The Journal of Risk Finance

Cognitive risk culture and advanced roles of actors in risk governance: a case study

Ruchi Agarwal, Sanjay Kallapur,

Cognitive risk culture and advanced roles of actors in risk governance: a case study

Ruchi Agarwal and Sanjay Kallapur
Indian School of Business (ISB), Hyderabad, India

Received 30 November 2017
Revised 28 March 2018
12 June 2018
1 September 2018
Accepted 25 September 2018

Abstract

Purpose – The purpose of this study is to explore the best practices for improving risk culture and defining the role of actors in risk governance.

Design/methodology/approach – This paper presents an exemplar case of a British insurance company by using a qualitative case research approach.

Findings – The case study shows how the company was successful in changing from a compliance-based and defensive risk culture to a cognitive risk culture by using a systems thinking approach. Cognitive risk culture ensures that everybody understands risks and their own roles in risk governance. The change was accomplished by adding an operational layer between the first and second lines of defense and developing tools to better communicate risks throughout the organization.

Practical implications – Practitioners can potentially improve risk governance by using the company's approach. The UK regulator's initiative to improve risk culture can potentially be followed by other regulators.

Originality/value – This is among the few studies that describe actual examples of how a company can improve risk culture using the systems approach and how systems thinking simultaneously resolves several other issues such as poor risk reporting and lack of clarity in roles and responsibilities.

Keywords Corporate governance, Enterprise risk management, Risk reporting, System theory, Three lines of Defense model

Paper type Research paper

Introduction and background

The state of the art in risk governance is to use control self-assessment (CSA) as a tool for risk assessment[1], enterprise risk management (ERM) framework for risk management and three lines of defense model for risk governance. Risk culture ties together ERM and risk governance with the understanding of risk, beliefs and values. A well-known risk theorist, Otwin Renn, defines risk governance as a complex web of actors, rules, conventions and processes concerned with how relevant risk information is collected, analyzed and communicated and how management decisions are taken (Renn, 2008). Gontarek (2016) explains that risk governance is the core responsibility of Board and to execute this responsibility effectively, they must include board-level risk committees, empowered chief risk officers (CROs), use risk appetite statements and establish a robust risk culture. The three lines of defense model offers a fundamental structure along with generic guidelines on roles of actors across various organizational levels in risk-related matters (Deighton *et al.*, 2009). The objectives of the first line, second line and third line of defense are to implement risk management, risk oversight and assurance, respectively.

As we describe in the next section, the view in the academic and practitioner literature is that risk governance needs improvement, but there are differing perspectives on how to do it. Bogodistov and Wohlgemuth (2017) argue that setting priorities and managing resources

The Journal of Risk Finance
© Emerald Publishing Limited
1526-5943
DOI 10.1108/JRF-11-2017-0189

are essential to make organizations resilient to fluctuations in external business environment, emphasizing that the most critical issues should be resolved first. Others argue that even if firms have appropriate structures in place, risk governance is ineffective without appropriate risk culture (Sheedy and Griffin, 2018). Despite the acknowledged importance of risk culture, there is little research on how to develop one (Viscelli *et al.*, 2017). Our purpose is to understand the best practice in defining the roles of actors and improving risk culture. This is a how question for which a case study that can trace operational processes over time is ideally suited (Yin, 2017, p. 18). To answer the question, we present a case study of a British insurance company that was widely recognized within the industry as having been the most successful in this effort.

The UK financial industry is a good setting to study the issue. After the financial crisis 2007-08, regulators pressured companies to implement risk governance with clearly defined roles and accountability (FSB, 2014). They became stricter and called for improvements in risk governance, particularly in the financial industry (e.g. Basel norms in banking and Solvency directives for insurance). Paape and Speklè (2012) show that due to stricter regulations, financial institutions have better ERM practices than do firms in other industries. Furthermore, in 2013, Financial Service Authority (FSA), a financial regulatory body in the UK, split into two: Prudential Regulatory Authority and Financial Conduct Authority (FCA), which enhanced the regulatory requirements. We, therefore, choose the UK financial industry as a setting to explore the issue.

The insurance industry in the UK is well-established and mature, contributing over £25bn to UK GDP (Association of British Insurers (ABI), 2014). In the aftermath of the 2007-08 crisis, an initial draft of Solvency II directives, also known as “Basel for Insurers,” was prepared. The aim was to establish systems to provide early warning to reduce risks and promote confidence in the financial stability of the insurance sector. Solvency II directive came into effect on January 2016 with three pillars: quantitative requirement (Pillar I) (amount of capital an insurer should hold as a cushion), risk governance (Pillar II) and disclosure and transparency requirements (Pillar III). The discussion of these pillars started in the year 2002 with a KPMG report (Eling *et al.*, 2007) and the Sharma Report[2]. The Sharma Report concluded that companies should focus on enhancing internal factors such as quality of risk governance and risk management with particular emphasis on risk culture.

Most of the large companies established the preliminary infrastructure of risk governance post-crisis and did not wait for Solvency II directives. Other issues were also evolving within the industry. For example, Royal Bank of Scotland, operating in banking and insurance industry, received a large number of customer complaints and regulatory penalties of over 50 million pounds due to lack of investment in IT infrastructure. Subsequent to the regulatory split mentioned above, new regulators set new risk governance priorities; in particular, FCA set a high expectation for the development of good risk culture. The UK insurance industry’s response to enhanced regulatory expectations makes it a good setting to look for best practices.

We began by interviewing top officials of four insurance companies, two actuary firms and an industry association to determine the state of risk governance. One company was consistently mentioned as being the most advanced in implementing risk governance. This company was willing to participate in our research, so in the second phase, we interviewed several officers of this company. The case study method is appropriate for how questions and a single case is appropriate given that it is an extreme or unusual case from which others can possibly learn (Yin, 2017, p. 67). Accordingly, we narrowed down upon a single case study as our research method. A British insurer operating in over 50 countries, the case study company was asked by the regulator to devise mechanisms to improve risk culture in the three lines of defense model. The company found gaps in the three lines of defense model and contributed an operational layer between the first line and second line of defense in the model. We analyze our findings using the theoretical lens of systems thinking. Our paper contributes to the academic literature and gives practitioners guidance on how to go about improving the risk culture and defining the roles of actors in risk governance.

