Journal of Management and Governance (2021) 25:475–508
https://doi.org/10.1007/s10997-020-09550-w

# Transparency and accountability influences of regulation on risk control: the case of a Swedish bank

**Shruti Kashyap**[1] · **Einar Iveroth**[1]

Accepted: 11 November 2020 / Published online: 9 December 2020
© The Author(s) 2020

## Abstract

This qualitative in-depth case study explores the influence of financial regulation on risk control within Banque de Montagne, a large listed bank in Sweden. Specifically, the purpose of this paper is to investigate the impact of the European Banking Authority´s Guidelines on Internal Governance (GL 44), through Swedish Financial Regulation FFFS 2014:1, on the bank's risk organization along the three lines of defense model of internal control. FFFS 2014:1 requires banks to reform risk control structures, processes, and roles through a mandated split between the operational risk and compliance functions of the internal risk organization. Through an analysis of 41 interviews, more than 2100 pages of internal and external documents, and over 200 hours of observations from 2015 to 2017, the research identifies the relevant changes to transparency and accountability mechanisms across the three lines of defense within the organization. The operationalization of these concepts through risk control mechanisms is an important consideration for both banks and regulators who rely on the three lines of defense model as an industry-wide adoption for effective risk control. The findings suggest that whilst intra- and inter-organizational accountability mechanisms have strengthened under the changed organizational structure through the implementation of FFFS 2014:1, challenges to effective transparency remain and may have ambiguous consequences for both organizational and regulatory aims

**Keywords** Accountability · Internal control · Regulatory compliance · Risk control · Three lines of defense · Transparency

✉ Shruti Kashyap
shruti.kashyap@fek.uu.se

Einar Iveroth
einar.iveroth@fek.uu.se

[1] Department of Business Studies, Uppsala University, Box 513, 751 20 Uppsala, Sweden

## 1 Introduction

This study addresses the research question of how prudential regulation in the financial sector has impacted accountability and transparency in the risk control and governance mechanisms of regulated organizations. The purpose is to investigate the organizational change process resulting from the implementation of the European Banking Authority Guidelines on Internal Control (GL 44) through Swedish Financial Regulation FFFS 2014:1 (updated) has impacted the risk control organization within a large listed bank with Swedish and international presence. The theoretical framework of analysis is the three lines of defense (3LoD) model of governance and control. The analysis further rests on discussions of transparency and accountability, two central concepts within the text of GL 44 and FFFS 2014:1. These two concepts are also importantly implicated in the risk control improvements highlighted within the broader prudential measures and governance reforms introduced by financial regulatory developments after the 2008 global financial crisis (EBA 2011; Liikanen 2012; Finansinspektionen 2014; Crawford et al. 2017).

After the 2008 financial crisis first reached European shores, the continuing shift towards strengthening regulatory monitoring in the European financial sector is evident through the strong influx of post-crisis EU prudential regulation and the increasingly centralized harmonization of prudential financial supervision within the European Union and Eurozone (Binder 2015). The development and implementation of this evolving regulatory regime is underscored by a heightened post-crisis focus on systemic stability through increased transparency and accountability demands on banks (Garciano and Lastra 2010; Liikanen 2012). Post-crisis regulation has thus broadened its organizational focus to include demands on the corporate governance and internal control of banks (Hopt 2013; Van der Stede 2011). Specifically, the regulatory focus on transparency and accountability has required regulated financial firms to effectuate changes in external reporting whilst simultaneously developing more robust internal frameworks of governance, compliance, and risk control (Bamberger 2010; Hopt 2013).

Within the specific context of risk control, one main aim of post-crisis prudential regulation is to ensure both micro- and macro-stability within the financial sector; that is, promoting the continued stability of individual organizations within the financial sector, minimizing contagion risk between organizations, and maintaining overall systemic stability within the field. Here, in addition to the traditional capital and liquidity considerations inherent in banking regulation and practice, transparency and accountability mechanisms comprise an important portion of the basis for new prudential regulatory developments. Given the importance of banks in financial systems and the often opaque interconnections and risk linkages that often exist in the financial sector, prudential regulation that targets internal control and governance may be understood best as micro-prudential regulation that seeks to ensure systemic stability through promoting the implementation and continued use of effective risk control and resilience measures in individual organizations.

An evolution in how regulators and financial organizations understand the concept of risk in risk management and control is evidenced by the evolving

iterations of risk recognition and control over the past few decades. As recommended by the Basel Committee since the 1980s, the concept of risk in banking has evolved from pure numbers based considerations of capital and liquidity risks, to a broader holistic concept of risk that includes corporate governance considerations, issues of regulatory compliance, and operational factors within the bank (Drennan 2004; Power 2004).

For regulators, this increased reach is founded in arguably well-meaning regulatory aims that nonetheless present an as-yet new testing of the overall regulatory toolkit. For banks, in addition to strategic and competitive concerns, regulations that influence their internal control and governance structures have strong implications for the risk organizations within the regulated firms. Here it is important to recognize that, although banks may vary in their business model mix, all banks function as risk intermediaries and absorb risk through various banking activities (e.g.: corporate loans, financial service provision, wealth management activities, investment trading and trade facilitation through the provision of trade execution and clearing services). Under its own set of organizational constraints, a well-governed bank may well find itself reaping the benefits of sensible risk-taking, provided that it also mitigates negative or downside risks that, if realized, may lead to losses. In order to achieve this kind of effective risk governance, a bank may be motivated to take a proactive approach to identifying, measuring, managing and mitigating the risks with which it contends.

Within the more specific context of GL 44 and the implementation of FFFS 2014:1, the concepts of risk management and control have functionally been cemented further as a set of processes and techniques aimed at two outcomes: first, an explicit alignment between internal control and mechanisms of accountability and transparency; and second, the holistic integration of risk control across the operational and strategic dimensions of the organization. The concept of 'holistic integration' as it applies to risk management and control further develops the traditional view that risk within organizations exists in discrete silos comprised by measurable risks. Under the holistic view, risks such as strategic failures, operational risks, compliance risks, and other forms of risk that may arise unpredictably, have unpredictable outcomes, or otherwise pose a difficulty in being quantified (Mikes 2011, pp. 25–26) are also relevant to the risk management and control activities within organizations.

Such ideas have been evident even before the wave of post-crisis regulatory reform that followed the 2008 financial crisis, with a recognition that risk management involves broader considerations of management control, strategy and market and regulatory factors rather than quantifiable financial measures alone (see e.g.: Spira and Page 2003; Beasley and Frigo 2007; Power 2007). However, research following the 2008 financial crisis more clearly identifies how this initial concept of a holistically integrated risk function within organizartional settings, including the banking sector more specifically, has become more formalized in post-crisis landscape (Mikes 2009, 2011; Giovannoni et al. 2016). The same recognition is also clearly apparent in the 3LoD model, which has gained widespread usage and legitimacy in the years following the financial crisis, and which recognizes the interconnections and in some sense, permeable boundaries between Board functions,

internal audit, internal risk supervision and assessment, and operational activities within financial organizations (Potter and Toburen 2016; Giovannoni et al. 2016; Arwinge and Olve 2017). Nonetheless, insight into the intra-organizational perspective and responses to regulatory developments following the crisis, particularly in the context of risk control and governance models, remains scarce (Crawford et al. 2017).

Where intra-organizational research in the area of financial sector risk management has been undertaken, it has focused on issues of risk control in relation to management control and strategy interactions (e.g.: Arena et al. 2010; Kaplan and Mikes 2012; Mikes and Kaplan 2014; Soin and Collier 2013), governance and performance (e.g.: Iannotta et al. 2007), and how actors and groups within organizations culturally and conceptually respond to changes in risk management within organizations (Arena et al. 2010; Mikes 2011; Giovannoni et al. 2016). Such studies have identified two issues of relevance to the present study: first, the trend towards more holistic integration between risk control systems and the broader management control systems in organizations (Malmi and Brown 2008; Arena et al. 2010; Mikes 2011; Kaplan and Mikes 2012; Otley 2016); and second, the role of structures, processes, and actors in aligning risk control with broader organizational goals and approaches (Mikes 2008, 2011; Kaplan 2009; Kaplan et al. 2009; Arena et al. 2010; Magnan and Markarian 2011; Soin and Collier 2013; Giovannoni et al. 2016). While the influence of regulation on practice is accepted implicitly if not explicitly within these research endeavors, the question of how financial regulation (prudential regulation) impacts risk management and control at the intra-organizational level still remains relatively unexplored (Soin and Collier 2013; Giovannoni et al. 2016; Crawford et al. 2017). This is particularly true across the conceptual dimensions of transparency and accountability, both of which are of recognized importance not only to regulators, but also to organizations within the regulated sphere (Spira and Page 2003; Liikanen 2012). While the relevance of transparency and accountability considerations in the interconnected sphere between risk management, compliance, and corporate governance are well-recognized (Keasey et al. 2005; Short and Keasey 2005; Seal 2006; Power 2007; Bhimani 2009), deeper descriptive studies into the impact of regulation on transparency and accountability in risk control within financial organizations are still lacking (Giovannoni et al. 2016; Crawford et al. 2017). This presents an important research gap that is of interest to regulators, practitioners, and academics.

This paper addresses the identified gap by exploring how a specific regulatory mandate (FFFS 2014:1) has impacted the risk control organization within a large listed bank. Specifically, it looks into the influences of FFFS 2014:1 on the structural, process-based, and actor-oriented role and mechanism changes in the risk control organization of Banque de Montagne. The case study organization is one of the four listed Swedish banks. It has an international presence and has been anonymized to protect its confidentiality.

From a theoretical perspective, this study traces how these changes may be reflected across the dimensions of accountability and transparency within the 3LoD governance model used by financial organizations. The use of this conceptual framing is motivated by the strong focus on transparency and accountability reform as

reflected in financial regulation and policy discussions following the financial crisis. The findings suggest that, while intra- and inter-organizational accountability mechanisms have strengthened under changed organizational structures, challenges to effective transparency remain and may have ambiguous consequences. Although these findings are specific to the case organization in question, the increasingly harmonized approach within both financial regulation and industry practice allow for an extrapolation of the findings to the more generalized context of the EU financial sector.

