold and bought units on that. So this is a debate that we have [...] how [...] can you develop internal systems and internal control to avoid this. (Informant 1)

The verifications proposed were of three types. First, the documental analysis was purported to evaluate the adequacy of the documentation by verifying the official documentation produced by the different functions. Second, empirical analysis of data was promoted to ensure the level of implementation and performance of processes/systems. Third, practice verifications using interviews and on-site visits were suggested. However, these verification principles were high-level, and their actual implementation was left to lower-level operations (IA manual of large bank 2). As informant 7 noted, *Then you have cultural problems, cultural differences actually [...], that you need to somehow take into consideration. And then you have the relationship between head office and subsidiary, which somehow creates situations that you have to be, how can I say, to be able to differentiate between different situations.* The verification approaches also promoted the traceability of evidence:

If you ask the insurance manager, do our sales people receive training [...], but then he'd say yes. I want to see some proof like certification, e-learning certification for example. What is not written does not exist in our world. (Informant 4)

To achieve traceability, the implementers recommended formalization and documentation of line management activities and sought their involvement in this regard. As informant 4 recalled, *Even the activities to be carried out by line management have to be formalized in some way. [...] It has to be formalized because we need proof of it. In case we get an inquiry from supervisory authorities or the board.* Informant 10 suggested employee participation in this process of formalization: *What you would do is you would initially have all the interviews with them (employees) to*

*understand what are the developments, what are their objectives, what do they plan for the future? You would collect a lot of information, and you would do your own analysis. Then you would do the risk assessment how you see where the biggest risks are. Then you will go to them and say, Well this is how we see the risk. How do you see the risks?*

Despite promoting the involvement of employees and the first line of defense, the board's guidance on risk appetite and level of risk-taking was identified as crucial.

What we're trying to do is to strengthen the first line of defense regarding risk management. [...] We have appointed risk owners to make sure that we all mention the risks in line with the decided risk cap types that are decided by the Board. (Informant 5)

The risk appetite framework and governance process and its embedding at all levels of the organization will help to make the risk culture tangible by promoting and enabling the right understanding and conversations at all levels.- HSBC responding to FSB risk culture paper

The proper implementation of board-driven risk appetite and involvement of the first line of defense, i.e., employees, was reinforced through proper compensation frameworks and monitoring by the control functions.

On a daily basis, we're monitoring the risk, managing the risk evolution or development to make sure that the company is managed within the decided risk cap size. So, these figures are frequently monitored. (Informant 5)

We believe many mechanisms support the development of a sound risk culture including (but not limited to) the compensation framework, the performance assessment process, and the risk appetite and risk management frameworks. - - Deutsch Bank responding to FSB risk culture paper

Even advanced approaches demonstrated the control and monitoring-based understanding of the IA of risk culture. Informant 18 (of the FSB), reflecting on her recent banking risk culture workshop, remarked, *Some banks are using big data to monitor their risk culture. They can analyze the behavioral patterns of the big data to assess culture.*

The IA processes of implementers focused on measurement, reporting, and issue-handling processes, as well. informant 4 remarked, *[Y]ou need to measure it, you need to steer it, you need to follow up and report it, and these four steps are critical in the first line of defense work within the financial institution.* Measurements and reporting especially involved metrics such as inadequate training, ineffective processes, or lack of procedures.

Our reports will include issues that are symptoms of broader culture issues within a business area such as inadequate training, ineffective processes, or lack of procedures, and we will work with the appropriate level of management to develop action plans that adequately address the underlying root cause. (IIA case-document quoting IA head-1)

It includes such elements as a history of errors, a pattern of repeat audit findings, concerns about management surfaced by IA, or concerns presented to IA by others. (IIA case-document quoting IA head-2)

The implementers promoted a measurement and metrics-based approach of IA of risk culture audit, arguing that metrics are useful for the boards to make consistent judgment considering the subjectivities of risk culture:

Given [...] subjectivity across many jurisdictional boundaries, what we, as risk professionals, have to offer is a direction toward a quantitative floor for boards and their management from which to allow supervisors to make consistent judgments. – Blue Ribbon Advisory Panel of the Professional Risk Managers' International Association responding to FSB risk culture paper

Apart from metrics, issue identification itself was shown to be valuable for promoting changes in the systems. As noted by Informant 5, *[The] intention is to set up a form so we can prioritize how these incidents should be avoided in the future and how they should be solved, if they are not solved instantly, if there are many incidents – if you need to change the process or if you need to change the system or whatever.* Issue identification was not considered sufficient for IA activities; issue-handling processes were employed to advise the line functions. Informant 4 remarked, *No, we don't [fix] the deviation, we make suggestions [on] how the deviation could be or should be [fixed], – we [audit and the auditee] agree on – there has to be a deadline timeframe.* Here, some implementers suggested that they see themselves as helping to line managers.

We try to see the internal auditor as help [to the auditees] rather than just writing something bad [about them] that we found. Having open issues is normal. It's perfectly fine everyone has it. If you don't have them, that's really weird. (Informant 10)

The involvement of line managers also meant that the issue-handling processes relied on negotiation with the line managers. Informant 10 remarked, *When we do an audit, and we identify irregularities, a lot of the times there are process irregularities. We will report all of the findings, but before we report we, of course, will have the discussion with the auditee, and we will agree that this is*

*a problem and how we describe the problem.* However, communication with line managers was considered tricky, and the informants identified compromised independence of the control functions in this regard:

Yes, but this is one issue that has been brought up from the control functions like myself [the risk control function], the compliance function and [the] IA, as we see that there is a risk of not being independent and that could be a risk of conflicts of interest. (Informant 5)

Consequently, to maintain the independence of control functions, some implementers even opposed the advisory roles attributed to control functions:

The wording seems to suggest that compliance and other control functions' primary activity is to act as advisors. We have a strong view that these functions should first and foremost act as a risk control function and then secondly, and to a much lesser extent, an advisory function. - - HSBC responding to FSB risk culture paper

Although issue identification, mitigation advice, and reporting were carried out in consultation and communication with line managers, issue closing was dependent on verification. As noted by informant 10: *Well you have a lot of communication on open issues, right. Because for example these open issues that are in our system they need to get closed. Whenever something has been done to close the issues, then we have to look at it and ascertain that it's really been closed.*

We speculate that the implementers stuck to the traditional view of IA as verification because they recognized that controlling the behaviors of employees (such as compliance to a set rule or adherence to policies) was essential in curbing problems within organizations. Hence, the focus of IA and control was on reducing dysfunctionality or intentional breaches of policies from employees.