Literature review

The state of risk governance

Despite some consensus about the elements of ERM and governance (Bromiley *et al.*, 2015), the existence of two frameworks, namely, COSO 2004 and ISO 31000:2009, and requirements for risk management under different regulatory regimes, the practice of risk governance has not generated the hoped-for results. Risk management approaches are largely unproven and still emerging (Mikes and Kaplan, 2015). This is especially so in financial institutions, although they are among the most advanced in adoption because of regulatory pressure (Paape and Speklè, 2012). The failures are evidenced by the events leading to the financial crisis of 2007-2008, as well as the record fines levied on financial institutions in 2013-14 for subsequent misconduct such as mis-selling and trade sanctions violations.

The literature mentions several possible reasons for risk governance failures. Paté-Cornell and Cox (2014) show that organizational actors give many excuses for poor risk management. Eling and Marek's (2014) research on the UK and German insurance markets identifies poor risk culture as the major problem and attributes it to executives' variable compensation. Viscelli *et al.* (2017) discuss issues such as poor integration of risk in strategy, poor risk culture and lack of clarity in roles and risk reporting. Many papers argue that the failure to embed risk across the organization is due to poor risk culture. Kleffner *et al.* (2003) find in Canadian insurance companies that organizational structure was a deterrent to adopt ERM, and there is a high resistance to change. The resistance to change results in a defensive and calculative risk culture, wherein employees go through the motions but do not actually manage risk (Gigerenzer, 2015; Mikes, 2009). Recent research by Sheedy and Griffin (2018) in Australia and Canada finds that reliance on risk structures without addressing risk culture is ineffective because the structures can be undermined by poor risk culture. Thus, a recurring theme among the reasons for risk governance failures mentioned in the literature is poor risk culture, but there is scant research on how to improve it; an examination of best practices could therefore contribute to both theory and practice.

In addition, the role of the CRO is unclear. Integrated risk management is supposed to be implemented by the CRO under the guidance of Board and in discussion with CEO (Lam, 2000). Mikes's (2008) findings in the banking sector reveal that CROs' roles expanded dramatically as compliance champions and business partners due to their frequent involvement in firms' strategic decision making. The rising responsibilities of CRO, however, became more a problem than a solution to implementation issues in risk management because the risk was considered to be the CRO's responsibility rather than everybody's (Pernell *et al.*, 2017). Thus, while it is understood that risk governance is a team effort, precise responsibilities are unclear. Another purpose of our study is to understand how to define the roles of the actors for better implementation of risk governance.

Theoretical approaches to the "how" of risk governance

Most traditional approaches for managing risks such as cost-benefit analysis and fault tree analysis are reductionist (Abraham and Shrives, 2014; Beasley *et al.*, 2015; White, 1995). The reductionist method tries to simplify the problem by breaking it into smaller parts, understanding the behavior of each part and deducing the behavior of the whole from an understanding of the behavior of the parts.

In contrast to the reductionist approach, systems thinking promotes understanding of the system as a whole over a period (Kim and Senge, 1994; Lee and Green, 2015). It posits that a system is more than the sum of individual parts (Ackoff, 1994); the system can have emergent properties that are not present in any of its parts. The relationships between the elements are more important than the elements themselves. These relationships constitute a network of reinforcing and balancing loops that interact with each other. O'Donnell (2005) explains the use of systems thinking for risk event identification, and Lee and Green (2015) link it to ERM which is extended for risk governance.

As part of systems thinking, Argyris and Schon (1978) discuss balancing and reinforcing loops to explain how a system adjusts based on the difference between expected and actual outcomes, like a thermostat. Reinforcing loops enhance the outcomes such as vicious or virtuous cycles, while balancing loops try to bring things to the desired state and keep them there, much like a thermostat regulates the temperature in a house.

Vester (1988) emphasizes six errors by non-system thinkers originally mentioned by Dörner *et al.* (1983): insufficient goal description, concentration on isolated concepts, focus on immediate problems, one-dimensional proceedings without understanding the side effects, tendency to over-react and authoritarian and dictatorial behavior in execution. To sum up, non-system thinkers believe in quick-fix solutions of immediate problems (Senge, 1990). Systems thinkers on the other hand look for root causes and deep understanding, which makes for what we call a "cognitive risk culture." Cognitive risk culture focuses on improving the understanding of risk and resolving the problems by addressing their root cause.

Cognitive risk culture stands in contrast to compliance-based and defensive risk cultures. For many companies, the aim of risk governance is to furnish compliance. Regulators expect companies to disclose how they are governing risks; the last step (disclosure) is the major motivator for the first step (adoption) in many companies, leading to a compliance-based culture. Another commonly observed phenomenon is a defensive culture that promotes professionally sub-optimal or even wrong decisions for the sake of preventing law-suits and blame. This happens due to innumeracy (not understanding risk meaningfully) and prioritizing profits over professional ethics (Gigerenzer, 2015). Blame prevention is the key theme and people low in the hierarchy feel they may become scapegoats in situations where real risk and real culprits are not identified (Douglas, 2013; Spira and Page, 2003).

Another theoretical approach to risk management proposed in the literature is the resource-based dynamic capabilities view (Bogodistov and Wohlgemuth, 2017; Bromiley *et al.*, 2015). This view posits that there are too many risks to manage, and ERM's emphasis on identifying and ex ante preparing for risks is misplaced. Instead, firms need to invest in creating dynamic capabilities to respond to risks as they arise and transform the resource base of the firm accordingly. In other words, the firm should make itself resilient to risks (Agarwal and Ansell, 2016). Firms should develop the capabilities to adapt successfully when unlikely events occur.

