A theory of enterprise risk management

Håkan Jankensgård

Abstract

Purpose – *The purpose of this paper is to develop a theory of enterprise risk management (ERM).*

Design/methodology/approach – *The method is to develop a theory for ERM based on identifying the general risk management problems that it is supposed to solve and to apply the principle of deduction based on these premises.*

Findings – *ERM consists of risk governance, which is a set of mechanisms that deals with the agency problem of risk management and risk aggregation, which is a set of mechanisms that deals with the information problem of risk management.*

Research limitations/implications – *The theory, by identifying the central role of the Board of Directors, encourages further research into the capabilities and incentives of directors as determinants of ERM adoption. It also encourages research into how ERM adoption depends on proxies for agency problems of risk management, such as a decentralized company structure.*

Practical implications – *The theory encourages Boards of Directors to focus on understanding where the under and over management of risk are likely to be greatest, as opposed to the current practice of mapping a large number of risk factors.*

Originality/value – *The theory complements existing theory on corporate risk management, which revolves around the role of external frictions, by focusing on internal frictions in the firm that prevent effective risk management. It is the first work to delineate ERM* vis-a-vis *existing risk theory.*

Keywords *Board of directors, Enterprise risk management, Risk governance, Economic capital*

Paper type *Research paper*

Håkan Jankensgård is based at Lunds Universitet, Helsingborg, Sweden.

Enterprise risk management (ERM) is, at a fast clip, establishing itself as the dominant paradigm of corporate risk management. The past two decades have witnessed a large increase in the demand for ERM and improved governance of firms' risks more generally. Pressure from outside stakeholders has been an important influence on this development reflecting corporate scandals involving excessive risk-taking (Gates, 2006).

The distinguishing feature about ERM is that it represents risk management as viewed from the perspective of the firm's top executives and directors. It is not about project risk or investment risk or any particular risk. The perspective taken is rather how to manage the net, aggregated risk exposures of the entire enterprise and how to frame the firm's willingness and capacity to accept such exposures.

In this paper, I submit a theoretical analysis of ERM. The analytical tools of corporate finance are used to derive a description of two general risk management problems faced by firms. ERM is proposed as the solution adopted by the firm's Board of Directors to address these problems, which revolve around agency and information asymmetries *within* the firm. Because of these imperfections, a firm may engage in formal risk management even when external frictions are absent or fail to use risk management when external frictions are at hand. The theory therefore complements traditional corporate risk management theory, which focuses on eliminating the effects of frictions that exist *outside* the firm, such as taxes or contracting problems between the firm and other market actors (Smith and Stulz, 1985; Froot *et al.*, 1993).

Received 18 February 2018
Revised 19 August 2018
7 November 2018
Accepted 7 January 2019

Why is a theory of ERM desirable in the first place? ERM is sometimes described as an evolving phenomenon which may take many years before it becomes codified and practiced in a consistent way (Fraser *et al.*, 2015). In this view, there is an ongoing search for best practices that eventually will settle into a body of concepts and practices that will constitute ERM. While there is certainly something to be said for allowing robust best practices to evolve, in a Darwinian-like manner, the problem with the *laissez-faire* approach is that it leaves ERM vulnerable to capture by special interests, such as fee-hungry consultants and the expediency of key actors. As will be argued extensively in this paper, risk management is replete with agency problems. Simply letting practice evolve presents us with the risk that these interests dictate the evolution of ERM and its eventual codification. A stronger emphasis on theoretical analysis may to some extent counter these forces, and both the thinking and practice of ERM stand to benefit from a more rigorous description, at the theoretical level, of the problems it is supposed to solve.

A more theoretical approach may also help address the demarcation problem of ERM. At first glance, there appears to be a broad consensus that ERM is about taking an integrated approach to managing a firm's risks so as to provide reasonable assurance that the firm's objectives are met. A closer look, though, reveals it to be a sprawling subject. Some authors argue that ERM ought to be "strategic" in its outlook and mesh with the firm's strategic decision-making (COSO, 2016). Others opt for a more quantitative approach, framing ERM in terms of statistical summary measures of risk concerning financial "bottom lines" (Alviniussen and Jankensgård, 2009). Yet others remain within the basic framework of ERM as tool for risk control, driven by "an accounting and auditing logic" (Power, 2009). Bogodistov and Wohlgemuth (2017), on the other hand, seek to integrate ERM into the resource-based view and dynamic capability framework, whereby a firm directs its risk management resources toward protecting and enhancing the firm's core competencies. It hardly needs pointing out that a concept that is made out to be all-encompassing is at risk of becoming seriously diluted. If ERM is anything one wants it to be, it may also be approaching the point where the term itself becomes near-meaningless.