We agree that non-adherence to a code of conduct should affect compensation and career prospects. - World Savings and Retail Banking Institute (WSRBI) responding to FSB risk culture paper

It should be clearly stated that only those breaches in internal policies, procedures and risk limits which prove to be intentional should have an impact on the compensation and career of the employees that are responsible for them. - - WSRBI responding to FSB risk culture paper

The implementers also resented the tight guidelines of the regulatory authorities. For example, the implementers and

their associations opposed detailed recommendation on risk appetite by the regulators:

While DB's current risk appetite framework is largely in line with the principles, we are concerned that a requirement to establish risk limits at a legal entity level is too broad-reaching. - - Deutsch bank on risk appetite framework by the FSB

It should thus be mentioned that, even though setting definitions may be useful, institutions shall retain some flexibility in the way they will articulate their own framework and in the key elements they wish to use in order to do so. - - French Banking Federation on risk appetite framework by the FSB

However, when the regulators issued risk culture guideline, the implementers and their lobbying organizations opposed such measures by saying that risk appetite was enough:

We feel, however, that the Risk Appetite Framework (RAF) is the embodiment of an institution's risk culture and that it is unnecessary to go beyond assessing the robustness of the RAF [...]. Therefore, the guidelines for assessing risk culture should avoid adding new layers or expectations of new processes being created and leverage existing tools and requirements to assess risk culture - - CRO forum on risk culture

To keep the control loose, the implementers demanded fluidity in IA guidelines, a "rules-based approach," and "tools" from the regulators:

All the tools listed here may be helpful, but it is important that the final guidance is clear that no suite of tools should be considered as a checklist for either management or supervisors. - - Deutsch Bank responding to FSB risk culture paper

Practitioner-based organizations helped implementers in promoting their views. In this regard, the discussion with the FSB informant revealed an influential body of practitioners known as the G30. The G30 introduced its views on risk culture, its audit, and supervision in October 2013. In this document, the G30 moved from the issue of risk governance and risk appetite to risk culture, thereby latching on to the existing secondary system for verification. Although the G30 did not detail the IA of risk culture, it indicated that compliance with an *a priori* set standard was the preferred way to audit risk culture in banks. The G30 later confirmed this in a separate document in 2015 by recommending the development of *a comprehensive set of indicators to monitor and assess individual and team adherence to firm values and desired conduct.*" (G30, Banking Conduct and Culture document, page 50). The G30 also recommended upgrading

of the IA “skill set” and strengthening of the “organizational independence.” (G30, Banking Conduct and Culture document, page 63).

## Discussion

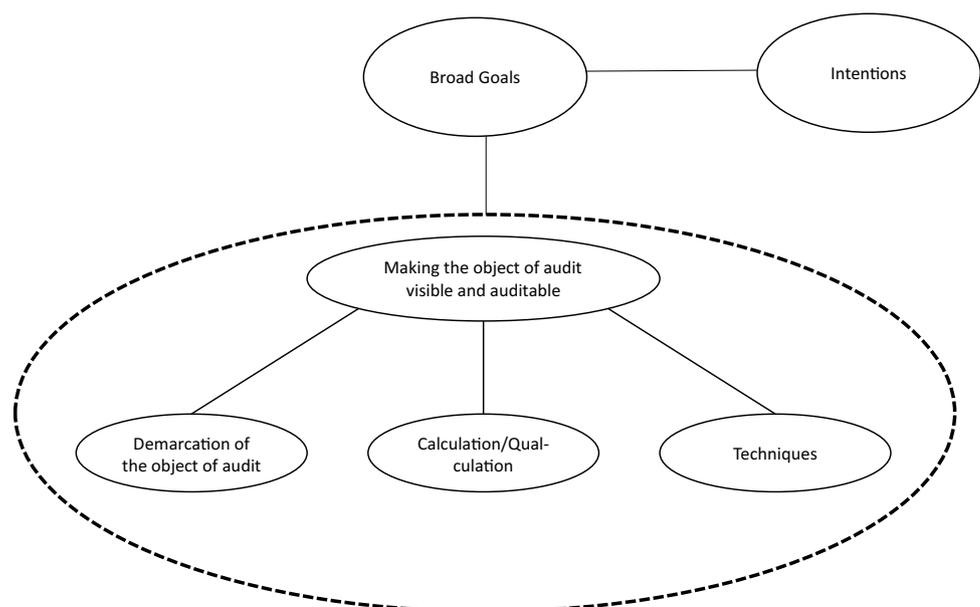
Our results, summarized in the model of Fig. 1, suggest that the intentions of the actors affected their broad goals on the IA of risk culture. Both the intentions and broad goals, in turn, were contingent on the history and context (Parker and Johnson 2017). The broad goals influenced the approaches of demarcation, calculation/qualculation, and techniques that attributed visibility and auditability to the object of IA.

Analyzing the perspectives of different actors (summarized in Table 6), we can highlight that both the regulators and the implementers posited IA as a control mechanism (w.r.t risk culture) to monitor and control the behavior of employees. The monitoring and control were aimed at the conformance of employees’ conduct to codes and policies set by top management and the board. The emphasis on monitoring and control promoted the objectification of individuals’ conduct, highlighting dysfunctional and unwarranted behavior as the prime reason for failures and disasters (Baud and Chiapello 2016; MacLulich 2003; Vaughan 1999). However, the two actors had divergent goals and political intentions. The regulators’ rationale on installing new self-checks and balances to curb excessive risk-taking by banks in the aftermath of the financial crisis was linked to their historical perception of IA as a control and governance mechanism (Chambers 2014; Collier and Zaman 2005; Mihret 2014; Sarens et al. 2013). However, contrary to the recent thesis of Baud and Chiapello (2016), the regulators,

in our case, still believed in self-regulation and hesitated to suggest a strict approach to the IA of risk culture (Power 1997, 1999). The implementers, in contrast, promoted the status quo of IA avoiding costly implementations, fearing intervention in the profiteering activities by regulators (Wahlström 2006, 2009).