These rival (but not mutually exclusive) theories form the basis for our interpretation of our case findings (Yin, 2017, p. 47). However, given the view that risk management approaches are unproven (Mikes and Kaplan 2015), our study is exploratory and not designed as a test of theoretical propositions. We use the theories as a blueprint for exploration and generalization.

Research method

As little is known about how companies define the roles of actors and create a culture for effective risk governance, we did the field work in two stages. In the first stage between 2013 and 2014, we created a purposive sample of four UK insurance companies from the top 50 (by revenues), two professional actuarial firms and a professional association. The interviewees from those organizations included CRO, group risk director, group CRO, head ERM and head actuaries involved in the implementation of risk governance. Our purpose was to understand the current state of risk governance in the UK insurance companies. We chose the interview method over others such as surveys because Judge and Zeithaml (1992) and Mintzberg (1979) argue that field interviews are critically important to understand the complex organizational processes such as strategic board role.

From interviews, we found that one company had adopted several new tools and techniques to resolve issues in the implementation of risk governance. The three lines of defense model were well adopted in the UK insurance market, but this company was considered unique in improving the model to derive higher benefits. This company's advanced work in risk governance was acknowledged by professional actuarial firms and the association. Accordingly, we chose this company for a case study, and it was willing to participate in the research. The case study methodology is appropriate when studying new and emerging phenomena, and purposive sampling rather than random selection is especially appropriate in such situations (Eisenhardt, 1989).

We collected data from multiple sources during the period 2014-2016: interviews, websites, documents shared and published on-line interviews. To keep the identity of our respondents and company anonymous, we are not citing the details of online documents or PPT titles. For the same reason, we are quoting from interviews instead of online documents. We carried out ten semi-structured, recorded, face-to-face interviews with senior management of the company at the company's head office meeting room according to the participants' availability and convenience. The interviewees included group chief risk officer (CRO), group risk director, group fraud director, CRO (UK), CRO (China), ERM head, actuary and head operations to name a few (all males). The transcripts run into 79 pages in total. The multiplicity of informants reduces concerns about bias due to impression management or retrospective sense-making by them (Eisenhardt and Graebner, 2007).

Interviews ranged from 0.5 to 1 h, except one interview where group risk director was willing to discuss the topic beyond the appointed time. All interviews were transcribed. Additional data were also shared by senior management during interviews and also through follow up discussions and emails with group CRO and actuaries. Some of the documents include CRO committee meetings minutes, company's three lines of defense model, company structure, company ERM DOCUMENT, ORAC (software used for CSA) screenshots and PPTs shared by executives during interviews. Further, the company website, online published interviews and annual reports were used to update the data with recent developments in the company. We used these to triangulate the findings from interviews.

Case study findings

Company A is a full-service life and pension insurance company of British origin with total assets worth over GBP 300bn and operating with 9000 employees in over 50 countries. In the year 2016, Company A generated over GBP 18bn in revenue. The company is considered as the pioneer in introducing risk and capital models in the UK financial industry. Over its life exceeding 100 years, the company passed through several crisis periods and upswings in the economy. Listed on London Stock Exchange and a constituent of the FTSE 100 Index, the company is designated as a systemically important company in the UK and has a strong tone from the top for implementing risk governance. The company was the pioneer in implementing own risk and solvency assessment (ORSA) and considered as one of the strongest companies for its financial models and investments in the global market.

Risk governance in the case company functions by the three lines of defense model similar to other large financial institutions worldwide. Front line staff such as insurance agents, advisors and managers are assigned delegated authorities and limits. They are at the forefront of risk management and take daily decisions for acceptance or rejection of risks. The second line of defense consists of senior management, central risk unit headed by CRO, risk committee, board risk committee, and the board. The role of the second line of defense is to ascertain risk infrastructure and best practice standards for ERM. The third line of defense is internal auditors who independently verify the adequacy and effectiveness of internal control and risk.

Senge (1990) discusses four initial steps to break through organizational gridlock from system thinking perspective. The case company was facing two gaps between regulatory expectations and reality (one leading to another) over a period (Figure 1). During our analysis, we found that the company closed the gaps using a system thinking approach discussed below. First, the company identified the original problem symptom and mapped all quick fixes. Then it identified the undesirable impacts and fundamental solutions which led to identifying high leverage actions such as apps and advanced roles, overcoming the gaps.

Step 1: identify the original problem symptom

Post 2007-08 crisis, policymakers worldwide were concerned about poor risk outcomes in financial institutions despite their having implemented the best practices in risk governance structures, namely, dedicated board-level risk committee, independence of board and CRO as a part of board (Aebi *et al.*, 2012; FSA, 2011). Therefore, regulators in the financial industry were putting pressure on companies to improve risk governance. Later, the UK regulator was dissatisfied with financial institutions for the poor working of their ERM and attributed the reasons to poor risk culture and conduct of executives. The regulatory dissatisfaction created Gap 1 and acted as trigger (Figure 1). The company identified that

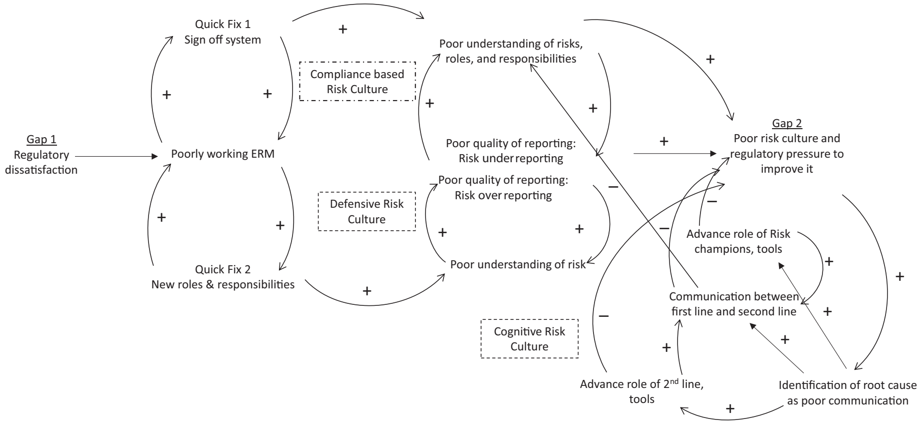

Figure 1.
Cognitive risk culture and role of actors

risk reporting is the major barrier in risk governance system as each of the three lines of defense works in its own silo.