## 2 The empirical frame

In the wake of the 2008 global financial crisis, a major transparency and accountability development in financial regulation was apparent in the regulatory shift of attention from market efficiency and competition concerns to prudential issues of systemic stability and the organizational management of risk. Consequently, regulatory impact on organizational reporting and control, most importantly in the arena of risk management and compliance has increased (Mülbert and Citlau 2011; Avgouleas and Cullen 2014). An important component of this regulatory reaction includes an enhanced focus on the inner governance and risk control structures of banks. In the EU, there have been many developments addressing this area following the 2007 crisis. Most notably, the shift in regulatory focus towards internal control and governance mechanisms may be seen through new inclusions in the Capital Requirements Directive and Regulation (collectively, the CRD IV Package), recent governance and internal control guidelines issued by the European Commission (Green Paper on Corporate Governance in Financial Institutions and Remuneration Policies), and the 2011 European Banking Authority Guidelines on Internal Governance (GL 44), all of which identified poor risk management and corporate governance infrastructures as important contributing factors to the crisis (Liikanen 2012; Avgouleas and Cullen 2014). These developments are in line with increased regulatory focus on transparency and accountability in the financial arena, and encompass areas of business operations, compliance and oversight, as well as independent assurance through internal audit.

This work takes its empirical point of departure from the implementation and impact of GL 44, enacted in Sweden through FFFS 2014:1. GL 44 follows Article 22 of Directive 2006/48/EC in requiring that all credit institutions possess robust internal control and governance arrangements in the areas of risk management, reporting, accounting, and remuneration, following the same general approach set out in the EC Green Paper and CRD IV. In practical terms, the most direct impact of GL 44 through FFFS 2014:1 has been the mandated split between the operational risk control function and the compliance function at the second line, and the increased delineation between risk management, control, and compliance responsibilities across the first and second lines. What this structural divide means for risk control within banks and how it impacts organizational processes, actors, and activities is still relatively unknown. Below, the empirical foundations of this study are explained in greater detail, beginning with the background and implementation of

FFFS 2014:1, and followed by an explanation of how and why Banque de Montagne was selected as a representative case for this study.

### 2.1 Regulation in action: the background and implementation of FFFS 2014:1

In 2008, a survey by the Committee of European Banking Supervisors (CEBS) on the implementation of internal governance measures in large financial institutions identified the high likelihood of mismatches between institutional and organizational complexity on the one hand and risk management on the other—a factor that was undoubtedly implicated in the financial crisis. Internal governance arrangements in particular displayed notable weaknesses in regard of supervisory oversight, risk management, and internal control frameworks. In 2011, the succeeding body to CEBS, the European Banking Authority (EBA), followed up on this earlier work and issued updated Guidelines on Internal Governance (GL 44) that specifically addressed transparency and accountability structures of internal corporate governance mechanisms across the generally accepted 3LoD model (Fig. 1). Additionally, GL 44 also expanded on the expected role, tasks and responsibilities of risk managers and supervisors within regulated financial organizations.

One of the most notable outcomes of post-crisis GL 44 implementation in EU Member States has been a mandated separation between operational risk control and compliance functions at both first and second lines of defense within banks and other regulated entities. This structural change raises important questions regarding the impact of regulation on the risk management, control practices and role of risk experts in financial organizations. With strong prudential aims of improving trust and stability in the financial sector, the foundation of GL 44 is that "… effective internal governance arrangements are fundamental if institutions, individually, and the banking system, are to operate well" (EBA 2011, p. 7). GL 44 relates weak oversight by the banks' internal supervisory structures as an integral failure that allowed

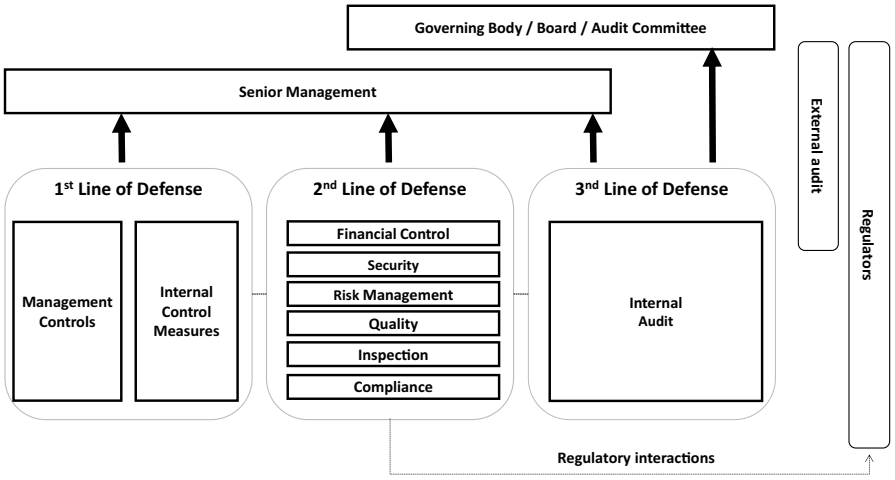


**Fig. 1** The 3LoD model ( adapted from: FERMA/ECIIA 2010, p. 9; IIA 2013, p. 2)

excessive risk taking at both actor and process levels to go undetected. Within the text of GL 44, weaknesses in understanding the complexity of banking and its accompanying risks, and failures in translating such understandings into effective systems and processes were implicated in the overall shortcomings of the internal control and governance mechanisms of banks leading up to the widespread effects of the crisis.

GL 44 has been incorporated into the national Swedish regulatory framework through the Swedish Financial Supervisory Authority's Regulations and General Guidelines regarding Governance, Risk Management and Control at Credit Institutions (FFFS 2014:1). This new regulation has had a significant impact on the organizational reform required of Swedish banks. Most notably, the banks' internal risk-control function, which is directly reliant on the 3LoD model, has faced significant changes at both the first and second line in direct consequence of regulatory implementation. Effective from April 1, 2014, one of the most important developments through this implementation has been the formal separation of the compliance and risk management functions within Swedish financial organizations and the delineated responsibility of the Board in connection with each function (SFAS 2014).

In terms of transparency and accountability developments, in addition to the impact of FFFS 2014 itself, it is important to understand the increased role and supervisory authority of the Swedish Financial Supervisory Authority (FSA) in relation to Swedish banks after the financial crisis. Beginning in 2009, the authority of the FSA expanded to cover banking activities in the areas of anti-money laundering (AML) and counter-terrorism financing (CTF). In 2013, these supervisory powers were expanded further to include prudential oversight authority in the areas of commercial lending and other banking activities. This increased scope of oversight has had three implications: first, this has made the FSA more authoritative in its monitoring the activities of banks, reducing the scope and potential for self-regulation by banks. Second, the increased authority of the FSA has come with corresponding obligations for the FSA itself to report and be accountable to the government and Riksbank to a higher degree than before. Finally, as the Swedish financial regulations mirror EU regulations and directives, this has meant that the activities of the Swedish FSA are in close alignment with EU developments.

These changes to transparency and accountability interactions through closer alignment with EU regulations have come with their own set of challenges in translation to action. In its most recent response to updates to GL 44 for example (SBA 2017, p. 3), the industry representative agency, the Swedish Bankers Association (SBA), stated in representation of the interests of Swedish banks that it "believes that the draft guidelines in some parts are too detailed and therefore too restrictive. A fundamental problem is the lack of a clear breakdown of the requirements stipulated for the management body on the different parts of the management and the board in relation to the various corporate structures within the EU. Even though the guidelines do not advocate any particular structure and are intended to embrace all existing governance structures it appears to miss the aim to create a guidance that easily can be applied to all sorts of governance structures". Specifically with regard to the complex challenges of adapting internal transparency and accountability mechanisms to align with new regulatory demands on actors and processes, the

SBA (2017, p. 8) provided a detailed identification of issues that could impede intra-organizational governance and control.

Given the reach of FFFS 2014:1 into the risk control structures, processes and roles of risk control and compliance within banks, it is instructive to take an inside perspective on how the influence of this regulation plays out in practice. Hence the selection of a representative case to illustrate and explain the influence of this regulation on the risk control and compliance function within banks. The empirical setting of the Swedish banking sector and the selection of Banque de Montagne as a representative case are explained in the following section.

### 2.2 Banque de Montagne

As is the case in most if not all economies, the health and scope of the Swedish banking sector is strongly linked with the economic growth, stability, and performance of the Swedish economy as a whole. Since the late 1970s, the Swedish financial sector saw the same deregulatory cycle and technological advancements as other Western economies at the time, with the result that the Swedish banking sector expanded considerably during the 1980s onwards. At the same time, the market concentration of the Swedish banking sector also narrowed, particularly after the banking crisis of the early 1990s. By the time of the 2008 Global Financial Crisis, aggregate bank assets amounted to approximately 370% of the national GDP, with the four major (listed) Swedish banks of Handelsbanken, Nordea, SEB and Swedbank accounting for over two-thirds of all lending and bank deposit activity in the country. All four listed banks also exhibit complex and widely spread organizational structures thanks to their long history of merger and acquisition activities, and their strategic spread through the Nordics and Baltics, particularly in the years following the 1990–1992 banking crisis in Sweden (Larsson and Söderberg 2017).

As a precursor to the in-depth case study described in Sect. 3, the researchers first conducted interviews with three of the four listed banks in Sweden, the Swedish Bankers Association and the Swedish Securities Dealers Association. Based on the pilot study, the researchers decided that the research question of how prudential regulation in the financial sector has impacted accountability and transparency in the risk control and governance mechanisms of regulated organizations would be best answered through a case study of a representatively large and complex listed domestic bank with a strong international presence and adherence to EU financial regulations and guidelines. The compliance function selected as the focal point for the inquiry, given that this function is the first point through which such organizations make sense of the regulations that they must comply with. It was determined that any of the largest four listed Swedish banks would serve as a suitable representative case for the study. Banque de Montagne, as one of the four listed banks, was thus selected for the case study.

Although compliance was a well-established function within the bank even prior to the implementation of FFFS 2014:1, it existed largely in combination with operational risk management within different business units and along different areas of banking operations. This represented a more dispersed format rather than the

consolidated and independent function called for under FFFS 2014:1. In addressing this call for regulatory implementation, the bank was, in effect, building up a newly reformed risk management structure through the formal separation of operational risk and compliance functions, and the establishment of an independent second line compliance function. Thus, as the compliance function represented the more directly reshaped formal function in consequence of FFFS 2014:1, a determination was made that this would provide a suitable opportunity to observe the direct influence of regulation on organizational structures, processes, and action.

We formally approached Banque de Montagne in September 2015 in order to initiate a case study with their newly formalizing independent compliance function. A confidentiality agreement between the bank and the researchers was signed at the end of October the same year, initiating a deep and open research access into the bank. The findings and analysis of this case study are presented in Sects. 5 and 6 of this paper, respectively.