The regulators and the implementers reached the IA of risk culture in steps that involved making risk culture visible with existing systems of risk appetite and risk governance. Furthermore, both the regulators and the implementers focused on the four qualitative areas of assessment: presence of the definition of risk culture, risk appetite, and risk governance in policy documents; communication of such definitions to employees; monitoring by the board; and promotion of “appropriate” behavior through incentives. None of these areas of assessment were new (Abbott et al. 2010; Morgan 1980), but they were adapted to include the elements of risk culture. While suggesting such simplistic adaptations, the regulators and the implementers accepted the inadequacy of the calculability of risk culture, the requirement of the involvement of all employees, and the ineffectiveness of the traditional IA outcomes (Power 1999). Although the regulators noted “problems” with the existing practices of IA, they thought it to be irrelevant when it came to modifying the IA techniques. In maintaining status quo and avoiding investments, the implementers also favored the inclusion of risk culture elements in their existing routines of IA. In summary, both actors endorsed the adaptation of existing IA techniques, such as tracing evidence in interviews, surveys, and documents informing on protocols, process ownership, and departments (Norman et al. 2010; Power 1999, 2000).

**Fig. 1** Internal auditing approaches for risk culture



In contrast to the regulators and the implementers, the normalizers and the consultants propounded IA as a control mechanism coupled with the empowerment of the first line of defense (employees). The empowerment included training and allowing employees to freely raise their views (Foucault 1988b; Townley 1994). The normalizers' documents reveal that they worked regularly with consultants in developing their framework, and thus, the consultants' viewpoints affected them (Hayne and Free 2014). The normalizers also wanted to legitimize their expertise as thought leaders. Consequently, the normalizers tied their view on the IA of risk culture to their professional frameworks (Roussy and Brivot 2016). Motivated to keep their thought leadership, the normalizers reconciled efforts from the regulators and the consultants to promote a library of toolkits and a bricolage of ideas to guide implementing organizations. The consultants were interested in positing IA as a part of a comprehensive control framework within organizations. Apart from their not-so-narrow focus on IA, consultants idea to sell solutions and monetize them played an important role in addressing the IA of risk culture as a paradigmatic change (Christensen and Skærbæk 2010).

Similar to the regulators and implementers, the normalizers and the consultants relied on the concepts of risk appetite and risk governance to render risk culture visible. However, these actors emphasized the assessment of risk culture through psychological and behavioral measurements using surveys and interviews. In doing so, these actors acknowledged that the business of banking is based on appropriate risk exploitation and risk-taking (Mikes 2009; Palermo et al. 2016). Consequently, these actors also proposed training, employee participation and self-assessment of employees that could enable employees to make informed decisions on risk-taking (Foucault 1988b; Miller and Rose 2008; Rose and Miller 1992). To sum up, these groups of actors understood that human beings could be empowered by expertise and knowledge to mobilize the appropriate contextual conduct (Dean 1999, p. 22), allowing them to be critical decision makers (McCabe 2014).

The heterogeneity of the conceptions of IA among different stakeholders might seem unsurprising given the ambiguity of the object of IA (risk culture in our case) and the variety of current IA practices. However, our findings reveal several relevant theoretical implications. First, the absence of the implementers' support or coercive regulation on changing the conventional IA notions and techniques raises doubt on whether IA in the near term would be able to break free from its current paradigm of securing tangible processes to the new paradigm of securing individual motivations and attitudes of the employees guided by risk culture and ethical values within organizations. There is a danger that a direct transfer of knowledge, without critical considerations on intangibility of risk culture,

**Table 6** Different risk culture audit approaches

Actors Elements	Standard Setters	Normalizers	Consultants	Implementers
Making the object of audit visible and auditable				
Demarcating boundaries of audit	Not fully calculable, use secondary systems of risk governance and risk appetite	Not fully calculable, mélange of risk appetite, governance, and a new system	Not fully calculable, "branded" new systems involving risk appetite and governance	Not fully calculable, use secondary systems of risk governance and risk appetite
Calculation/qualculation	Areas for qualitative and quantitative assessment	Areas for qualitative and quantitative assessment	Areas for qualitative and quantitative assessment	Areas for qualitative and quantitative assessment
Techniques	Existing	new tools of behavior measurement, employee empowerment and training	new tools of behavior measurement, employee empowerment and training	Existing
Broad goals for IA of risk culture	Control and Governance through the third line of defense	Control and Governance through the third line of defense, empowerment and training of employees (first line of defense)	Control and Governance through the third line of defense, empowerment and training of employees (first line of defense)	Control and Governance through the third line of defense, compliance
Intentions	New checks and balances	Thought leadership	Monetizing new solutions	Status quo to avoid investment