Step 2: map all the quick fixes

To deal with Gap1, the company senior executives implemented two quick fixes: sign off the system and setting new roles and responsibilities. Quick Fix 1 introduced a "Sign off System," where every employee signs a self-declaration for the reporting of risk at year end. Like many companies, Company A was using control-self-assessment (CSA), which is an online repository of self-assessed risks. The company aimed CSA as a Red Cross Parcel for setting a clear line of accountability for controls:

> You have given something to the first line by providing "Red cross parcels"-things the people can say, here is the tool – Control Self-Assessment (CSA), risk register which I can use to manage the risk in my area. (Interview Transcript, Head ERM)

The sign off system, wherein employees at each level signed off that they had reported relevant information was not working well, as indicated by "+" sign on the arrow linking signoff system and poor risk governance nodes in Figure 1. All employees signed off within defined timeframes, but without asking many questions. Overall, it was considered as a part of compliance, and they assumed they were exonerated once they signed off. The sign off is usually considered an end-of-the-year exercise with a tick mark approach for compliance and audit. Compliance-based culture flourished and led to a vicious reinforcing loop of deterioration, as indicated in Figure 1 by the fact that both arrows within the loop linking the above-mentioned nodes have "+" signs. Quick Fix 2 was the setting of new roles and responsibilities relating to communication of risk (see Figure). The Board had set a tone from the top that if the first line did not report risks, they would be questioned later about why they did not report and held responsible if something went wrong.

Step 3: identify undesirable impacts

The quick fixes led to employees simply going through the motions for the sake of compliance and not understanding risks or the value of reporting. Also, they were not clear about their roles and responsibilities in risk governance; Quick Fix 2 also led to a vicious reinforcing loop (see "+" signs on both arrows linking Quick Fix 2 and Poor risk governance in Figure 1).

The head of ERM explained with an example why the understanding of risk was poor. In the UK business, for instance, there were 200 processes which specified the owner of the process, controls, possible failures in control and self-assessment techniques. The front-line managers were reporting risks based on "what is being asked" as a tick mark approach, rather than real ones. The company's deep pockets shielded it from the consequences of such reporting. The employees were neither able to understand the risks nor were they clear about what to report or not to report. The reporting failed to engage employees. The issue was how to engage 9,000 company employees working across 50 geographical locations and cultures. The poor understanding and lack of engagement of employees in risk governance led to risk under-reporting (see figure). Employees felt that if they reported more risks, more questions would be asked during audit and they had to show what they were doing about controls.

Quick Fix 2 made front-line managers responsible for reporting every possible risk and put penalties on non-reporting; this made them report as much as possible rather than risk the consequences of non-disclosure. The company was producing a risk report of around 700-1,000 pages which no executive could read. Comprehending this information was difficult task for the second line. Moreover, regulatory requirements changed frequently, which made the problem worse over time. This resulted in a defensive risk culture. Lack of understanding of risk and risk over-reporting were identified as undesirable impacts (see figure).

Step 4: identify the fundamental solution and implement it

As a result of Gap 2 where regulators insisted on better risk culture (see figure), the company identified poor communication between the first and second lines as the root cause of compliance-based and defensive risk cultures in the company. The reasons for poor communication were lack of understanding of risks and roles and responsibilities, which had led to Gap 2 in the first place through a reinforcing loop. Having identified the root cause, the company board set a vision to establish a cognitive risk culture where everyone in the organization understood the risks and their roles and responsibilities. Establishing a new vision provided a creative tension to senior executives (Senge, 1990). Company executives defined what they mean by cognitive risk culture and its characteristics:

> Risk culture underpins everything. By risk culture, we mean the tone from the top, understanding of risk at each line of defense, the system of governance you have, the roles/responsibility of your board, risk committee and the nature of the group policy framework and the high-level principles you need to adhere to. The risk management needs to articulate and deliver the practice. (Interview Transcript, Head ERM)

The other senior executives explained what they meant by high-level principles. The explicit expectations were linked to performance appraisal and therefore led to embeddedness of risk governance:

> The way the risk management and risk governance work, it is not the pointing out the fingers towards the fault. People have their individual roles and responsibilities. – I have my individual responsibilities and I am measured against these for my pay and performance. (Interview Transcript, CRO)

The company set a new expectation to understand the risks that could impact the achievement of long-term goals. To do so, senior executives were asked to enhance the dialogue with front-line employees to engage senior management in risk discussions to set a clear message:

> The risk is here to help not to hinder. (Interview Transcript, Group Risk Director)

Through the dialogue the company found that although the first line was not able to report risks appropriately to senior management, the reason lay in a lack of tone from the top. Therefore, multiple actions were taken: advancing the role of senior executives and senior management and introducing several tools across layers to bridge the gap. These changes enhanced the understanding of risks at the first and second lines, thereby helping create a cognitive risk culture. Company A's approach was therefore both top-down and bottom-up.

At Level 1 (top-down), the company advanced the role of senior executives and provided them tools such as ORSA Live App for their convenience in reading reports quickly and keeping them abreast with day to day risks. At Level 2 (bottom-up), the employees were provided with a tool management awareness of risks (MARs) to clarify their roles and responsibilities. Selected first-line employees were given the role of risk champion; an operational layer was thereby developed to bridge the gap between the first and second lines of defense.

The roles and responsibilities of senior executives were changed, i.e. group CRO would be responsible for company risk, conduct and compliance, and overall management of the assets worth over GBP 300bn and over 6 million customers across 50 countries. External communication to all stakeholders was another responsibility of the group CRO. The company hired one of the best CROs, highly experienced and well reputed in the insurance industry as group CRO, and re-allocated an actuary to the position of group risk director to drive the organizational growth. CRO, group risk director, and group fraud risk and supervision head report to group CRO (see details of roles in Table I).