In the present theory, the Board of Directors adopts ERM to address two general risk management problems faced by firms. The first is the problem of getting managers, who may be self-serving and are under the influence of behavioral biases, to undertake risk management actions that are in the best interest of the firm's investors. I will refer to this as the "agency problem of corporate risk management" (Jensen and Meckling, 1976; Smith and Stulz, 1985; Tufano, 1998). The second is the problem of collecting information about risk exposures in a timely, intelligible and relevant format, so as to be used to support centralized decision-making regarding the firm's total risk-return profile (including the deployment of economic capital). This is referred to as "the information problem of corporate risk management". The problem occurs because decisions are usually delegated in an organization, and the operating units have information not freely available to the Board of Directors (Harris and Raviv, 1996). Weak internal capabilities to create a big-picture view of the firm's aggregate net exposures is regarded as having contributed to the financial crisis of 2007-2009 and is considered one of the major challenges in risk management today (Basel Committee on Banking Supervision, 2013).

ERM consists of risk governance and risk aggregation. The Board of Directors, on behalf of shareholders, adopts risk governance to deal with the agency problem of risk management. As will be discussed extensively in this paper, managers are prone to undermanage one category of risks (low probability-high impact risks) and over-manage another category of risks (high probability-high salience [HPS] risks), which reduces the expected mean of future cash flows. Risk governance is a set of mechanisms that counteract the incentives and behavioral biases that lead to these problems. The Board of Directors adopts risk aggregation to deal with the information problem of risk management. Risk aggregation is a set of mechanisms used to ensure that information about risk is aggregated and processed

in such a way that it supports the task of assessing and managing the firm's total risk-return profile. As will be discussed later in the paper, the theory accounts for most observed ERM practices today.

ERM is related to two optimization problems. When risk governance is applied successfully, the firm has an optimized portfolio of business risks, i.e. risks that arise as a natural consequence of doing business. The agents take risk management decisions unaffected by conflicts of interests and behavioral biases, thus maximizing the expected mean of future cash flows. Using the information made available through risk aggregation, the firm then optimizes its total risk-return profile. In this step, the firm's aggregate business risk is balanced against the capacity for risk-taking provided by the firm's economic capital (Alviniussen and Jankensgård, 2009). Economic capital, various definitions of which are discussed in this paper, acts as a cushion to potential losses that may occur in the firm's business operations. While it reduces the expected costs associated with various forms of financial distress, economic capital is costly, so the Board of Directors trades off the costs and benefits of keeping economic capital[1].

The theory relates primarily to Nocco and Stulz (2006). It bears more than a passing resemblance to their view of ERM as providing both "micro" and "macro" benefits, where the macro-benefits refer to the role of risk management in optimizing the total risk of the firm [2]. Nocco and Stulz do not articulate the problems of over- and under-management of risk, whereas I attempt to recognize the full extent to which risk management takes place within the context of an agency relationship and information asymmetries internal to the firm. Mikes and Kaplan (2015) set out a very different theory of ERM. They argue in favor of a contingency theory that seeks to identify various design parameters that can explain the large observed variation in how ERM is implemented. Their theory stresses that there is no one universal form of ERM that will maximize firm value. Rather, each firm chooses from the available design parameters to obtain an "ERM-mix" that is suitable given its particular circumstances. The contingency theory of ERM is strongly in accordance with the evolving search for best practices discussed earlier.

The present theory, on the other hand, stresses a set of underlying themes that should be of concern to the Board of Directors in any firm. The under- and over-management problems of risk are affected by behavioral biases and incentive schemes that are common in practice. Thus, a board adopting ERM will do well to first identify how behaviors and incentives influence risk management practices in the firm (Lynch, 2008). Rather than sorting risks into the usual categories of operational, strategic and market risks, the theory encourages directors of the board to classify risks according to where the problems of over- and under-management of risk may be the most severe. Another theme is that of information about risk. The need to secure the supply of risk information, and to process it analytically to support centralized decision-making, suggests a focus on developing sufficient data infrastructure and analytical capabilities. This would serve to bridge the gap between risk reporting (which is where most ERM programs today "stop") and the financial analysis needed to determine economic capital (Alviniussen and Jankensgård, 2009).

The theory presented in these pages sheds new light on one of the most consistent findings in the empirical literature, which is that large firms are more likely to adopt ERM (Gatzert and Martin, 2015). Because large firms are less likely to experience financial distress, this finding is inconsistent with traditional risk theory emphasizing financial distress risk as a justification for risk management (Smith and Stulz, 1985). According to the logic of the theory presented here, the propensity of larger firms to use ERM makes sense because they are also more likely to be conglomerates with multiple operating units, which exacerbates the information and agency problems of risk management[3].