could lead to ritualistic thinking among implementers, promoting an ineffective tick-box-based compliance approach of IA in controlling culture (McCabe 2014; Power 1999). Second, the current control and governance focus of the different stakeholders is based on the calculation (Callon and Muniesa 2005; Vaivio 1999, 2006) and qualculation (Callon and Law 2005; Cochoy 2008) associated with tangible processes that facilitate discernible trails for verification and accountability during traditional applications of IA (Goodwin and Yeo 2001; Vaivio 1999, 2006). This type of control approach mired in calculation/qualculation, if extended to employees' behavior, could rob employees of their individuality as well as their critical and moral thinking (leading to the colonization of employees' emotional self) (Ezzy 2001; McCabe 2014). Third, the approaches of normalizers and consultants to the implementation of IA as a control mechanism balanced by the empowerment of employees through training seem theoretically plausible but could be pragmatically difficult to attain (McCabe 2014; Simons 1995). Theoretically, empowering employees through training and self-assessment might help control the problems arising from an uncritical mechanistic approach of thinking and avoid colonization of the employees' self. At the same time, independent and objective control by IA could help curb problems due to policy violation, dysfunctionality, and abnormal decisions that harm organizations (Vaughan 1999). In practice, empowered employees could contribute to value creation through their innovative ideas, but they could also be difficult to control and could harm organizational well-being (Simons 1995). Also, solutions with a delicate balance of "control and empowerment," if achieved, could be context dependent (Simons 1995). While the context dependency might help IA practices in becoming suitable to organizational ambiguities (Englund et al. 2013) and professionalization endeavors by requiring non-transparent judgmental approaches (Power 1999), at the same time, it could diminish the independence and objectivity of IA (Christopher et al. 2009; Goodwin and Yeo 2001; Roussy and Brivot 2016).

Our results also raise several ethical implications for teams conducting IA of risk culture. First, the competency-related deontological ethics of IA by the IIA warns IA teams in indulging in any activities where they lack "the necessary knowledge, skills, and experience." This means that IA teams would need to undergo proper training and acquire knowledge on assessing culture, especially psychology and personality of employees, before they can audit culture. Second, since auditing culture would mean more freedom of judgment on a vast number of issues for the IA teams, it would become difficult for IA teams to ascertain the moral ethos of independence and objectivity in their judgment. Third, IA teams would be handling personality- and motivation-related information of employees through survey

instruments; this would mean that IA teams would need to handle such personal information of employees without dehumanizing employees to bits and bytes of data. Fourth, since IA teams would be seeking more personal information from employees during one-to-one interviews, it might impair their already impaired ethos of independence and objectivity further because they would need to be close to employees in seeking such information. Fourth, if independence and objectivity form the deontological ethical frame of IA, then how can IA teams be independent and objective in auditing culture while being a part of it.

## Conclusion

This paper set out to analyze how different actors—regulators, normalizers, consultants, and implementers—conceive the IA of risk culture and embrace different approaches to achieve this aim. Before highlighting our contribution, we acknowledge several limitations of our study and explicate avenues for future research. First, our study relies on heterogeneous data sources (e.g., documents drafted for different purposes) with possible implications for the reliability of the results. Hence, we promote future studies employing a "homogeneous" set of data generated by interviews, focus group, or experiments. Second, our study has not exhausted the disparate viewpoints on the IA of risk culture. In fact, differences in viewpoints may exist at different organizations and different levels within organizations. Consequently, we recommend further investigation on the views of different internal stakeholders (such as board, audit committees, internal auditors, compliance team members, and risk managers) in different organizations. Furthermore, longitudinal research could inform whether the differences in the IA approaches to risk culture elaborated in this study will continue to exist or whether a new dominant approach will prevail over all other approaches. Third, since many studies provide evidence on IA being an ethically compromised governance practice (Everett and Tremblay 2014; Ferry et al. 2017; Roussy 2013; Roussy and Rodrigue 2016), it could be important to understand how an ethically compromised IA could assure and consult on risk culture and ethical issues. Consequently, we also promote further studies on the ethical dilemma faced by internal auditors in carrying out risk culture or ethics audit. Fourth, we limited our focus to auditee-related data collection techniques of IA, and therefore, we promote further studies on judgment approaches and "auditee's account giving" as a means to problematize the conceptions of IA in the risk culture domain.

Finally, our research posits three main contributions. First, we contribute to understanding how IA practices could

include intangible objects such as risk culture and ethics. While our proposed framework may not be perfect and concrete, it does provide a helpful systematic way of thinking on how objects of audit could be made visible by demarcation (Abbott 1995; Bowker and Star 1996) and then auditable by measurement (Callon and Law 2005; Callon and Muniesa 2005; Cochoy 2008) and IA techniques (Power 1999).

Second, we address scholars' call to examine how audit gets accepted into new domains (Kaspersen and Johansen 2016; Pentland 2000; Power 1996). However, in contrast to the existing studies on external audit expansions (Free et al. 2009; Power 1996; Robson et al. 2007), we focused on IA expansions where theoretical literature is scarce (Gramling et al. 2004; Parker and Johnson 2017), and practices tend to be heterogeneous (Arena and Jeppesen 2015; Roussy and Brivot 2016). The unbounded and intangible nature of risk culture allowed us to extend the "systems of audit" concept currently applied to tangible processes (Power 1997, 1999) by including ideas on the boundaries, measurement, and audit approaches linked to such boundaries and measurement.

Third, we address scholars' call to understand the manifold conceptions of IA and its contextual and historical drivers (cf. Erasmus and Coetzee 2018; Roussy and Brivot 2016). In doing so, we enrich the literature on the IA of risk culture that focused on either the contextual viewpoints of implementers (Carretta et al. 2017; Cornia et al. 2016; Palermo et al. 2016) or the regulatory viewpoints (Power 1999; Ring et al. 2016) by highlighting its manifold notion.

**Acknowledgements** This paper is produced as part of the EMJD Program, European Doctorate in Industrial Management (EDIM), funded by the European Commission, Erasmus Mundus Action 1. We also thank two anonymous referees and the handling editor, Prof. Steven Dellaportas, for valuable suggestions and guidance.

## Compliance with Ethical Standards

**Conflict of interest** The authors declare that they have no conflict of interest.

**Ethical Approval** All procedures performed in this study were in accordance with the ethical standards of the institutional and/or national research committee and with the 1964 Helsinki Declaration and its later amendments or comparable ethical standards.