## 3 Methodology

This research applies an in-depth single-case study design (Yin 2003; Eisenhardt and Graebner 2007) to trace organizational change in response to regulatory influence, by taking a longitudinal process-oriented perspective. Specifically, we ask how the implementation of the EBA Guidelines on Internal Control (GL 44) have impacted the risk control organization within a large and complex bank that is subject to the specific regulation issued in Sweden (FFFS 2014:1). A qualitative research design is considered an appropriate choice when the phenomenon under investigation is one that requires thick, descriptive, contextual, and real-time data (Bryant 2006) to capture a moving target of sorts—a contemporary and ongoing phenomenon (Yin 2003; Bryant 2006; Eisenhardt and Graebner 2007). Regulatory reach into the internal control mechanisms of financial organizations and the creation of a reshaped risk organization in response to regulatory demand comprises such a phenomenon. It is thus well-suited to the in-depth case study design adopted here.

The revelatory nature of case studies in general (Yin 2003) represents an aspect of this methodology that contributes in an especially useful manner to the field of banking research. To date, there are relatively few qualitative studies that provide insight into the inner workings of banks, particularly in the context of transparency and accountability in the context of risk control (Crawford et al. 2017). This case study thus provides a unique opportunity to obtain deep insights from within the risk organization of a large bank in a context and manner that has earlier largely been inaccessible to researchers.

In endeavors such as this, the strength of a qualitative case study approach rests not on uniform methodological applicability across different scenarios, but rather on the affordance offered by the case study method to understand the contextual meaning of the specifically studied phenomenon in a flexible, reflexive, and tailored manner. Whilst generalizability in a strictly methodological sense is not possible to achieve through such an approach, the richness and specificity of the method allows for a much deeper understanding of the phenomenon, which in turn can be

extrapolated to more general theoretical insights and, arguably, practical applicability based on the similarity between large international financial organizations and the supranational regulatory landscape they share (Lee and Baskerville 2003; Yin 2003).

### 3.1 Data collection

As stated in Sect. 2.2, a confidentiality agreement and formal access to the bank began in October 2015. Data collection through interviews started in the beginning of 2016. The interviews also provided retrospective information concerning the 2014–2015 time period. Furthermore, access was granted to internal documents such as training reports and meeting minutes, which served to build a retrospective and real-time account of the bank's response following the implementation of FFFS 2014:1.

Given the formal split between compliance and operational risk control functions under the mandate of FFFS 2014:1, the depth of investigation and the time-sensitive nature of data collection in a real-time context meant that a choice had to be made between focusing on the reshaping formal compliance function versus the operational risk function of the risk organization within Banque de Montagne. As the focus of the study was on regulatory impact and that the compliance function was the natural starting point of how regulatory demands were translated into organizational understandings, we decided to focus on the compliance function. A natural limitation introduced by this approach was that a deeper insight into the operational risk component of the organization was lost. In consequence, although theoretical and empirical saturation was reached, this saturation cannot be said to encompass the entirety of the organizational risk function. Some elements of intra-organizational interactions, tensions, and synergies thus undeniably remain outside the scope of this work.

The empirical data gathered consists of three sources: 41 semi-structured interviews with 23 interviewees, over 2100 pages of internal and external documents, and over 200 h of field observations across four Nordic countries. These materials represent retrospective accounts and the ongoing change developments within the organization, covering a time-period of 2014–2017. Some of the interviews covered more general understandings of risk identification, control, and regulatory compliance, as well as a more historic view towards the development of risk control in Banque de Montagne. Each interview lasted on average between 45 min and 2 h.

The first interviewees were identified in 2015 by the key contact who granted access, who then suggested additional interviewees. The interviews focused on broad key themes that were developed both from a priori theoretical areas (e.g. legal developments as causes for internal changes, reflexive understanding of transparency and accountability in relation to risk control,) as well as key empirical determinants of the organizational change that gradually emerged out of the empirical data (e.g. components of risk control activities and understandings from the organization's multi-level perspective). The semi-structured nature of the interviews entailed an adjustment to the setting of each interview and the insight of each interviewee.

The interviewees consist of members of the Executive Management team, the change management team, and compliance officers in different field offices, representing a holistic, multi-level perspective from within the compliance unit of the risk organization.

The second source of empirical data consisted of more than 2100 pages of internal and external documents. These were of six types: planning and guidance documents, training materials, strategy documents, organizational & policy documents, operational documents, and external documents (annual reports 1992–2018, news articles 1992–2018, legislative texts and policy documents 1986–2018). The documents enabled the researchers to trace earlier discussion about risk control and, following the regulatory mandate in 2014, how compliance activities and the formation of the group compliance function later became a more structured part of the risk organization.

Finally, observations were performed in 2016 totaling over 200 h at the different sites. These included mainly non-participant observations of the following activities: final rollout at four different field offices (with the executive management group representative, supporting staff, and external consultants), three full days of training sessions, planning and steering meetings led by the executive management team of group compliance, and planning meetings between those in charge of specific components of the change process. Overall, the observations provided a deeper understanding of both the emerging identity of the compliance function and how transparency and accountability featured among their risk controls. In doing so, these observations served as additional properties of richness (Weick 2007) to the primary data-sources of interviews and documents.

### 3.2 Data analysis

The analytical process was executed concurrently with data collection. The analysis process consisted of three phases following a cyclic trajectory with attentiveness to both similarities and dissimilarities in theory and data (inspired by Miles and Huberman 1994; Kvale and Brinkmann 2009). Data collection was performed until saturation was deemed to have been reached.

In the first phase, the patterns in the data were open-coded into descriptive categories. These codes consisted of key phrases and terms uttered by the interviewees. For example, references to specific regulations as they talked about the ongoing change process within the risk organization as well as specific areas of risk control (such as Anti-Money Laundering and Know Your Customer requirements). The coding was inductive in nature and focused on the key themes that recurred within and across the different data sets. For example, it consisted of patterns of what the participants believed to be issues of concern, such as risk taxonomy, process design and structural components of the compliance function.

Conducting analysis is an attempt "to achieve a practical middle ground between a theory-laden view of the world and an unfettered empiricism," (Suddaby 2006, p. 365). Accordingly, the open-coding procedure inspired the second more deductive phase of studying theory related to the emergent patterns in the data. This theoretical

reflection was initially broad (e.g. transparency and accountability) and later more focused (e.g. the qualitative aspects of these concepts—for example information overload, intra- and inter-organizational reporting, and interactive accountability within the organization and between the organization and regulators). Finally, the data were recoded into narrower conceptual categories, for example, nominal transparency, retrospective transparency, and real-time accountability. The understanding gained from the open coding, concurrent data collection, and theory insights from phase two influenced this third phase. This re-coding procedure was conceptual, and less broad and inductive compared to the open coding.

A three-fold strategy was used to establish reliability and validity. First, method triangulation between the interviews, observations and documents was deployed to achieve validity and avoid confirmation bias. Second, feedback meetings with five interviewees (composed of the key-personnel of the entire change process) were conducted, where the emergent findings were discussed with the most significant interviewees. Third, bearing in mind that rigorous research should strive for reliability across settings, interviews and observations were performed at four different sites throughout Scandinavia and at different levels of the risk organization during the last part of the study.

## 4 Theoretical and conceptual background

The background of this paper is based on two sets of conceptual developments that link banking regulation with practice. The first conceptual development is the introduction and assimilation of the 3LoD model of organizational control that has largely set the current industry and regulatory standard within the banking sector. The second development is the understanding of the dynamic relational concepts of accountability and transparency as they emerge in intra-and inter-organizational interactions within the financial sector.

### 4.1 The three lines of defense model

The 3LoD model may be understood as a model of intra-organizational risk ownership, control, and assurance (Arwinge and Olve 2017). With its origins in practice traceable to the 1990s, the 3LoD model has been both referenced and relied upon in policy guidelines issued by Bank of International Settlements (BIS) through the risk control frameworks put forth in the Basel Agreements and corresponding guidelines (BIS 2011), the guidelines for internal governance issued by the EBA that form the direct empirical line of inquiry for this paper (EBA 2011), and the Committee of Sponsoring Organizations of the Treadway Commission (COSO) in their updated framework on internal control (COSO 2013; Anderson and Eubanks 2015). Its use within the financial sector is thus well recognized, established, and uncontested (Arndorfer and Minto 2015; Decaux and Sarens 2015).

The concept of "internal control" as an activity / outcome that traverses all levels of the organization is described explicitly in the Guidelines on Corporate

Governance Principles for banks, issued by the Basel Committee in July 2015. Specifically, these guidelines identify that it is not only individual business units (the first line of defense) but also the organization´s second and third lines of defense as well as the management body that are collectively responsible for the organization´s "internal control" (BIS 2015). As a system of internal governance and control, the normative 3LoD thus encompasses considerations of organizational as well as environmental complexity. The model additionally recognizes how technological progress and shifting market landscapes have increased the variety and complexity of risk factors that banks are exposed to (Westman 2011). The model also encompasses a conceptualization of how these risks are managed within organizations of increasing size structural intricacy, and internal complexity of integrated control systems. Banks are additionally subject to agency and moral hazard considerations that are themselves complex and often opaque. These add to the complicated nature of internal control within banking. The model is presented in Fig. 1, although as the findings of the case study show, the delineations between control activities and measures are not as clearly separated or defined as the model would suggest.

It may also be important to note that in Fig. 1, the first line of defense includes not only internal control, commonly in the purview of compliance, but also management controls. Even prior to the implementation of FFFS 2014:1, risk control in banks generally relied on distinct controls for compliance and operational risk albeit without the formal separation between these two functions. In stressing the importance that *all* controls will be important for risk management, the 3LoD model when applied to banks teaches us to include a broad scope in investigations of how regulation will impact behavior through the *joint* impact of both management controls and internal control measures. In this context, the paper represents one part, or perhaps a first step, in a more detailed investigation into regulatory impacts on risk control in banks.

While in-depth empirical research into the workings of the 3LoD model remain few at the time of this study, conceptual discussions and analytical interpretations of the model do exist within the Scandinavian management stream of literature (see e.g.: Arwinge and Rost 2013; Arwinge and Olve 2017). Within this stream as well as the broader European corporate governance literature, there is recognition that what the 3LoD model touches in both direct and indirect fashion are the lines of accountability between different levels of organizational activity, and between the organization itself and its stakeholders (Hopt 2013, 2015; Arwinge and Olve 2017). In the context of risk control, there are two underlying assumptions that must be acknowledged in the current European guidelines and Swedish regulations, representing areas of potential tension and gaps between regulation and practice: First, at the EU level, rules outlining best practices for Board and management-level monitoring over the internal control and risk management systems often presuppose that a state-of-the-art risk management system is already in place within the organization, or that such a system can be seamlessly enacted within a reasonable and relatively short-term period of time. Secondly, in terms of business strategy and operations, there tends to be an assumption of correspondence and alignment between the risk, business, and strategy profiles of the financial organizations under supervision,

based primarily on historical accounting and performance data indicators of these organizations.