A new understanding of risk and how it should be dealt with had been created. Company A executives found that some business experts had been given a role of divisional risk managers (DRM) and risk champions (RC) and attached to the central risk team headed by CRO. DRM and RC were not risk experts but business experts:

> The culture and other aspects involve some people who are supporting marketing, IT, finance and so on. There are called divisional risk managers. It is a part of second line risk function and all their time is spent in first line counter boxing, how the company can help in reporting. How can the company help you in using risk registers? The company spent lots of time on thinking about culture and tone from the top. (Transcript, CRO UK)

> Each division has risk champions [. . .]. Over a couple of years, we are doing regular theme days: Risk Monday, Risk Tuesday, Risk Wednesday, Risk Thursdays [. . .] to keep things alive at the forefront of people's mind. That's had been very successful exercise. (Slightly changed Transcript, Head ERM)

The tools deployed to bridge the gap between the first and second lines included MARs and ORSA App, explained below:

> We have an automated reporting system because we don't have all singing and all dancing. Manual reporting is tough. Management Awareness of Risk (MARs) is standardized which takes some of the manual element out of it. What a Group CRO and ERM committee see is not what a business manager would like them to see. It is gone again back to very different language. It helps people to manage the day to day business because it adds value. The other side, you should have an industry standard way of reporting. The problem is – executives don't want to read the long report but want to have complete information as well. When everything goes fine, the high level is

Executives	Reporting to	Roles and responsibilities
Group CRO	Group CEO and board	Overall responsible for company risk, conduct and compliance, and overall management of the assets External communication to all stakeholders
CRO	Group CRO and CEO	Furnish compliance, risk reporting to Group CRO and CEO, and implement ERM Handle internal communication vertically
Group risk director	Group CRO	Identify issues and root cause in risk governance Suggest change in the system Handle internal communication horizontally and networking with regulator Promote cognitive risk culture and trainings Understanding inter-relatedness of risk across groups, interpreting them and ways to enhance risk-based strategic decision making
Group fraud and supervision head	Group CRO	Supervision and surprise audits of over 50 regions and internal audit
Risk champions	Group Risk Director	Create risk awareness in the organization Create a dialogue between first line and second line

Table I. Structure of risk governance

> fine – the minute anything goes wrong, their first question – why did not you inform us? I don't have enough details; you should have flagged it to me. (Transcript, Head of Operations)

The tool enabled speedier communication of information, substantially reducing the defensive culture and promoting a cognitive risk culture. The first line was assured that their job would not be at risk in case of any mishap.

To make risk governance a daily activity rather than year-end activity, Company A installed an application "Live Own Risk and Solvency Assessment (Live ORSA)" on the iPads of each board member and member of executive committees. This ORSA App provided the latest results and information and helped to get away from the notion that ORSA is a once-a-year activity. Live ORSA App kept the Board abreast of organizational risks on an on-going basis and provided a higher degree of convenience comparing to reading 1,000-page reports.

Listing of actors' roles and expectations facilitated inclusion of risk in the performance appraisal system. It also assisted in identifying risks: when some common risks were observed across a few departments, senior management asked other department heads why they were not facing similar risks:

> When risk is reported, there is a lot of discussion about the risk because the operational team also challenge it. So, if the company has an operation risk person assigned to one area when risks are put up in our system, comparative analysis comes up. (Slightly changed quote, Transcript of Senior management)

Based on the Index, a MARs report is generated. The report has information on the processes to handle operational and conduct risks. This supported visibility and accountability for each unit and helped the first line managers to better score the risk exposures. MARs tool was particularly helpful in identifying capability gaps. Online courses in generic and specific areas and a risk graduate scheme for young professionals were offered.

The company clarified the role of DRM as a part of the second line, and RC as a part of the first line to bridge the communication gap between the first and second lines. The RCs are the highly motivated first line managers willing to communicate the value of adoption of good risk management practices across the first line and were given a generic duty to create risk awareness in the organization. DRMs (the second-line senior business executive) had the main role to understand the current and emerging risks of several units, issues in risk reporting and spreading the clear expectations of cognitive risk culture across divisions. One to one meeting with front-line managers were conducted to understand issues in-depth. Those common issues were discussed at board level and supported the review of controls in the next Board meeting:

> A key aspect is to make the people understand – this is your process, therefore, your risks. Don't say risk function is there to worry about. (Transcript, CRO UK)

The senior executive roles were changed from bureaucratic to enabler:

> Earlier, my particular role is something like bureaucratic and box-ticking, getting in their way, clue them what to do. So, I was working in last year, to replay back to them. This is what we discuss about enabling the business to act and have more confidence in the outcome. That's you can't really achieve by impactful power point slides, you can only achieve it through people genuine experience and building a platform of relationship. So, what I do, I have emails of these people, I am taking the opportunity whether I am in the UK or overseas to meet them. So that they can understand me and my objective and role. (Transcript, Group Risk Director)

Identification of poor communication as the root cause of ineffective risk governance led to several actions (see in Figure 1 arrows with "+" sign from identification of root cause to advanced role of risk champions, tools; communication between first and second lines; and advanced roles of second line). Each of these improved risk governance (see '-' sign from these nodes to poor risk culture). Each of these nodes is on a separate loop from identification of root cause to poor risk culture; the loops are therefore balancing, and keep the system in equilibrium.

The CRO of the company explained that the company follows a reverse testing exercise which is important to test the scenarios to check the solvency and viability of the company. Reverse testing is different from the traditional stress testing where stress scenarios are chosen based on expert knowledge or historical evidence. When roles and responsibilities were clearly set, and the risk reported by the first line was randomly tested on a monthly basis for checking whether they are really embedded in the system, it encouraged a cognitive risk culture in the company. When the second line of defense was executing this test, they also become aware of reality.