**Informed Consent** Informed consent was obtained from all individual participants included in the study.

**Open Access** This article is distributed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made.

## References

- Abbott, A. (1995). Things of boundaries. Defining the boundaries of social inquiry. *Social Research*, 62(4), 857–882.
- Abbott, L. J., Parker, S., & Peters, G. F. (2010). Serving two masters: The association between audit committee internal audit oversight and internal audit activities. *Accounting Horizons*, 24(1), 1–24. <https://doi.org/10.2308/acch.2010.24.1.1>.
- Abdolmohammadi, M. (2013). Correlates of co-sourcing/outsourcing of internal audit activities. *Auditing: A Journal of Practice & Theory*, 32(3), 69–85. <https://doi.org/10.2308/ajpt-50453>.
- Arel, B., Beaudoin, C. A., & Cianci, A. M. (2012). The impact of Ethical leadership, the internal audit function, and moral intensity on a financial reporting decision. *Journal of Business Ethics*, 109(3), 351–366. <https://doi.org/10.1007/s10551-011-1133-1>.
- Arena, M., Arnaboldi, M., & Azzone, G. (2010). The organizational dynamics of enterprise risk management. *Accounting, Organizations and Society*, 35(7), 659–675. <https://doi.org/10.1016/j.aos.2010.07.003>.
- Arena, M., Arnaboldi, M., & Palermo, T. (2017). The dynamics of (dis)integrated risk management: A comparative field study. *Accounting, Organizations and Society*, 62, 65–81. <https://doi.org/10.1016/j.aos.2017.08.006>.
- Arena, M., & Jeppesen, K. K. (2009). The jurisdiction of internal auditing and the quest for professionalization: The danish case. *International Journal of Auditing*, 129, 111–129. <https://doi.org/10.1111/j.1099-1123.2009.00408.x>.
- Arena, M., & Jeppesen, K. K. (2015). Practice variation in public sector internal auditing: An institutional analysis. *European Accounting Review*. <https://doi.org/10.1080/09638180.2015.1018917>.
- Bartlett, G. D., Kremin, J., Saunders, K. K., & Wood, D. A. (2016). Attracting applicants for in-house and outsourced internal audit positions: Views from external auditors. *Accounting Horizons*, 30(1), 143–156. <https://doi.org/10.2308/acch-51309>.
- Baud, C., & Chiapello, E. (2016). Understanding the disciplinary aspects of neoliberal regulations: The case of credit-risk regulation under the Basel Accords. *Critical Perspectives on Accounting*. <https://doi.org/10.1016/j.cpa.2016.09.005>.
- Berger, P. L., & Luckmann, T. (1966). *The social construction of reality*. Penguin Group. <https://doi.org/10.2307/323448>.
- Bowker, G. C. G., & Star, S. L. S. (1996). How things (actor-net) work: Classification, magic and the ubiquity of standards. *Philosophia*, 25(3–4), 195–220.
- Brody, R. G., Golen, S. P., & Reckers, P. M. J. (1998). An empirical investigation of the interface between internal and external auditors. *Accounting and Business Research*, 28(3), 160–171. <https://doi.org/10.1080/00014788.1998.9728907>.
- Burton, F. G., Starliper, M. W., Summers, S. L., & Wood, D. A. (2015). The effects of using the internal audit function as a management training ground or as a consulting services provider in enhancing the recruitment of internal auditors. *Accounting Horizons*, 29(1), 115–140. <https://doi.org/10.2308/acch-50925>.
- Callon, M., & Law, J. (2005). On calculation, agency, and otherness. *Environment and Planning D: Society and Space*, 23(5), 717–733. <https://doi.org/10.1068/d343t>.
- Callon, M., & Muniesa, F. (2005). Peripheral vision. *Organization Studies*, 26(8), 1229–1250. <https://doi.org/10.1177/0170840605056393>.
- Caplan, D. H., University, I. S., Kirschenheiter, M., & University, C. (2000). Outsourcing and audit risk for internal audit services. *Contemporary Accounting Research*, 17(3), 387–428. <https://doi.org/10.1506/8CP5-XAYG-7U37-H7VR>.
- Carretta, A., Fiordelisi, F., & Schwizer, P. (2017). *Risk Culture in Banking*. London: Palgrave Macmillan.