One further consideration for the impact of corporate governance regulation and organizational practice is that, regardless of the level of uniformity or harmonization at the EU level, recommendations or rules regarding corporate governance, jurisdictional differences are going to continue to exist in regard of board structure, monitoring control, stakeholder protections and institutional structures (La Porta et al. 1998; Shleifer et al. 1999). In this regard, a relatively recent article by Hopt (2015) identifies that where the setting up and implementation of internal control systems is primarily a task of management, either by law or in practice, the board must be aware that managers often underestimate risks. However, one may rightly question whether the board is positioned to effectively carry out such a check, since it is admittedly very difficult to identify unlikely or improbable risks *ex ante*. Additionally, detailed questions about risk can only be asked by management and not the board members themselves—a factor that introduces another potential area of misalignment in between strategic control at the board level and operational control at different levels of management.

To resolve the potential misalignment in intra-organizational risk monitoring and control, additional checks and risk assessment procedures are often built in within the board structure. For example, through a legal requirement for a separate audit committee at the Board level, which may require particular or specific areas of financial expertise; through the inclusion of a specific and independent risk committee at the Board level (as is the case in Sweden); and also ultimately through an independent internal audit function within the organization (the third-line of defense) and periodically mandated external audit.

### 4.2 Transparency and accountability: an internal governance perspective

This paper subscribes to the concepts of transparency and accountability in line with the following definitions: *Accountability*, as it surfaces in the regulation-practice interface of banking, may be understood broadly as "the giving and demanding of reasons for conduct" (Roberts and Scapens 1985, p. 446). In a more expanded form, accountability may be understood as a reflexive connection, relationship, or relational construct between the actors that demand accounts and the actors that provide those accounts. These actors themselves are normally bound in a duty-based relationship, that may be subject to either formal or informal mechanisms of verification and enforcement.

An accountability relationship between actors may arise in either an intra- or inter-organizational context. In the case of risk control within the financial sector, accountability relations within the regulation-practice interface are often intertwined due to the nature of bank regulation and supervision. For example, structures and actors within the risk organization of a bank may be responsible for intra-organizational responsibilities across vertical and horizontal dimensions as well as responsibilities and direct interaction/ accountability towards regulators as well.

*Transparency* may in turn be recognized as a similarly information-based and relational construct, which may exist within specific accountability relationships as well as independently. Effective accountability rests, in a very real sense, on effective transparency; that is, the provision of relevant and timely information in a manner that is accessible and understandable to the recipient, and accurately captures the phenomenon or information that is demanded. In the intra-organizational context, issues of effective transparency (as linked to accountability structures) emerge at both report issuance and process design levels, with the risk that either issued reports or designed processes fail to achieve effective transparency in their design and output.

In the corporate governance context, the concepts of accountability and transparency may be understood to be reflected through activities and systems of reporting, decision-making, and roles or responsibilities of specific actors and functions within the organization (Davies and Hopt 2013; Arwinge and Olve 2017). Who is responsible for what, how these responsibilities are fulfilled, and how effectively the fulfillment processes and outcomes are communicated vertically (and where appropriate, horizontally) form the basis of transparency and accountability channels within the organization. Additionally, these same relational attributes between the organization and external parties, in this case regulators, set the basis for accountability across inward (regulatory accountability and transparency to the organization,) and outward (organizational accountability and transparency towards regulators) dimensions, as illustrated in Fig. 2.

One important facet of accountability and transparency is the notion of nominal versus effective mechanisms and outcomes of accountability and transparency interactions (Heald 2006; Hood 2007). What is meant by this distinction is that transparency (or accountability) is only effective, rather than merely nominal, if it is timely, accurate, useful, and understandable to its recipients such that it provides them with the relevant information necessary to act, verify, or enforce.

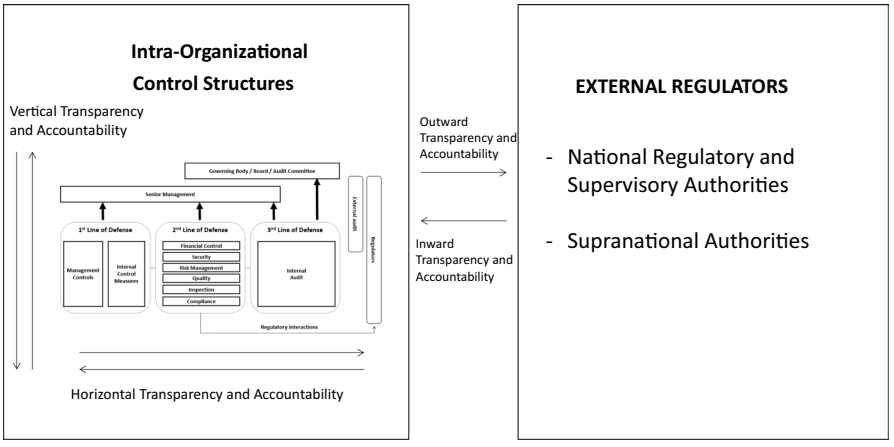


**Fig. 2** Dynamic transparency and accountability: inter-organizational and intra-organizational levels ( adapted from: FERMA/ECIIA 2010, p. 9; IIA 2013, p. 2)

In the context of both inter- and intra-organizational transparency and accountability, a certain level of uniformity in intra-organizational understandings and communication is necessary to form the basis of effective control and communication across all dimensions of corporate activity, including in the context of risk control. Here, it is perhaps useful to note that risk control activities and the effective communication of these activities, processes, and outcomes depend in large part not only on *individual* understandings and actions, but also on a *harmonized organizational understanding and communication of* different risks and uncertainties as they relate to the organization through its contemplated and realized choices and actions. Within the 3LoD model, this interaction between intra-organizational systems and actors is important to bear in mind in the context of accountability and transparency, as discussed in Sect. 6.

## 5 Findings

For the risk organization within Banque de Montagne, the influence of FFFS 2014:1 triggered a change process composed of a number of activities that took place between October 2014 and June 2017. As the process of investigation that uncovered the identified organizational activities followed an iterative and concurrent process of data analysis and data collection, an overview of the change process and the resultant activities are first presented in Sect. 5.1. After this, Sects. 5.2 and 5.3 delve deeper into the individual phases of the change process. Both the conceptual framework of the 3LoD, and the operationalization of accountability and transparency have shaped the analysis as well as the presentation of the findings in Sects. 5.2 and 5.3. Within these latter two sections, the presentation of the findings attempts to highlight the importance of understanding that accountability and transparency may operationalize at the structural, process, and actor levels through hierarchical and horizontal monitoring, reporting, and decision-making response systems and processes as well as the roles and responsibilities of specific actors and functions within the risk organization as a whole and the compliance function in particular.

### 5.1 An overview of the change process within Banque de Montagne

One way of understanding the organization´s response was through a classification of these activities into four phases, summarized in Table 1.

### 5.2 Phases 1 and 2: initial understandings and translations within the risk organization

The five main areas of activities that emerged in Phase 1 and evolved through Phase 2 are outlined as follows:

**Table 1** Overview of the change process

| Phase | Recurring activities |
|---|---|
| Phase 1, October 2014–December 2015: initial organizational response to regulatory demand | The creation of a new 2L[a] group: compliance function, definition of roles at 2L, and identification of broad areas of overhaul, the creation of risk compliance channels at the BoD level |
| Phase 2, December 2015–March 2016: refining organizational understandings of the risk control function and the goals of the risk organization within the bank | Narrowing the scope of process activities at the group level, collecting data and analyzing inputs from 1L, refining/revising the risk compliance presence at BoD and lower vertical levels, refining understandings of the role of compliance in the risk control function of the bank. This was the "testing" phase, where new units were created and new architecture was built, not all of which survived through phase 3 and 4. What did not survive did not disappear completely, but was to some extent or another subsumed within new categories and structures, or else removed to more general control structures within the bank (outside of the scope of compliance, but with links to compliance) |
| Phase 3, March 2016–September 2016: Translating organizational understandings, into concrete responses regarding structures, processes, and roles within the risk organization | Further translating regulatory demand into specific areas of overhaul; refining the content/ channels, identifying explicit and implicit links with 1L, and opening new areas for further development between 1L and 2L in specific risk areas, finalizing centralized risk compliance rollout; very importantly, building up a concrete and formal centralized infrastructure of systems and processes by which 1L and 2L compliance activities were linked |
| Phase 4, September 2016–June 2017: Formal rollout of the compliance framework, and the invitation of feedback from Compliance function representatives at all foreign offices and business units in order to further refine the framework | Rollout of compliance risk framework at field offices—communication between 1L and 2L through training and communication sessions; collection of feedback from 1L and field offices, gathering information for further refinement of the compliance risk function (this later development is outside the scope of this study). This was the first time that the formal outcomes of Phases 1–3 were presented in an international/ multi-level context through the rollout/ training meetings at the four different field offices |

[a]1L and 2L refer to the first two "lines" in the 3LoD model

### 5.2.1 Risk analysis

Risk analyses were performed within specific risk areas with the aim of identifying the risk of non-compliance within those areas. In an interview with the head of compliance monitoring on March 10 2016, the interviewee identified that based on the themes of regulation, it was important for those building the compliance function to understand how these regulatory themes impacted risk areas, and what the highest

inherent risk factors were within those areas. During that interview as well as subsequent interviews and observations, what emerged through retrospective accounts was that a lot of understandings regarding how to identify risks were based on regulatory demand at the outset. Following the call of the relevant regulation in areas such as Know Your Customer (KYC), Anti Money Laundering (AML) and Counter Terrorism Financing (CTF), the structured evaluation of non-compliance risks in these areas depended on some formula of professional (non-legal) judgment, but was still highly reliant, at least at the first and second phases of this study, on the call of the applicable regulations.

### 5.2.2 Control design analysis

Control design analyses were performed to identify how first line controls fit with second line monitoring activities. During the first phase, this was a highly theoretical exercise, as the compliance function was still in the process of building the second line function. Thus, alignment with first line was more based on the ideal of building a process/ system of monitoring and oversight that would aid first line operations on the business activity side through project management in specific risk areas or functions, expertise building through training activities, and quality assurance through second line functions. In this way, a strong vertical downward link was envisioned and effectuated between second line and first line functions, although the second line was clear that ultimate risk ownership rested at first line, with individual business units.