As the development of risk culture was a primary issue raised by FCA, it was considered a priority. However, the company also found issues related to auditing which was given the next priority. The company believed that in-depth analysis of a single issue at a time is more helpful than working on many issues at a time. This approach is easy to follow and in fact resolves many related issues at the same time; pursuing several issues often resolves none. Earlier when the company was using a linear approach the results were not up to expectations; systems thinking led to understanding of relationships, leading to several problems getting resolved at the same time.

Analysis

The regulatory trigger to improve risk culture has led to inculcate cognitive risk culture in the company. The company benefited in several ways by implementing the initiative to improve risk culture:

Revised three lines of defense model of risk governance

Change in risk culture led to improved roles in three lines of defense model. The first-line staff earlier reported the risks which management wanted them to tell rather than the actual risks. Also, they did not know what to inform and how much to inform. Several risk culture initiatives improved the fundamental understanding of risk and controls at the first line which was reflected in the quarterly sign off.

The job of the risk management team was to have an open dialogue with the first line. The reasons were attributed to:

> They don't fear to report at all. Part of this is found very recently, a tool to start discussion itself. So, we have an operational risk team that will see the visibility of these control issues and breaches. They can go and talk the people in the first line, and there is no more dialogue in a few years that how we can help and resolve it [. . .] It is also important that we have Management Awareness Rating System known as "MARS". (Transcript, Group CRO)

Previously, based on the traditional model of risk frequency and impact, it was believed that the role of the second line is to filter the top ten or so significant risks to discuss during the risk committee meeting (Bogodistov and Wohlgemuth, 2017). The redefined role of the second line was to act as a bridge between the Board which set the controls and operational staff who understand and accept or reject risks on a daily basis. The role of the second line is to match the two, namely, the controls set at the organizational level with the self-risk assessment by individuals.

One of the major issues for the third line is the horizon of risk and risk management. To audit effectively, the auditor needs to be aware of the on-going risk in the department. The Company developed a tool recently which is in the trial phase:

> There we are trying to work on the audit, and the people within the process of this operational risk process has to sign off something "A Management Outline System". There they have to do – they have outlined the key risk of the area, and we are just defining what area means, so they will define after they present that every quarter and sign off on it and keep it for their use. (Transcript, Group CRO)

Improved risk reporting

The case study demonstrated three type of risk reporting: under-reporting, over-reporting and state of improved risk reporting using several tools and advanced roles.

In compliance-based risk culture, the risk was not reported enough due to the fear factor as if it comes in the audit; regulator may ask questions. In defensive risk culture, more than enough risks were communicated without a proper understanding of risk what should be reported and what not. However, in a cognitive risk culture, the company followed:

> Manager knowing that we have a certain number of risks but that helps if there is an audit why because if I am the first line and I am a business person, and I am aware of my risks, and I have written down what I am doing about them, an audit cannot write them up. Because that is not a finding of any kind. If I already know that my risk model does not work and I have a corrective action plan that says over six months we are testing a new thing and it will be done. All audit can say at that time, "are you doing it timely or not timely", "is your action point enough" but they cannot write it as an issue. So, there is a huge incentive for management for being open and put it in the report. (Transcript of Actuary)

The case demonstrated progress in daily risk reporting such as Live ORSA App on iPads on executives to keep them abreast of ongoing risks on a daily basis. Simultaneously, it reduced the issue of over-reporting. The identification of capability gaps using MARs tool supported management in enhancing the capabilities of managers with adequate training. Enhanced understanding again led to cognitive risk culture.

Apart from tackling these issues, the company is also able to understand the risk horizon, its capability of dealing with the risk. All these improved the overall efficiency in terms of reducing time of reporting, reporting risk quickly, and thereby improving the company's capability to handle those risks.

Cognitive risk culture

The case study revealed three stages of risk culture: compliance-based risk culture, defensive risk culture and cognitive risk culture.

During Stage 1, the company made all the mistakes of non-system thinkers highlighted by Vester (1988). The company defined its goal as compliance, not as creating a cognitive risk culture that would serve the company to manage risks effectively. The company attempted to deal with the isolated problem of how the first line should report risks, not how the system as a whole should change to ensure that risk reporting would serve its purpose. As a consequence, the senior executives of the company claimed that they did not know what their risks were. The corrective actions were also not helpful as they led to defensive risk culture. At Stage 2, when new accountabilities were set without diagnosing the root cause, it resulted in over-reporting of risk. One of the major issues at the compliance stage was a reinforcing loop whereby a tick-box approach led to poor risk governance, which in turn led to the use of a tick-box approach for compliance.

In contrast, at Stage 3 (cognitive risk culture), the company used several elements of systems thinking. The company asked *why* questions to get at the root cause: why are the three lines of defense model not working well in practice? How are risk culture and risk governance related? To identify the root cause, the company began with the first line where actual risk is managed and found that the CSA method fails to engage employees and promotes a defensive attitude (Gigerenzer, 2015). Further, risk reporting is in general treated as compliance activity and year-end exercise. A dialogue resulted in understanding that the first and second lines were effectively operating in their own silos. Their solution was to improve the communication between the first and second lines to ensure that every employee understood the risks of their processes and their associated role and responsibilities in risk governance. Adding risk champions between the first and second lines helped both operations and integration. It also created an open culture for a discussion of risk.

The examination of the system to understand the root cause, and the changes made to it, constitute double feedback learning. As shown in Figure 1, it led to a better understanding of risks throughout the organization and created a cognitive risk culture. Before understanding the root cause, when the company was faced with a problem of under-reporting, it changed the responsibilities which led to over-risk reporting and poor understanding of risk; although this is seemingly a balancing loop, it is, in fact, a reinforcing loop in that a poor understanding of risks led to actions that perpetuated the poor understanding. Corrective actions post understanding of root causes, and several corrective actions in the system led to a cognitive risk culture and balancing loop which solved the problems.

Discussion and limitations

Although the literature has identified risk culture as a critical element of good risk governance, there is scant research on how to improve risk culture. This paper fills the gap by presenting a case study of an exemplar company whose solution can best be interpreted using systems theory. Our paper thereby contributes to both theory and practice. These contributions reinforce each other: the application to practice contributes to theory by contextualizing it, and support from theory gives confidence to generalize the findings from Company A's practice.