- Castanheira, N., Rodrigues, L. L., & Craig, R. (2009). Factors associated with the adoption of risk-based internal auditing. *Managerial Auditing Journal*, 25(1), 79–98. <https://doi.org/10.1108/02686901011007315>.
- Chambers, A. D. (2014). Guidance on internal audit's interface with regulators: An analysis and appraisal of recent developments. *Managerial Auditing Journal*, 29(3), 268–283. <https://doi.org/10.1108/MAJ-08-2013-0927>.
- Chambers, A. D., & Odar, M. (2015). A new vision for internal audit. *Managerial Auditing Journal*, 30(1), 34–55. <https://doi.org/10.1108/MAJ-08-2014-1073>.
- Chartered Institute of Internal Auditors. (2014). *Culture and the role of internal audit: looking below the surface*. <http://auditandrisk.org.uk/policyblog/cultureandtheroleofinternalaudit>.
- Christ, M. H., Masli, A., Sharp, N. Y., & Wood, D. A. (2015). Rotational internal audit programs and financial reporting quality: Do compensating controls help? *Accounting, Organizations and Society*, 44, 37–59. <https://doi.org/10.1016/j.aos.2015.05.004>.
- Christensen, M., & Skærbæk, P. (2010). Consultancy outputs and the purification of accounting technologies. *Accounting, Organizations and Society*, 35(5), 524–545. <https://doi.org/10.1016/j.aos.2009.12.001>.
- Christopher, J., Sarens, G., & Leung, P. (2009). A critical analysis of the independence of the internal audit function: evidence from Australia. *Accounting, Auditing & Accountability Journal*, 22(2), 200–220. <https://doi.org/10.1108/09513570910933942>.
- Cochoy, F. (2008). Calculation, qualculation, calculation: Shopping cart arithmetic, equipped cognition and the clustered consumer. *Marketing Theory*, 8(1), 15–44. <https://doi.org/10.1177/1470593107086483>.
- Cohen, J., Krishnamoorthy, G., & Wright, A. M. (2002). Corporate governance and the audit process. *Contemporary Accounting Research*, 19(4), 573–594. <https://doi.org/10.1506/983M-EPXG-4Y0R-J9YK>.
- Collier, P., & Zaman, M. (2005). Convergence in European corporate governance: The audit committee concept. *Corporate Governance*. <https://doi.org/10.1111/j.1467-8683.2005.00468.x>.
- Corbin, J. M., & Strauss, A. (1990). Grounded theory research: Procedures, canons, and evaluative criteria. *Qualitative Sociology*, 13(1), 3–21. <https://doi.org/10.1007/BF00988593>.
- Cornia, A., Dressel, K., & Pfeil, P. (2016). Risk cultures and dominant approaches towards disasters in seven European countries. *Journal of Risk Research*, 19(3), 288–304. <https://doi.org/10.1080/13669877.2014.961520>.
- Covalesski, M. A., Dirsmith, M. W., & Rittenberg, L. (2003). Jurisdictional disputes over professional work: The institutionalization of the global knowledge expert. *Accounting, Organizations and Society*. [https://doi.org/10.1016/S0361-3682\(02\)00029-6](https://doi.org/10.1016/S0361-3682(02)00029-6).
- de Zwaan, L., Stewart, J., & Subramaniam, N. (2011). Internal audit involvement in enterprise risk management. *Managerial Auditing Journal*, 26(7), 586–604. <https://doi.org/10.1108/0268690111151323>.
- Dean, M. (1999). *Governmentality Power and Rule in Modern Society* (2nd edn.). London: SAGE Publications.
- Deloitte. (2015). *Cultivating a Risk Intelligent Culture: Understand, measure, strengthen and report*.
- E&Y. (2014). *Shifting focus: Risk culture at the forefront of banking*. <https://www.ey.com/Publication/vwLUAssets/ey-shifting-focus-risk-culture-at-the-forefront-of-banking/FILE/ey-shifting-focus-risk-culture-at-the-forefront-of-banking.pdf>.
- E&Y. (2015). *Risk culture: How can you create a sound risk culture?* [https://www.ey.com/Publication/vwLUAssets/Risk\\_culture\\_-\\_How\\_can\\_you\\_create\\_a\\_sound\\_risk\\_culture/\\$FILE/EY-risk-culture-model-brochure.pdf](https://www.ey.com/Publication/vwLUAssets/Risk_culture_-_How_can_you_create_a_sound_risk_culture/$FILE/EY-risk-culture-model-brochure.pdf).
- Englund, H., Gerdin, J., & Abrahamsson, G. (2013). Accounting ambiguity and structural change. *Accounting, Auditing & Accountability Journal*, 26(3), 423–448. <https://doi.org/10.1108/09513571311311883>.
- Erasmus, L., & Coetzee, P. (2018). Drivers of stakeholders' view of internal audit effectiveness. *Managerial Auditing Journal*, 33(1), 90–114. <https://doi.org/10.1108/MAJ-05-2017-1558>.
- Everett, J., & Tremblay, M.-S. (2014). Ethics and internal audit: Moral will and moral skill in a heteronomous field. *Critical Perspectives on Accounting*, 25(3), 181–196. <https://doi.org/10.1016/j.cpa.2013.10.002>.
- Ezzy, D. (2001). A simulacrum of workplace community: Individualism and engineered culture. *Sociology*, 35(03), 631–650. <https://doi.org/10.1017/S0038038501000323>.
- Fanning, K., & David Piercey, M. (2014). Internal auditors' use of interpersonal likability, arguments, and accounting information in a corporate governance setting. *Accounting, Organizations and Society*, 39(8), 575–589. <https://doi.org/10.1016/j.aos.2014.07.002>.
- Felix, W., Gramling, A., & Maletta, M. (2001). The contribution of internal audit as a determinant of external audit fees and factors influencing this contribution. *Journal of Accounting Research*, 39(3), 513–533. <https://doi.org/10.1111/1475-679X.00026>.
- Ferry, L., Zakaria, Z., Zakaria, Z., & Slack, R. (2017). Watchdogs, helpers or protectors?—Internal auditing in Malaysian Local Government. *Accounting Forum*. <https://doi.org/10.1016/j.accfor.2017.10.001>.
- Foucault, M. (1988a). *Discipline And Punish The Birth of the Prison*. New York: Vintage Books.
- Foucault, M. (1988b). Technologies of the Self. In L. H. Martin, H. Gutman, & P. H. Hutton (Eds.), *Technologies of the Self: A seminar with Michel Foucault*. Amherst: The University of Massachusetts Press.
- Free, C., Salterio, S. E., & Shearer, T. (2009). The construction of auditability: MBA rankings and assurance in practice. *Accounting, Organizations and Society*, 34(1), 119–140. <https://doi.org/10.1016/j.aos.2008.02.003>.
- Friedberg, A. (1998). Ethical aspects of internal auditing. *Journal of Business Ethics*, 17(8), 895–904. <https://doi.org/10.1023/A:1005738307884>.
- Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2013). Seeking qualitative rigor in inductive research. *Organizational Research Methods*, 16(1), 15–31. <https://doi.org/10.1177/1094428112452151>.
- Goodwin, J. (2003). The relationship between the audit committee and the internal audit function: Evidence from Australia and New Zealand. *International Journal of Auditing*, 7(3), 263–278. <https://doi.org/10.1046/j.1099-1123.2003.00074.x>.
- Goodwin, J., & Yeo, T. Y. (2001). Two factors affecting internal audit independence and objectivity: Evidence from Singapore. *International Journal of Auditing*, 5(2), 107–125. <https://doi.org/10.1111/j.1099-1123.2001.00329.x>.
- Gramling, A. A., Maletta, M. J., Schneider, A., & Church, B. K. (2004). The role of the internal audit function in corporate governance: A synthesis of the extant internal auditing literature and directions for future research. *Journal of accounting literature*, 23, 194.
- Hall, M., Mikes, A., & Millo, Y. (2015). How do risk managers become influential? A field study of toolmaking in two financial institutions. *Management Accounting Research*, 26, 3–22. <https://doi.org/10.1016/j.mar.2014.12.001>.
- Hayne, C., & Free, C. (2014). Hybridized professional groups and institutional work: COSO and the rise of enterprise risk management. *Accounting, Organizations and Society*, 39(5), 309–330. <https://doi.org/10.1016/j.aos.2014.05.002>.
- Jiang, L., André, P., & Richard, C. (2018). An international study of internal audit function quality. *Accounting and Business Research*, 48(3), 264–298. <https://doi.org/10.1080/00014788.2017.1357461>.