What this meant, essentially, was that risk *management* was not possible through the compliance function. However, the second line was responsible for *control* through monitoring processes and *quality assurance* through an analysis of the match between intra-organizational activities and regulatory intent. In an upward vertical direction, there was a strong recognition of the need of the senior management and Board to have clear and comprehensive reporting of the risk control analysis and outcomes at both first and second lines, in order for an adequate alignment of the risk control function with the overall risk appetite and risk-based strategy of the bank. Here, one important task for the second line at stage 1 was identifying extant gaps between regulatory aims, the risk control aims of the bank, and the higher-level strategic trajectory and risk appetite of Banque de Montagne as a whole.

### 5.2.3 Operational effectiveness

Analyses of operational effectiveness regarding the compliance design were in strongest focus across horizontal interactions between the first and second lines of defense. Analyzing operational effectiveness occurred in tandem with the control design analysis, and consisted of a series of design tests to anticipate actual alignment outcomes between the operational processes under design and translations to risk appetite levels and risk mitigation within specific risk areas (e.g.: AML, CTF, etc.). Here, there was an implicit link between the compliance function, rooted in risk control, and the strategic alignment of risk management with business activities at first line.

#### 5.2.4 Reporting and alignment

Another major activity was reporting and alignment of functionality, form, and process across horizontal and vertical levels. Here, the link to the control design area was an ongoing process-based second line assessment of how effective the design development was, which gaps and misalignments were being mitigated, and where areas of misalignment and challenges for adequate development still remained.

In a sense, this amounted to self-assessment based on feedback from vertical dimensions at the board level, the third line, and the first line. Additionally, coordination with operational risk, the parallel second line risk organization to compliance, was also anticipated. What was also strongly recognized here was that risk reporting should be delivered not just to the Board but also to the first line risk owners who would best be able to manage those risks. In this regard, there was a strong recognition of the potential need for appropriate action plans originating at first line levels, which the second line could provide oversight and approval for, in order to enhance the alignment across first and second lines with the Board.

#### 5.2.5 Refinement

The refinement of specific issues was executed through follow-ups and overall system design adjustments between the first and second lines of defense. This last area was tied directly to reporting and alignment. It addressed the processes through which specific risk issues could be logged, analyzed, addressed, and resolved across first and second lines. The alignment between specific business areas and the second line was identified as being especially important for an effective and resilient system of risk control to be achieved.

The vertical link here was that business units at first line should be aided in developing a report functionality that both logged appropriate risks and provided the appropriate evidence of those risks being resolved once addressed. Second line, being responsible for monitoring first line outcomes and assessing them in term of regulatory and organizational compliance aims, would have to build adequate and accurate systems of aggregation and analysis to understand the risks. The quarterly and annual reporting to the Board from second line would necessarily build on all monitoring of first line risk control outcomes and would thus need to convey accurate understandings of the outcomes at the first and second lines of defense.

### 5.3 Phases 3 and 4: refining and translating organizational understandings

During these last two phases studied, the focus was building an action plan leading up to a framework that addressed the areas identified in Phase 1. What emerged during Phases 3 and 4 was a narrowing down of organizational development to the core functions of the second line that spanned the five areas identified in Phases 1 and 2. Consequently, the broad areas of organizational focus and development evolved from the broader contexts of risk analysis, operational effectiveness, and so on into

more detailed and activity-oriented components during the last two phases. During the last phase (Phase 4) of the study, the framework of the compliance function was formally presented and disseminated across the international offices of Banque de Montagne by the end of 2016. During the rollout process, the following core functional areas were formalized, with important connotations for *structure*, *process*, and *actor* perspectives, as presented below:

### 5.3.1 Risk identification and assessment

*Structurally*, this core function represented the common language of understanding risk across the risk organization. Risk identification and assessment emerged as both a top-down and bottom-up engagement, with the need for clear structures and channels between the Board and second line, as well as between second and first lines. At the same time, there was a strong delineation between compliance and operational risk at second line, and Business risk assessments at first line. One explanation for this was that the second line had to take in not only formal regulatory compliance considerations, but also in some sense regulatory aims (in principles-based regulation). Thus, structurally, independence was extremely important in risk identification and assessment under the compliance function. At the same time, it was equally important for there to be a common risk language for communication and understanding how risk existed and was being handled across the entire bank. In this sense, identification and assessment seemed to span all three lines of defense, although it was technically an independent second line function within the compliance function. What was importantly reiterated during these latter two phases of the study was that that risk *ownership* still rested at first line, underscoring the importance of coordinated understandings and activities between how the compliance function engaged in risk identification and assessment, and how this linked to first line activities and understandings.

Across the *process* dimension, the importance of a principles-based approach and convergence between regulatory and organizational aims was highlighted. There were over 1000 risk descriptions in the system as of the end of Phase 4. Around two-thirds of these centered around one specific risk area: AML.

AML remained a high priority area of focus for Swedish regulators as well as Banque de Montagne, given the number of regulatory violations that the Swedish banks had incurred in recent years. There were extremely strong links to the other core processes, as the risk identification and assessment function was involved to some degree in all of them. What was of particular interest regarding the risk ID and assessment function was that even when gaps in the function were identified, the regulatory consequences of this were not always clear. For example, if the organization flagged internal shortcomings to regulatory authorities, they might get a "stay of execution" on penalties; however, if resolution was not achieved in a timely fashion even with good faith efforts to reform any known shortcomings, the organization could face even higher penalties as a result.

From an *actor* perspective, second line actors identified a need to be clear on the role and "language" of risk. In this sense, the delineation between compliance actors and other risk actors (primarily operational risk actors) emerged as important. While

both functions shared a second line responsibility for risk control, it emerged that understandings of risk could differ between operational risk, which is mainly tied to capital adequacy controls, and compliance, which is broader and in one sense 'fuzzier' as it involves direct regulatory requirements/ mandates as well as an interpretation of broader regulatory aims.

For both the process and actor dimensions, it was identified as extremely important for compliance to stake out its position at first line in regard to how risks are understood and that there is a shared understanding.

### 5.3.2 Risk monitoring and reporting

*Structurally* speaking, the monitoring function emerged as responsible for risk prevention and the beginning of mitigation where potential and realized risk events were discovered. A triangulated analysis of the interview and observation data together with the internal documents that reflected the change process collectively yielded that individual actors and decision-makers had constructed a clear understanding that good monitoring could not by itself mitigate or prevent risks; rather, the role of the monitoring and reporting function was understood as being to identify and highlight known, realizable, and also already realized risks at the system and event levels. Once such risk events were identified by the monitoring function, actors would need to reply on other core functions such as training or advice to improve the organizational risk control activities and to effectively address the existing risk issues.

In the above context, the main delineation that arose was between second line and third line, as it was primarily these two lines that were responsible for broader "monitoring" functions. The distinction of the compliance function in this regard was that compliance at second line was responsible not just for reporting its monitoring findings, but also for issuing advice on how to resolve potential issues. Internal Audit (third line) was not responsible for advising or recommending any changes.

The *process* of monitoring could be broken down into three steps: first, an analysis must be conducted to determine the motivation and scope of the monitoring activity. Next, a control design analysis must be conducted to identify existing controls, evaluate the effectiveness in identifying and mitigating non-compliance risks, and making testing decisions to see how the extant controls work in practice. Finally, if the existing controls were found to be inadequate, an appropriate response of situation-specific advice could be initiated.

The second step of control design analysis and testing followed a flow-chart assessment process: First, were controls working as designed? If yes, was the design itself effective? If unclear, the design could be tested through data samples available through internal information reporting. Additionally, independent tests could also be conducted to understand how certain activities or events were occurring within the organization or by the organization in response to external events. These independent tests could then be linked to advice-giving needs but could admittedly also fail to provide assurance in all situations.

The link between monitoring activities and regulatory interactions/ demand where considered to be particularly strong, as the monitoring capacity and capability

of the bank is what allows it to respond to regulatory demands. With a strong link to internal rules, one interesting perspective that emerged through the interviews and observations was that there are certain informal controls that may emerge at first line (such as, for example, managers not doing/ doing certain things so that their bonus structures are not negatively impacted). These were understood to be indicative of weak control systems, but it was also acknowledged be difficult to identify and document.

From an *actor* perspective, the following understandings emerged: monitoring in general has a high reliance not only on documentation but also on professional knowledge and judgment. It is possible to monitor *some* activities even without formal templates. However, even where professional judgment plays a large role, documentation remains important for compliance actors to file and review. Any monitoring assurance offered and any actions originating from the first line should be documented to build an overall "map" of organizational activity.

With a strong link to internal rules, what seemed important in regard of monitoring was that good guidelines by themselves were not enough to ensure sound monitoring; how actors conducted themselves according to the guidelines matters a lot. Even so, actors within the compliance function seemed to hold a clear understanding that identifying direct causal links between actions and outcomes was often tricky at best, particularly in the context of compliance. In this context, the need for testing and the strong link between *actors* and *process* was expressed.

Both the observations and interviews in the third and fourth phases indicated that there was a strong sentiment that there was a need for more informed selection of the technological systems they used. At the same time, the compliance function also accepted that there was a need to look into *what was making the selected system challenging*—was it a poor understanding or application, in which case the compliance function faced the challenge of adapting to the system? Or, was it that the system was a wrong fit, in which case the selection of a new system was more justified? During the time of this study, the answer to these questions did not emerge in full. Yet, what the discussions and the change process itself highlighted was a subtle awareness of the compliance function´s resource dependence as well as its mandated focus on risk control, even if this entailed higher costs.

### 5.3.3 Oversight and advice

*Structurally*, this function of risk control extended across first and second lines, and across different areas of risk activity across business units and activity type. On a *process* level, an important recognition was that advice was not necessarily always proactive. In some cases, such as with the introduction of a new system or activity within a new or previously unrecognized risk area, advice could also be reactive.

For *actors*, in determining what compliance officers and second line compliance actors were responsible for, there emerged distinctions between different business areas and between the types of situation on which advice was being sought. In addition to analyzing the nature and complexity of the advice needed and the actual process of communicating and following up on that advice, compliance officers also

needed to know when to refer cases to the operational risk units, or other units outside the compliance function.