Our contribution to theory is to explicate the systems thinking view in the context of risk governance. Systems thinking enables us to identify that the company's original actions in implementing the signoff system and making front line staff responsible for reporting risks were quick fixes because they focused on immediate problems and did not consider system-wide side effects. On the other hand, when the company identified poor communication between the first and second lines as the root cause and created the role of risk champion and deployed tools for better communication, not only did communication improve but also created a cognitive risk culture that solved the risk under- and over-reporting issues. Therefore, systems theory allows us to draw conclusions while other theories mentioned in the literature do not. For example, the dynamic capabilities view (Bogodistov and Wohlgemuth, 2017) focuses on developing resilience; it is not able to explain the inter-relation of elements that iteratively influence each other.

Our contribution to practice is to show how systems thinking can be implemented to improve risk governance. Specifically, the steps followed by the company which others can potentially emulate are identify the original problem symptom, map the quick fixes, identify undesirable impacts and identify fundamental solution and implement it. Knowledge relating to risk is dispersed across the organization. Front-line employees have immediate knowledge of day-to-day risks, while the risk function and top management have knowledge of aggregate level exposures and strategy. Appropriate communication between them and the establishment of a cognitive risk culture is therefore likely to be the key to good risk governance, as Company A found.

It was the UK regulator's nudge that led Company A to identify the root cause and establish a cognitive risk culture. This suggests that regulators' insistence on improving risk culture could benefit even companies that already have a state-of-the-art risk governance system (i.e. the use of CSA, ERM and the three lines of defense model), as well as a tone at the top that supports risk governance. Our literature review suggests that there are many organizations in this state. Our findings therefore suggest that other regulators could benefit from emulating the UK example (as some already have, e.g. Australian PRA).

A limitation of our research is that our study stopped before the company dealt with the relation between the second and third lines of defense. Future research can fill this gap. It can also determine other potential solutions, refine the solution of Company A and determine conditions under which different solutions work best. As mentioned above, Company A already had a state-of-the-art risk governance system; our findings may not generalize to settings where risk governance is well below the state of the art.

Notes

1. Control Self-Assessment (CSA) was introduced in Gulf Canada in 1985; the early pioneers adopted CSA in the 1990s, and within five years CSA was widely accepted by internal auditors worldwide for risk assessment. In the year 2000, it was rated as the default internal audit methodology (Melville, 1999). Its value is still being debated as some authors consider it a powerful way to improve organization's control environment, audit coverage and understanding of risk (Allegrini and D'Onza, 2003) while others consider it a tick box approach for compliance and argue that companies who implement CSA don't know their risk (Lieng-Seng, 2005).

2. The Sharma Report, named after Paul Sharma, set the strong plinth of Solvency II directive due to high attention on the study of actual failures of insurance companies using a survey and 21 detailed case studies.

References

Abraham, S. and Shrives, P.J. (2014), "Improving the relevance of risk factor disclosure in corporate annual reports", *The British Accounting Review*, Vol. 46 No. 1, pp. 91-107.

Ackoff, R.L. (1994), "Systems thinking and thinking systems", *System Dynamics Review*, Vol. 10 No. 2-3, pp. 175-188.

Aebi, V., Sabato, G. and Schmid, M. (2012), "Risk management, corporate governance, and bank performance in the financial crisis", *Journal of Banking and Finance*, Vol. 36 No. 12, pp. 3213-3226.

Agarwal, R. and Ansell, J. (2016), "Strategic change in enterprise risk management. Strategic change", *Strategic Change*, Vol. 25 No. 4, pp. 427-439.

Allegrini, M. and D'Onza, G. (2003), "Internal auditing and risk assessment in large Italian companies: an empirical survey", *International Journal of Auditing*, Vol. 7 No. 3, pp. 191-208.

Argyris, C. and Schon, D. (1978), *Organizational Learning: A Theory of Action Approach*, Addision Wesley, Reading, MA.

Association of British Insurers (ABI) (2014), "Key 2014", available at: www.abi.org.uk/~/media/Files/Documents/Publications/Public/2014/KeyFacts/ABIKeyFacts2014.pdf

Authority, F.S. (FSA) (2011), "Enhancing frameworks in the standardised approach to operational risk–guidance note", January, available at: www.fsa.gov.uk/pubs/guidance/guidance11.pdf

Beasley, M., Branson, B. and Pagach, D. (2015), "An analysis of the maturity and strategic impact of investments in ERM", *Journal of Accounting and Public Policy*, Vol. 34 No. 3, pp. 219-243.

Bogodistov, Y. and Wohlgemuth, V. (2017), "Enterprise risk management: a capability-based perspective", *The Journal of Risk Finance*, Vol. 18 No. 3.

Bromiley, P., McShane, M., Nair, A. and Rustambekov, E. (2015), "Enterprise risk management: review, critique, and research directions", *Long Range Planning*, Vol. 48 No. 4, pp. 265-276.

Deighton, S.P., Dix, R.C., Graham, J.R. and Skinner, J.M.E. (2009), "Governance and risk management in United Kingdom insurance companies", *British Actuarial Journal*, Vol. 15 No. 3, pp. 503-556.

Dörner, D., Kreuzig, H.W., Reither, F. and Stäudel, T. (1983), "Lohhausen: Vom umgang mit unbestimmtheit und komplexität".

Douglas, M. (2013), *Risk and Blame*, Routledge, Abingdon.

Eisenhardt, K.M. (1989), "Building theories from case study research", *Academy of Management Review*, Vol. 14 No. 4, pp. 532-550.

Eisenhardt, K.M. and Graebner, M.E. (2007), "Theory building from cases: Opportunities and challenges", *Academy of Management Journal*, Vol. 50 No. 1, pp. 25-32.

Eling, M., ; Schmeiser, H. and Schmit, J.T. (2007), "The solvency II process: overview and critical analysis. Risk managment and", *Risk Management and Insurance Review*, Vol. 10 No. 1, pp. 69-85.