- Kaspersen, M., & Johansen, T. R. (2016). Changing social and environmental reporting systems. *Journal of Business Ethics*, 135, 731–749.
- KPMG. (2009). *What's your company's risk culture*. <https://www.bloomberg.com/news/articles/2009-05-12/whats-your-companys-risk-culture>.
- KPMG. (2016). *Approaching the crossroads of conduct and culture: Improving culture in the financial services industry*. <https://assets.kpmg.com/content/dam/kpmg/us/pdf/approaching-the-crossroads-of-conduct-and-culture.pdf>.
- Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic Inquiry*. Thousand Oaks: Sage Publications. <https://doi.org/10.1177/1473325006070288>.
- MacLean, T., Litzky, B. E., & Holderness, D. K. (2015). When Organizations don't walk their talk: a cross-level examination of how decoupling formal ethics programs affects organizational members. *Journal of Business Ethics*, 128(2), 351–368. <https://doi.org/10.1007/s10551-014-2103-1>.
- MacLulich, K. K. (2003). The emperor's 'new' clothes? New audit regimes: insights from Foucault's technologies of the self. *Critical Perspectives on Accounting*, 14(8), 791–811. [https://doi.org/10.1016/S1045-2354\(02\)00206-X](https://doi.org/10.1016/S1045-2354(02)00206-X).
- Mat Zain, M., Zaman, M., & Mohamed, Z. (2015). The effect of internal audit function quality and internal audit contribution to external audit on audit fees. *International Journal of Auditing*, 19(3), 134–147. <https://doi.org/10.1111/ijau.12043>.
- McCabe, D. (2014). Light in the darkness? Managers in the back office of a kafkaesque bank. *Organization Studies*, 35(2), 255–278. <https://doi.org/10.1177/0170840613511928>.
- Mihret, D. G. (2014). How can we explain internal auditing? The inadequacy of agency theory and a labor process alternative. *Critical Perspectives on Accounting*, 25(8), 771–782. <https://doi.org/10.1016/j.cpa.2014.01.003>.
- Mikes, A. (2009). Risk management and calculative cultures. *Management Accounting Research*, 20(1), 18–40. <https://doi.org/10.1016/j.mar.2008.10.005>.
- Mikes, A. (2011). From counting risk to making risk count: Boundary-work in risk management. *Accounting, Organizations and Society*, 36(4–5), 226–245. <https://doi.org/10.1016/j.aos.2011.03.002>.
- Miller, P., & O'Leary, T. (1987). Accounting and the construction of the governable person. *Accounting, Organizations and Society*, 12(3), 235–265. [https://doi.org/10.1016/0361-3682\(87\)90039-0](https://doi.org/10.1016/0361-3682(87)90039-0).
- Miller, P., & Power, M. (2013). Accounting, organizing, and economizing: Connecting accounting research and organization theory. *The Academy of Management Annals*, 7(1), 557–605. <https://doi.org/10.1080/19416520.2013.783668>.
- Miller, P., & Rose, N. (2008). *Governing the Present: Administering Social and Personal Life*. Cambridge: Polity Press.
- Morgan, G. (1980). Internal audit role conflict: A pluralist view. *Managerial Finance*, 5(2), 160–170. <https://doi.org/10.1108/eb013444>.
- Neu, D., Everett, J., & Rahaman, A. S. (2013). Internal auditing and corruption within government: The case of the Canadian sponsorship program. *Contemporary Accounting Research*, 30(3), 1223–1250. <https://doi.org/10.1111/j.1911-3846.2012.01195.x>.
- Norman, C. S., Rose, A. M., & Rose, J. M. (2010). Internal audit reporting lines, fraud risk decomposition, and assessments of fraud risk. *Accounting, Organizations and Society*, 35(5), 546–557. <https://doi.org/10.1016/j.aos.2009.12.003>.
- Palermo, T., Power, M., & Ashby, S. (2016). Navigating institutional complexity: The production of risk culture in the financial sector. *Journal of Management Studies*. <https://doi.org/10.1111/joms.12241>.
- Parker, S., & Johnson, L. A. (2017). The development of internal auditing as a profession in the U.S. during the twentieth century. *Accounting Historians Journal*, 44(2), 47–67. <https://doi.org/10.2308/aahj-10549>.
- Pentland, B. T. (2000). Will auditors take over the world? Program, technique and the verification of everything. *Accounting, Organizations and Society*, 25(3), 307–312.
- Power, M. (1996). Making things auditable. *Accounting, Organizations and Society*, 21(2/3), 289–315.
- Power, M. (1997). From risk society to audit society. *Soziale Systeme*, 3(1), 3–21.
- Power, M. (1999). *The Audit Society*. Oxford: Oxford University Press. <https://doi.org/10.1093/acprof:oso/9780198296034.001.0001>.
- Power, M. (2000). The Audit Society - Second Thoughts. *International Journal of Auditing*, (4), 111–119.
- Power, M. (2004). Counting, control and calculation: Reflections on measuring and management. *Human Relations*, 57(6), 765–783. <https://doi.org/10.1177/0018726704044955>.
- Power, M., & Gendron, Y. (2015). Qualitative research in auditing: A methodological roadmap. *Auditing: A Journal of Practice & Theory*, 34(2), 147–165. <https://doi.org/10.2308/ajpt-10423>.
- Prawitt, D. F., Sharp, N. Y., & Wood, D. A. (2012). Internal audit outsourcing and the risk of misleading or fraudulent financial reporting: Did sarbanes-oxley get it wrong? *Contemporary Accounting Research*, 29(4), 1109–1136. <https://doi.org/10.1111/j.1911-3846.2012.01141.x>.
- PwC. (2009). *Auditing risk culture: Art or science?*. [https://www.pwc.com.au/assurance/assets/auditingriskculture\\_feb09.pdf](https://www.pwc.com.au/assurance/assets/auditingriskculture_feb09.pdf).
- Ring, P. J., Bryce, C., McKinney, R., & Webb, R. (2016). Taking notice of risk culture—The regulator's approach. *Journal of Risk Research*, 19(3), 364–387. <https://doi.org/10.1080/13669877.2014.983944>.
- Robson, K., Humphrey, C., Khalifa, R., & Jones, J. (2007). Transforming audit technologies: Business risk audit methodologies and the audit field. *Accounting, Organizations and Society*, 32(4–5), 409–438. <https://doi.org/10.1016/j.aos.2006.09.002>.
- Rose, N., & Miller, P. (1992). Political power beyond the State: problematics of government. *The British journal of sociology*, 43(2), 173–205. <https://doi.org/10.1111/j.1468-4446.2009.01247.x>.
- Roussy, M. (2013). Internal auditors' roles: From watchdogs to helpers and protectors of the top manager. *Critical Perspectives on Accounting*, 24(7–8), 550–571. <https://doi.org/10.1016/j.cpa.2013.08.004>.
- Roussy, M. (2015). Welcome to the day-to-day of internal auditors: How Do they cope with conflicts? *Auditing: A Journal of Practice & Theory*, 34(2), 237–264. <https://doi.org/10.2308/ajpt-50904>.
- Roussy, M., & Brivot, M. (2016). Internal audit quality: a polysemous notion? *Accounting, Auditing & Accountability Journal*, 29(5), 714–738. <https://doi.org/10.1108/AAAJ-10-2014-1843>.
- Roussy, M., & Rodrigue, M. (2016). Internal Audit: Is the 'Third Line of Defense' effective as a form of governance? An exploratory study of the impression management techniques chief audit executives use in their annual accountability to the audit committee. *Journal of Business Ethics*. <https://doi.org/10.1007/s10551-016-3263-y>.
- Sarens, G., Christopher, J., & Zaman, M. (2013). A study of the informal interactions between audit committees and internal auditors in Australia. *Australian Accounting Review*, 23(4), 307–329. <https://doi.org/10.1111/auar.12024>.
- Sarens, G., & De Beelde, I. (2006). The relationship between internal audit and senior management: A qualitative analysis of expectations and perceptions. *International Journal of Auditing*, 10(3), 219–241. <https://doi.org/10.1111/j.1099-1123.2006.00351.x>.
- Sarens, G., De Beelde, I., & Everaert, P. (2009). Internal audit: A comfort provider to the audit committee. *British Accounting Review*, 41(2), 90–106. <https://doi.org/10.1016/j.bar.2009.02.002>.
- Sarens, G., & Lamboglia, R. (2014). The (mis)fit between the profile of internal auditors and internal audit activities. *Accounting and*