### 5.3.4 Internal rules of compliance

The *structures* of internal rules of compliance were largely based on documentation of applicable policies, procedures, and guidelines for corporate activities. In that sense, they were established along the line of forming a foundation for all corporate functions, and in some sense the organizational identity of Banque de Montagne itself. The internal rules of compliance were very much a second line compliance responsibility in terms of creation and oversight but extended to first line in terms of required inputs and activities. The objectives of the Internal Rules function were to provide quality assurance of compliance structures, processes, and activities with internal and external requirements, and to keep a track of incidents/ deviations from what is "normal" or "expected". In this regard, it is important to note that all *identified deviations* from internal rules did not necessarily amount to actual *breaches* of internal rules, so the compliance function retained a degree of flexibility in expert analysis of organizational activities in this regard. Relatedly, although other core processes were also responsible for reporting *deviations*, it was the responsibility of the Internal Rules function to identify *breaches*.

At the *process* level, internal rules covered two types of areas: (1) licensed activities, comprised by specific regulatory areas such as AML, conflict of interest, conflict of conduct, and detailed guidelines thereon; and (2) processes and roles owned by the second line compliance function.

There were basically two process components of Internal Rules within the compliance function, including for the core functions. First, regarding the regulatory areas, a defined scope of risk area documents that established how specific risks are managed in line with compliance requirements. These stretched across the organization at all level and were divided by risk area dependent on regulatory demand. So, for example, rather than being split by business area, these risk area documents could be specific to AML/CTF policies, conflict of interest guidelines, investor protection guidelines for different financial products, and so on.

Second, rules centering on the core processes focused on risk assessment and monitoring guidelines. These rules defined how the compliance function was managed. They originated from FFFS 2014:1, but were adjusted to the specific conditions within Banque de Montagne. Specifically, they took into account other aspects of the risk organization within the bank, business operations at the first line, and also what was communicated and expected by the Senior management and the Board of Directors. These rules illustrated how despite the high level of detail and prescription in many post-crisis regulations, there is still a certain element of principles-based flexibility in the application of regulatory requirements within the intra-organizational setting.

At the *actor* level, compliance actors were established as responsible for managing the life cycles of internal rules (policies and instructions, as well as responding to breaches triggered by compliance internal rules). Here, there emerged a clear delineation between first and second lines. During the final phase rollout, it was

specified that compliance officers (all of whom operate for the second line function of compliance) should *not* contact the internal rules unit for any breaches that are flagged by first line monitoring activities. These would fall under different monitoring and response systems, which were outside the scope of the second line function, at least at the lower level. What was unclear and appeared to be a "work in progress" was alignment between first and second lines in this regard. If the aim was to have a comprehensive risk picture of the bank, it remained unclear that the delineations during the time of the study allowed for that. However, considering that this study only captured one phase of an ongoing organizational evolution, it would perhaps be premature and inaccurate to label this as an established misalignment.

### 5.3.5 Compliance activity training

Regarding the *structure* of training within the compliance function, it is important to recognize that the broad function of training spans all three lines of defense. The training component largely made use of e-learning platforms as well as a digital repository of trainings that were accessible to all target employees and groups through the internal web system for Banque de Montagne.

In the context of Compliance Activity Training, the links blurred between structure, process, and actors. Training programs, whilst structurally stored in a collective database that could be accessed across all lines of defense, relied heavily on the process of training development and the role of actors in training execution. At Banque de Montagne, the interactions between actors (human beings) and information systems or processes led the compliance function to explicitly recognize its strong reliance on and need for heavy investments in training and onboarding activities. As the change process progressed, what became apparent was an organizational acknowledgement that even as technological reliance was growing, the human factor in compliance remained inescapable and significant in the overall role and execution of compliance responsibilities. This was reflected in multiple interviews and especially during the Phase 4 rollout, where the need for training and issues surrounding how training programs were being designed came into very strong focus. In general, what was indisputable was that even the design and use of systems was so reliant on user interfacing and the need for agent-driven professional judgment that in a very real sense, compliance activities arguably could not be separated from human actors within the organization.

The training *process* consists of three components: (1) needs assessment; (2) planning, and (3) execution. The target of training was all employees within Banque de Montagne, with the goal that compliance knowledge and capacity at the individual and group levels within the entire bank would be steadily and incrementally increased over an established timeline in line with regulatory requirements.

For *actors,* the Compliance Officer role was in a shifting state at the time of this study. Thus, one of the focus areas for training activities was to identify and cement the role of compliance officers within the organization. Whilst all compliance officers were in theory serving a second line function, those who operated at the different business units worked very closely with first line. The boundaries between what

their responsibilities are now as opposed to prior to FFFS 2014:1 (when they were more involved in first line functions) were thus blurry.

Regarding one responsibility of compliance officers, there was a strong indication during the final rollout phase that the process owners expected the responsible compliance officers who interacted directly with first line to establish contact with first line managers in order to gather information on which teams had done the required trainings or not. The reason for this was that the documentation function for training was still undeveloped, and such information would not be available to the compliance officers except through information provision by first line management.

## 6 Discussion and analysis

The data gathered while following the four phases of the bank's change process were analyzed in accordance with the conceptual understandings of accountability and transparency mechanisms as outlined in Sect. 4.2. A brief overview of the findings is presented in Table 2. This is followed by a more detailed discussion in Sect. 6.1 of how accountability and transparency were operationalized and analyzed in the data. Section 6.2 then provides a critical discussion of the empirical findings as relevant to both theory and practice.

### 6.1 Tracing the accountability and transparency responses to FFFS 2014:1

Within Banque de Montagne during the first phase of the study, the most immediate structural changes at the second line were the initial establishment of the formally consolidated and independent compliance function, and the definition of the broad areas of change that were to follow over the next three phases. Across a vertical dimension, the implementation of FFFS 2014:1 necessitated a more formalized reporting of compliance directly to the Board of Directors. The empirical data built a coherent indication that the direct and perhaps most immediate impact of regulatory implementation was an organizational response that adopted a heightened sense of outward accountability, directly translated into a high frequency and substantive depth in reporting across both vertically between the formal compliance function and the Board of Directors, as well as at the horizontal level in the context of establishing formal compliance responsibilities and delineations between first line and second line within the overall risk organization of the bank. In terms of transparency, the establishment of communication, reporting, and feedback channels across vertical and horizontal dimensions within the bank laid the foundation for increased transparency, while the planning surrounding this development involved a high level of vertical interaction between the Board, the reshaped second line of defense, and the overall risk organization within the bank. In this sense, both event and process transparency within the bank did increase in real-time.

As the implementation and change process continued through phases 2 and 3, the structural foundations of the formal compliance function began to be established across first line and second line. During this phase, new units and architecture were

**Table 2** Overview of accountability and transparency findings

| | Intra-organizational | Inter-organizational |
|---|---|---|
| Transparency | Reporting channels increased, but sensitivity of systems was too high for effective transparency to be achieved. There was a risk, at least in the first three phases, that adhering to the reporting systems as they stood would result in poorer risk management overall because the system was not adequately streamlined or desensitized. Thus, nominal transparency increased but effective transparency overall decreased | Process transparency increased, with increased meetings between the independent compliance organization and the regulators directly. However, in particular regard of meeting regulatory aims, event transparency remained sub-optimal according to internal interviewees. The reason for this could be traced to the still-ongoing development of information and risk control channels within the compliance organization as well as an ongoing effort to cement the role and scope of the Compliance function as a whole. In the absence of concrete stability in both these regards, it was felt that the transparency of accounts provided to regulators was still lacking |
| Accountability | Accountability channels underwent a change across both vertical and horizontal dimensions. Reporting and reflexive connectivity between the Board, senior management, and the Compliance function increased in both structure and reporting. Upward accountability in that sense increased greatly following the mandate of FFFS 2014:1. Horizontal accountability to the first-line, and also to different areas of risk and business activities similarly increased after the changes precipitated by FFFS 2014:1. This was apparent through the change activities across all core functions, at both process and actor levels | Outward and inward accountability mechanisms both increased, in the wake of FFFS 2014:1. Reporting requirements to regulators and regulatory interactions between the Compliance function and regulators both increased after the implementation of FFFS 2014:1. Through these interactions and reports, Banque de Montagne strengthened its accountability-based deliverables to Swedish regulatory authorities. Interestingly, regulatory accountability to the bank also increased, largely through the regulatory clarifications offered through such interactions, or at least a mutual sharing of areas and points of continued challenge for the bank. At the same time, as the bank identified, simply being open about organizational shortcomings did not mean that formal sanctions were avoided, although such accountability could lead to an understanding with regulators that allowed for additional time within which the bank could meet its obligations |

experimented with, and the boundaries between compliance and the broader risk organization began to solidify even though they maintained a high degree of flexibility. As one example of this—in early Spring 2016, we conducted three interviews and observed two meetings concerning the development of the technological structures that would define the new compliance function. This area was formulated as the new "technology and business architecture" unit. It collaborated closely with the executive management team and other developing units in the areas of risk identification and taxonomy as well as the compliance monitoring function. By July 2016, the "technology and business architecture" unit had dissolved, with some of it subsumed under the now more-established areas identified in Sect. 5.3 and other parts assigned elsewhere within the risk organization of the bank. As later empirical data indicated, rather than representing a reduction in focus on the aspect of information technology and its use in compliance, this development was more attributable to two factors: First, the formalization of a centralized compliance infrastructure across the bank as a whole; and second, a strong recognition of the need to link not only first line and second line within compliance but also to link compliance with other areas of the broader risk organization and business operations within the bank. Thus, whilst the structures, processes, and roles remained in flux during these phases, the *aims* underlying the initial impetus of the unit survived through these changes, however, and solidified into specific processes and roles by the end of phase 4. What could be seen in the above regard was that *accountability* across the dimensions of structure, process, and actors was in a consistent (if at times chaotic) state of increase—something that was clearly illustrated in the Phase 4 rollout of the focus areas described in Sect. 5.3.

*Transparency*, on the other hand, did not follow the same clear trajectory. What emerged was that the main issue in this regard was not an active intent to obfuscate either events or processes; rather, the arguable reduction in effective transparency seemed related to the number and magnitude of activities that were ongoing concurrently, as well as the need to test the sensitive risk identification and control systems, processes, and technological tools that were being implemented. On one hand, both event and process transparency of positive as well as negative progress were clearly identified through open and revealing face-to-face discussions and meetings, interactive planning sessions, and internal documentation of the development process during the study period. Nonetheless, the issue that seemed to arise regarding intra-organizational transparency between Phase 1 and Phase 4 was that of information overload. It was something that the compliance function itself seemed to be aware of through the explicit recognition during the Phase 4 rollout process that oversensitivity in their ongoing risk identification systems development were causing a high level of false positives in specific risk areas such as AML, thus contributing to more to granular opacity in risk identification rather than transparency.