Eling, M. and Marek, S.D. (2014), "Corporate governance and risk taking: evidence from the UK and german insurance markets", *Journal of Risk and Insurance*, Vol. 81 No. 3, pp. 653-682.

FSB(2014), "Guidance on supervisory interaction with financial institutions on risk culture", April, available at: file:///C:/Users/s0970797/Downloads/FSB_RiskCulture_0704.pdf

Gigerenzer, G. (2015), *Risk Savvy: How to Make Good Decisions*, Penguin, London.

Gontarek, W. (2016), "Risk governance of financial institutions: the growing importance of risk appetite and culture", *Journal of Risk Management in Financial Institutions*, Vol. 9 No. 2, pp. 120-129.

Judge, W.Q. and Zeithaml, C.P. (1992), "Institutional and strategic choice perspectives on board involvement in the strategic decision process", *Academy of Management Journal*, Vol. 35 No. 4, pp. 766-794.

Kim, D.H. and Senge, P.M. (1994), "Putting systems thinking into practice", *System Dynamics Review*, Vol. 10 Nos 2/3, pp. 277-290.

Kleffner, A.E., Lee, R.B. and Mcgannon, B. (2003), "The effect of corporate govenance on the use of enterprise risk management: Evidence from Canada", *Risk Management and Insurance Review*, Vol. 6 No. 1, pp. 53-73.

Lam, J. (2000), "Enterprise-wide risk management and the role of the chief risk officer", white paper, ERisk. com, 25 March.

Lee, L.S. and Green, E. (2015), "Systems thinking and its implications in enterprise risk management", *Journal of Information Systems*, Vol. 29 No. 2, pp. 195-210.

Mikes, A. (2008), "Chief risk officers at crunch time: Compliance champions or business partners?", *Journal of Risk Management in Financial Institutions*, Vol. 2 No. 1, pp. 7-25.

Mikes, A. (2009), "Risk management and calculative cultures", *Management Accounting Research*, Vol. 20 No. 1, pp. 18-40.

Mikes, A. and Kaplan, R.S. (2015), "When one size doesn't fit all: evolving directions in the research and practice of enterprise risk management", *Journal of Applied Corporate Finance*, Vol. 27 No. 1, pp. 37-40.

Mintzberg, H. (1979), "An emerging strategy of 'direct' research", *Administrative Science Quarterly*, Vol. 24 No. 4, pp. 582-589.

O'Donnell, E. (2005), "Enterprise risk management: a systems-thinking framework for the event identification phase", *International Journal of Accounting Information Systems*, Vol. 6 No. 3, pp. 177-195, available at: http://linkinghub.elsevier.com/retrieve/pii/S146708950500031X (accessed 7 November 2012).

Paape, L. and Speklè, R.F. (2012), "The adoption and design of enterprise risk management practices: an empirical study", *European Accounting Review*, Vol. 21 No. 3, pp. 533-564.

Paté-Cornell, E. and Cox, L.A. (2014), "Improving risk management: from lame excuses to principled practice", *Risk Analysis : an Official Publication of the Society for Risk Analysis*, Vol. 34 No. 7, pp. 1228-1239.

Pernell, K., Jung, J. and Dobbin, F. (2017), "The hazards of expert control: chief risk officers and risky derivatives", *American Sociological Review*, Vol. 82 No. 3, pp. 511-541.

Renn, O. (2008), *Risk governance: coping with uncertainty in a complex world*, Earthscan, Sterling, VA.

Senge, P. (1990), *The Fifth Discipline*, Doupleday Currence, New York, NY.

Sheedy, E. and Griffin, B. (2018), "Risk governance, structures, culture, and behavior: a view from the inside", *Corporate Governance: An International Review*, Vol. 26 No. 1, pp. 4-22.

Spira, L.F. and Page, M. (2003), "Risk management: the reinvention of internal control and the changing role of internal audit", *Accounting, Auditing and Accountability Journal*, Vol. 16 No. 4, pp. 640-661.

Vester, F. (1988), "The biocybernetic approach as a basis for planning our environment", *Systems Practice*, Vol. 1 No. 4, pp. 399-413.

Viscelli, T.R. Hermanson, D.R. and Beasley, M.S. (2017), "The integration of ERM and strategy: implications for corporate governance", Accounting Horizons.

White, D. (1995), "Application of systems thinking to risk management: a review of the literature", *Management Decision*, Vol. 33 No. 10, pp. 35-45.

Yin, R.K. (2017), *Case Study Research and Applications: Design and Methods*, Sage publications, Thousand Oaks, CA.

Further reading

Aabo, T., Fraser, J.R.S. and Simkins, B.J. (2005), "The rise and evolution of the chief risk officer: enterprise risk management at hydro one", *Journal of Applied Corporate Finance*, Vol. 17 No. 3, pp. 62-75.

About the authors

Ruchi Agarwal is a Senior Researcher at Indian School of Business (ISB), Hyderabad, and PhD from University of Edinburgh Business School, UK. Her thesis is titled "Implementation of Enterprise Risk Management (ERM) Practices." She is a fellow of the Insurance Institute of India (FIII) and certified with an Advanced Diploma from the Chartered Institute of Insurance (ACII), UK. She has been actively involved in consulting and business analysis with top MNCs in international markets over the past 12 years. Ruchi is currently undertaking research in risk governance, fraud risk, ERM, risk disclosures and strategic change. Ruchi Agarwal is the corresponding author and can be contacted at: ruchiagarwal1982@gmail.com

Sanjay Kallapur (PhD, Business Economics, Harvard University) is a Professor of Accounting and a Deputy Dean at the Indian School of Business (ISB). Prior to joining the ISB, he was a tenured Associate Professor at the Krannert School of Management, Purdue University. He conducts empirical research in financial and managerial accounting, auditing and corporate governance. From 2008 to 2011, he was an editor of *The Accounting Review* and is currently on the editorial boards of the *Australian Journal of Management* and *Journal of Financial Reporting*.