- Business Research*, 44(1), 41–62. <https://doi.org/10.1080/00014788.2013.857591>.
- Schein, E. H. (1990). Organizational culture. *American Psychologist*, 45(2), 109–119. <https://doi.org/10.1037/0003-066X.45.2.109>.
- Schein, E. H. (2004). Organizational culture and leadership. *Leadership*, 7, 437. <https://doi.org/10.1080/09595230802089917>.
- Simons, R. (1995). Control in an age of empowerment. *Harvard Business Review*, 73(2), 80–88. [https://doi.org/10.1016/0024-6301\(95\)91624-5](https://doi.org/10.1016/0024-6301(95)91624-5).
- Speklé, R. F., van Elten, H. J., & Kruis, A. M. (2007). Sourcing of internal auditing: An empirical study. *Management Accounting Research*, 18(1), 102–124. <https://doi.org/10.1016/j.mar.2006.10.001>.
- Spira, L. F., & Page, M. (2003). Risk management: The reinvention of internal control and the changing role of internal audit. *Accounting, Auditing & Accountability Journal*, 16(4), 640–661. <https://doi.org/10.1108/09513570310492335>.
- Stewart, J., & Subramaniam, N. (2010). Internal audit independence and objectivity: Emerging research opportunities. *Managerial Auditing Journal*, 25(4), 328–360. <https://doi.org/10.1108/02686901011034162>.
- Townley, B. (1994). *Reframing Human Resource Management: Power, Ethics and the Subject at Work*. London: SAGE Publications.
- Vaivio, J. (1999). Examining “the quantified customer. *Accounting, Organizations and Society*, 24(8), 689–715. [https://doi.org/10.1016/S0361-3682\(99\)00008-2](https://doi.org/10.1016/S0361-3682(99)00008-2).
- Vaivio, J. (2006). The accounting of “The Meeting”: Examining calculability within a “Fluid” local space. *Accounting, Organizations and Society*, 31(8), 735–762. <https://doi.org/10.1016/j.aos.2005.12.007>.
- Vaughan, D. (1999). The dark side of organizations: Mistake, misconduct, and disaster. *Annual Review of Sociology*, 25, 271–305. <https://doi.org/10.1146/annurev.soc.25.1.271>.
- Vinnari, E., & Skærbæk, P. (2014). The uncertainties of risk management. *Accounting, Auditing & Accountability Journal*, 27(3), 489–526. <https://doi.org/10.1108/aaaj-09-2012-1106>.
- Wahlström, G. (2006). Worrying but accepting new measurements: The case of Swedish bankers and operational risk. *Critical Perspectives on Accounting*, 17(4), 493–522. <https://doi.org/10.1016/j.cpa.2004.08.006>.
- Wahlström, G. (2009). Risk management versus operational action: Basel II in a Swedish context. *Management Accounting Research*, 20(1), 53–68. <https://doi.org/10.1016/j.mar.2008.10.002>.