From the perspective of inter-organizational accountability and transparency between regulators and Banque de Montagne, nominal outward accountability and transparency increased in line with the implementation of FFFS 2014:1. Particularly as the bank progressed from phase 1 towards its phase 4 rollout, the need for regulatory interpretation meant that inward accountability (from the regulators to the bank) was increasingly sought. While it was not possible to observe the meetings

conducted between the compliance function of Banque de Montagne and the Swedish Financial Supervisory Authority, retrospective accounts provided during the interviews indicated that inward accountability through clarifications offered by regulators in such interactions increased. At the same time, the interactions in some sense also represented a shared interpretive exercise that involved Banque de Montagne as an important contributor of insight to the regulators regarding what shape regulatory implementation could take in their specific organizational context.

### 6.2 Understanding the empirical findings

At a detailed level, the observations, particularly during Phases 3 and 4, indicated the strong shift in organizational culture towards a strengthening of accountability culture through compliance. This accountability on part of the compliance function itself was rooted in its independence from both operational risk and first line activities. In this regard, what was apparent fairly early on was that for the compliance team, a detachment from more financial considerations rooted in profit-based interests was not only a requirement, but a necessity.

The operational risk and compliance split effectively divided the risk control organization of the bank into two units—one of which (operational risk) was more based on risk measures as relevant to capital requirements and quantitative financial assessments of both risk and reactions to that risk. Compliance on the other hand was building an identity structured around regulatory aims as a launching point rather than purely organizational aims. This is an important consideration from a corporate governance perspective, as it (at least in principle) directly and indirectly heightens the voice and interests of stakeholders other than shareholders/owners in corporate management and decision-making (across all levels). One strong signal of this phenomenon was observed not through what was said, but rather what was not said. Namely, at no point of any of the phases did comments or considerations of bottom-line profitability impacts enter into discussions, indicating two points:

First, compliance at first and second lines saw itself as independent from profit line discussions, and responsible solely for *actual compliance with regulatory aims and internal rules of conduct integrity*. Second, it indicated the importance that the Board and CEO assigned to formal compliance, and the high level of independence concurrently offered to the fledging organization in order to develop and establish itself. Accountability in upward, downward, and horizontal directions (between the core function areas of compliance, for instance) similarly increased during the four phases of the change process. Here, however, it is important to shift the discussion to transparency in order to understand the changes effectuated and their implications.

While the findings showed clear increases in accountability structures, channels, and interactions, the findings on transparency were, rather ironically, not as clear. Integration in risk control activities and the goal of building a clear (transparent) and complete risk map of the bank as a whole remained high on the compliance agenda throughout. Even so, inward transparency was perceived as limited, as regulatory demand presented the bank with challenges that were difficult to contend with. While outward transparency about such challenges was sought, such transparency

in meeting regulatory demands for accountability did not aid the bank in ultimately avoiding potential sanctions or other negative consequences, although it did increase the likelihood that the bank would receive additional time to meet regulatory demands if required.

In general, transparency mechanisms seemed to increase, largely through the development of shared understandings regarding risk identification, assessment, and control and an enhanced informational database of risk activities, within the organization and the bank as a whole. At the same time, a misalignment continued regarding compliance risk control systems and other risk understandings and communications within the bank. At first line business unit operations in different areas of banking practice for example, a lack of transparency marked the information available on individual actor and business group levels of risk control. As the compliance group had neither the capacity nor the tools to identify misalignments between required risk control activities and issues such as decision-making conflicts arising from management control misalignments between, for instance, compensation and incentive structures. In this context, a reliance on first line inputs as related to transparency and accountability was deemed necessary, and a call for better alignment was identified.

From an intra-organizational perspective, increased inward transparency and accountability regarding regulatory interpretation and increased outward transparency regarding how Banque de Montagne was engaging in regulatory implementation and the accompanying organizational change collectively indicate that regulatory implementation, rather than being unidirectional, involves a process of interpretation and implementation that may be shaped or at least influenced to some degree by banks. At the same time, what emerged as a strong theme throughout the change process was that Banque de Montagne understood that in terms of the monitoring and enforcement component of intra-organizational accountability, an increase in transparency and accountability towards regulators did not decrease the potential severity of the sanctions or other disciplinary measures that the bank faced for any perceived serious shortcomings in its implementation response. In this regard, even in a shared interactive space of transparency and accountability, the structural and substantive outward accountability that Banque de Montagne and other regulated entities were required to achieve represented an indelible facet of the regulation-practice interface of banking.

## 7 Conclusions and avenues for future research

This study has addressed the research question of how prudential regulation in the financial sector impacts accountability and transparency in the risk control and governance approach of large and complex regulated organizations. This study finds that whilst intra- and inter-organizational accountability mechanisms have strengthened under the changed organizational structure through the implementation of FFFS 2014:1, challenges to effective transparency remain at the intra- and inter-organizational contexts.

Although recent studies have investigated some aspects of intra-organizational risk control in the context of risk control culture, understandings, and roles (see e.g.: Mikes 2009, 2011; Giovannoni et al. 2016), risk management in the banking sector remains largely black-boxed. This is particularly true in the context of the regulation-practice interface of banking where there are, to the best of our knowledge, no studies that investigate regulatory influence on risk control across the descriptive dimensions of structures, processes, and actors as well as the conceptual dimensions of transparency and accountability as this study does. This work, which adopts an in-depth case study approach to trace the change process within the risk organization of Banque de Montagne after the implementation of FFFS 2014:1 is thus one of only a few studies in the arena of banking sector risk management and control that have attempted to explore how external pressures such as regulatory implementation influence the intra-organizational structures, processes, and actor-oriented mechanisms that comprise intra-organizational response and change.

Our study contributes to current research in several ways. First, this work represents a unique study of the organizational impact resultant from ongoing regulatory implementation, importantly contributing to extant knowledge of the dynamics that exist in the regulation-practice interface of banking. By investigating how a regulatory mandate requiring organizational change and the formalization of a separate compliance function within banks affects the dimensions of risk control structures, processes, and actor-oriented mechanisms in different yet connected ways, it sheds more light on the generally black-boxed arena of organizational practices within the banking sector. It shows that regulatory implementation, rather than being a seamless, unidirectional liner process of organizational translation of regulatory aims, is a complex and reflexively interactive process that is affected by both external and intra-organizational dynamics. Here, the role of structures, processes, and actors emerged as distinct, but subject to highly fluid and in some sense permeable boundaries between them. In the context of risk control, the changes that emerged across the dimensions of structures, processes, and actor-oriented roles and mechanisms over the course of the study highlighted not only how these boundaries existed within the different emerging components of the compliance function, but also between the compliance function and operational risk. In particular, from an intra-organizational perspective, the detachment of compliance considerations of risk control from the arguably more financially-oriented considerations of operational risk control indicated that a potentially more fundamental disconnect between these two components of the bank´s risk organization as well as between the compliance function and the bank´s broader strategic and business objectives could exist. From an inter-organizational perspective, the establishment of an independent compliance function driven by more regulatory aims provided an indication of the permeable nature between regulators and banks, but also identified the difference and in some sense a potential tension between regulatory impetus and organizational motivations of shareholder primacy in inter-organizational governance and control.

Second, this study contributes to theory in the context of risk control by adding to the descriptive knowledge of how the 3LoD model functions in practice, and also by operationalizing the concepts of transparency and accountability within the 3LoD of Banque de Montagne. In this respect, the operationalization of transparency and

accountability importantly relied on shared communications regarding risk understandings as well as risk control across the 3LoD structures, processes, and actor-oriented mechanisms of the formalized compliance function of Banque de Montagne. These findings contribute to ongoing research discussions in the transparency and accountability streams of literature by providing descriptive granularity in extending the governance-oriented framework espoused by Heald (2006) and Hood (2007), amongst others.

Third, in the context of ongoing research dialogue within the area of risk management in financial organizations, this work provides a corroborative and complementary granular perspective to earlier investigations into risk management in practice. These include, amongst others, the studies by Mikes (2011) on different organizational approaches towards risk management, Giovannoni et al. (2016) on the longitudinal evolution and importance of risk management templates and roles within organizational change processes, and Kaplan and Mikes (2016) on the recognition of the more holistic and integrated non-financial considerations of risk that are increasingly gaining ground within the post-crisis landscape of banking.

In building effective models of risk control, the potential tension between regulatory aims in the financial sector and the foundation of share-value maximization that underlies extant corporate governance models seems ultimately to address the issue of shareholder primacy and its continued relevance in the banking sector. The central question for managerial bodies and regulators to consider is whether the unique leverage structure of banks makes it so that primary accountability to shareholders is the wrong model to follow in order to ensure that downside risks and their corresponding (often opaque) systemic implications are minimized in such financial organizations and, by implication, in the broader banking system.

It remains to be seen how internal needs and demands for risk control rooted in aims that are perhaps at odds with the regulatory intent captured through the formal compliance function are resolved within an evolving banking culture where regulatory compliance and the accompanying inclusion of broader stakeholder interests appear to be increasing in importance to bank strategy, operational management, and organizational decision making. These links, together with considerations of how transparency and accountability impact risk recognition and control in financial organisations and systems, present worthy and interesting avenues for future research.

**Funding** Open access funding provided by Uppsala University.

**Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

## References


Anderson, D. J., & Eubanks, G. (2015). Committee of Sponsoring Organizations of the Treadway Commission: Leveraging COSO across the three lines of defense. Retrived September 23, 2019 from https://www.heritageadvisorsllc.com/wp-content/uploads/2016/06/COSO.pdf.

Arndorfer, I., & Minto, A. (2015). The "four lines of defence model" for financial institutions. *Financial Stability Institute Occasional Paper, 11*(December), 1–26.

Arena, M., Arnaboldi, M., & Azzone, G. (2010). The organizational dynamics of enterprise risk management. *Accounting, Organizations and Society, 35*(7), 659–675.

Arwinge, O., & Olve, N.-G. (2017). Three lines of defense for organizing risk management. In A.-K. Stockenstrand & F. Nilsson (Eds.), *Bank regulation: Effects on strategy, financial accounting and management control* (pp. 284–309). New York: Routledge.

Arwinge, O., & Rost, I. (2013). Modellen om tre försvarslinjer skapar struktur kring riskägarskapet. *Balans: tidskrift för redovisning och revision, 6,* 32–35.

Avgouleas, E., & Cullen, J. (2014). Market discipline and EU corporate governance reform in the banking sector: Merits, fallacies, and cognitive boundaries. *Journal of Law and Society, 41*(1), 28–50.

Bamberger, K. A. (2010). Technologies of compliance: Risk and regulation in a digital age. *Texas Law Review, 88*(4), 669–706.

Beasley, M. S., & Frigo, M. L. (2007). Strategic risk management: Creating and protecting value. *Strategic Finance, 12,* 25–33.

Bhimani, A. (2009). Risk management, corporate governance and management accounting: Emerging interdependencies. *Management Accounting Research, 20*(1), 2–5.

Binder, J.-H. (2015). The Banking Union and the governance of credit institutions: A legal perspective. *European Business Organization Law Review, 16*(3), 467–490.

BIS. (2011). Basel committee on banking supervision: Principles for the Sound Management of Operational Risk. Retrieved September 26, 2019, from https://www.bis.org/publ/bcbs195.htm.

BIS. (2015). Basel Committee on Banking Supervision: Guidelines Corporate governance principles for banks. https://www.bis.org/bcbs/publ/d328.pdf Accessed 19 September 2019.

Bryant, M. (2006). Talking about change: Understanding employee responses through qualitative research. *Management Decision, 44*(2), 246–258.

COSO. (2013). The Committee of Sponsoring Organizations of the Treadway Commission: Integrated Framework on Internal Control. Retrieved September 23, 2019, from https://www.coso.org/Pages/ic.aspx.

Crawford, J., Kashyap, S., Nilsson, F., Stockenstrand, A.-K., & Tirmén, M. (2017). Accounting and control in banks: A literature review. In A.-K. Stockenstrand & F. Nilsson (Eds.), *Bank Regulation: Effects on Strategy, Financial Accounting and Management Control* (pp. 15–63). New York: Routledge.

Davies, P. L., & Hopt, K. J. (2013). Corporate boards in Europe: Accountability and convergence. *The American Journal of Comparative Law, 61*(2), 301–376.

Decaux, L., & Sarens, G. (2015). Implementing combined assurance: Insights from multiple case studies. *Managerial Auditing Journal, 30*(1), 56–79.

Drennan, L. T. (2004). Ethics, governance and risk management: Lessons from mirror group newspapers and barings bank. *Journal of Business Ethics, 52*(3), 257–266.

EBA. (2011). European Banking Authority: Guidelines on internal governance. Retrieved September 23, 2019 fromhttps://www.eba.europa.eu/documents/10180/103861/EBA-BS-2011-116-final-EBA-Guidelines-on-Internal-Governance-(2)_1.pdf.

Eisenhardt, K. M., & Graebner, M. E. (2007). Theory building from cases: Opportunities and challenges. *Academy of management journal, 50*(1), 25–32.

FERMA/ECIIA. (2010). Guidance on the 8th EU Company Law Directive, Article 41. Retrieved September 23, 2019 from https://www.iia.nl/SiteFiles/ECIIA%20FERMA.pdf.

Finansinspektionen. (2014). Finansinspektionens föreskrifter och allmänna råd om styrning, riskhantering och kontroll i kreditinstitut, FFFS 2014:1. Retrieved September 23, 2019, from https://www.fi.se/sv/vara-register/sok-fffs/2014/20141/.

Garciano, L., & Lastra, R. (2010). Centre for economic performance: Towards a new architecture for financial stability. Retrieved September 23, 2019 from http://cep.lse.ac.uk/pubs/download/dp0990.pdf.

Giovannoni, E., Quarchioni, S., & Riccaboni, A. (2016). The role of roles in risk management change: The case of an Italian bank. *European Accounting Review, 25*(1), 109–129.
Heald, D. (2006). Varieties of transparency. In C. Hood & D. Heald (Eds.), *Transparency: The key to better governance?* (pp. 25–43). New York: Oxford University Press.
Hood, C. (2007). What happens when transparency meets blame-avoidance? *Public Management Review*, *9*(2), 191–210.
Hopt, K. J. (2013). Corporate governance of banks and other financial institutions after the financial crisis. *Journal of Corporate Law Studies, 13*(2), 219–253.
Hopt, K. J. (2015). Corporate Governance in Europe: A Critical Review of the European Commission's Initiatives on Corporate Law and Corporate Governance. *New York University Journal of Law and Business, 12*(1), 139–214.
Iannotta, G., Nocera, G., & Sironi, A. (2007). Ownership structure, risk and performance in the European banking industry. *Journal of Banking & Finance, 31*(7), 2127–2149.
IIA. (2013). Institute of Internal Auditors: The three lines of defense in effective risk management and control. Retrieved September 23, 2019 from https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control.pdf.
Kaplan, R. S. (2009). Risk management and the strategy execution system. *Balanced Scorecard Report, 11*(6), 1–6.
Kaplan, R. S., & Mikes, A. (2012). Managing risks: A new framework. *Harvard Business Review, 90*(6), 48–60.
Kaplan, R. S., & Mikes, A. (2016). Risk management-The revealing hand. *Journal of Applied Corporate Finance*, *28*(1), 8–18.
Kaplan, R. S., Mikes, A., Simons, R., Tufano, P., & Hofmann, M., Jr. (2009). Managing risk in the new world. *Harvard Business Review, 87*(10), 68–75.
Keasey, E. K., Thompson, E. S., Wright, E., & Keasey, K. (2005). *Corporate governance: Accountability, enterprise and international comparisons*. Hoboken: Wiley.
Kvale, S., & Brinkmann, S. (2009). *Interviews: Learning the craft of qualitative research interviewing*. Los Angeles: Sage Publications Inc.
La Porta, R., Lopez-de-Silanes, F., Shleifer, A., & Vishny, R. W. (1998). Law and finance. *Journal of Political Economy, 106*(6), 1113–1155.
Larsson, M., & Söderberg, G. (2017). *Finance and the welfare state: Banking development and regulatory Principles in Sweden, 1900–2015*. Basingstoke: Palgrave Macmillan.
Lee, A. S., & Baskerville, R. L. (2003). Generalizing generalizability in information systems research. *Information Systems Research, 14*(3), 221–243.
Liikanen, E. (2012). Final Report, Brussels: High-level Expert Group on reforming the structure of the EU banking sector. Retrieved September 23, 2019 from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.348.5669&rep=rep1&type=pdf.
Magnan, M., & Markarian, G. (2011). Accounting, governance and the crisis: Is risk the missing link? *European Accounting Review, 20*(2), 215–231.
Malmi, T., & Brown, D. A. (2008). Management control systems as a package—Opportunities, challenges and research directions. *Management Accounting Research, 19*(4), 287–300.
Mikes, A. (2008). Chief risk officers at crunch time: Compliance champions or business partners? *Journal of Risk Management in Financial Institutions, 2*(1), 7–25.
Mikes, A. (2009). Risk management and calculative cultures. *Management Accounting Research, 20*(1), 18–40.
Mikes, A. (2011). From counting risk to making risk count: Boundary-work in risk management. *Accounting, Organizations and Society, 36*(4–5), 226–245.
Mikes, A., & Kaplan, R. S. (2014). Towards a contingency theory of enterprise risk management. *Harvard Business School: Working Paper 13–063.*
Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook*. Thousand Oaks, CA: Sage.
Mülbert, P. O., & Citlau, R. D. (2011). The uncertain role of banks' corporate governance in systemic risk regulation.
Otley, D. (2016). The contingency theory of management accounting and control: 1980–2014. *Management Accounting Research, 31,* 45–62.
Potter, P., & Toburen, M. (2016). The 3 lines of defense for risk management. *Risk Management, 63*(5), 16–18.

Power, M. (2004). The risk management of everything. *The Journal of Risk Finance, 5*(3), 58–65.
Power, M. (2007). *Organized uncertainty: Designing a world of risk management*. Oxford: Oxford University Press.
Roberts, J., & Scapens, R. (1985). Accounting systems and systems of accountability: Understanding accounting practices in their organisational contexts. *Accounting, Organizations and Society, 10*(4), 443–456.
SBA. (2017). Swedish Bankers Association: Position Paper on the EBA Draft Guidelines on Internal Governance. Retrieved September 23, 2019 from https://www.swedishbankers.se/media/3083/eba170127.pdf.
Seal, W. (2006). Management accounting and corporate governance: An institutional interpretation of the agency problem. *Management Accounting Research, 17*(4), 389–408.
SFAS. (2014). Swedish Financial Services Authority: Regulations and general guidelines (FFFS 2014:1) regarding governance, risk management and control at credit institutions. Retrieved September 26, 2019, from https://www.fi.se/en/our-registers/search-fffs/2014/20141/.
Shleifer, A., La Porta, R., & Lopez-De-Silanes, F. (1999). Corporate ownership around the world. *Journal of Finance, 54*(2), 471–517.
Short, H., & Keasey, K. (2005). Institutional shareholders and corporate governance in the UK. In K. Keasey, S. Thompson, & M. Wright (Eds.), *Corporate governance, accountability, enterprise and international comparisons* (pp. 18–53). Oxford: Oxford University Press.
Soin, K., & Collier, P. (2013). Risk and risk management in management accounting and control. *Management Accounting Research, 24*(2), 82–87.
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.
Suddaby, R. (2006). From the editors: What grounded theory is not. *Academy of management journal, 49*(4), 633–642.
Van der Stede, W. A. (2011). Management accounting research in the wake of the crisis: Some reflections. *European Accounting Review, 20*(4), 605–623.
Weick, K. (2007). The generative properties of richness. *Academy of Management Journal, 50*(1), 14–19.
Westman, H. (2011). The impact of management and board ownership on profitability in banks with different strategies. *Journal of Banking & Finance, 35*(12), 3300–3318.
Yin, R. K. (2003). *Case study research: Design and methods* (3. ed., Applied social research methods series, 5). Thousand Oaks, CA: Sage.

**Publisher's Note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

**Shruti Kashyap** is a lecturer and post-doctoral researcher in Accounting at Uppsala University. Her work centers around issues of transparency and accountability in the international financial sector. Her current research focuses on the inter-relationship between regulators, markets, and financial institutions within the European Union, specifically addressing the influence of regulation on innovation by incumbent banks and new market entrants in the EU fintech arena.

**Einar Iveroth** is Associate Professor at Uppsala University. His expertise and research includes management control, organizational change, digitalization, and strategic pricing. He has published widely in leading journals such as the California Management Review, Journal of Change Management, Journal of Environmental Management, European Management Journal, and Health Care Management Review, as well as a number of Routledge books.