The theory also provides new research directions for empirical research on ERM. It predicts that ERM should be more prevalent in firms that have high levels of agency costs of risk

management, and in those in which internal information asymmetries are the largest. This suggests a focus on large and decentralized organizations. Proxies for the number of operating units and their degree of autonomy *vis-à-vis* the corporate center can be used in tests of the determinants of ERM. Such variables should also condition the value-effects of ERM that some researches have begun to explore (Hoyt and Liebenberg, 2011). Jankensgård (2015) is an example of a study that incorporates information concerning the extent of centralization into the research design. In addition, the theory's presumption about an enlightened, empowered and value-maximizing Board of Directors suggests an emphasis on empirical proxies for the abilities and incentives of the firm's directors. Such an association is reported by Daud *et al.* (2011).

2. Existing enterprise risk management frameworks – overview and criticism

The principles of holistic risk management that underpin ERM were first developed in the mid-1990s by the people behind the Australian risk management standard (RM 4360) with later additions by their Canadian counterparts. Against the backdrop of corporate scandals involving unethical conduct, the Committee of Sponsoring Organizations of the Treadway Commission (COSO)[4] decided to extend its internal audit-framework to cover ERM, and the first COSO ERM framework was published in 2004. This document has subsequently become a standard reference in discussions on ERM implementation alongside ISO 31000 (2009), which is an internationally agreed standard for the implementation of risk management principles. The purpose of frameworks such as ISO 31000 is to ensure compliance, assurance and to improve decision-making.

COSO (2004) defines ERM as a process designed to identify events that could affect the firm and to manage these risks so as to keep risk within the firm's "risk appetite", thus providing reasonable assurance that its objectives are met. This process is to be carried out by personnel at all levels of the organization, including the firm's Board of Directors. Risk in ERM frameworks is generally taken to mean failure to achieve various targets set by management. This is very clearly stated in ISO 31000 (2009), where risk is defined as "the effect of uncertainty on objectives". To describe the COSO framework, Power (2009) invokes the metaphor of a thermostat. Firms seek to identify all material risks and to design controls for them, producing a residual risk consistent with a target risk appetite, akin to how a thermostat adjusts to changes in the environment subject to pre-given target temperature.

Aven and Aven (2015) criticize the emerging practice of target-centered ERM, which they label the "no-goal-no-risk"-approach (goal achievement risk). According to these authors, more or less arbitrary targets are set throughout the organization. Risks are then managed with reference to these locally set goals, regardless of whether they make sense for the firm as a whole. This goal-setting machine may produce the wrong focus, and yield results that are not optimal from the perspective of the enterprise (subgoal optimization).

Notably, ERM frameworks are framed in terms of a definition of a process, rather than in terms of a description of the fundamental problems that ERM attempts to solve. A useful theory of ERM, I argue, should revolve around an analysis of the general risk management problems that it is a response to. What are these general risk management problems? They are, as I will discuss extensively, impediments to effective risk management created by agency and information problems within an organization. Decisions are typically delegated in a firm, and the business units have information not freely available to the Board of Directors (Harris and Raviv, 1996). Managers are known to part with information only reluctantly (Nagar *et al.*, 2003). Decentralized decision-making therefore gives rise to information asymmetries between the units and the upper echelons of the firm, which makes it more difficult to comprehend and manage the firm's risk-return profile. As suggested by Aven and Aven (2015), the risk management agendas of the units may also differ markedly from what would be desirable from the shareholders of the company, resulting in either "too much" or "too little" risk management. These are, in broad terms, the information and

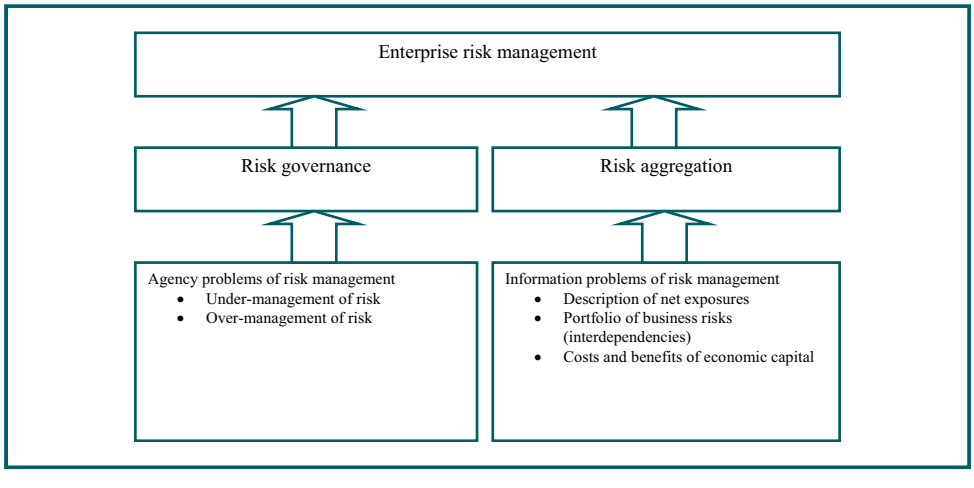
agency problems of risk management, and ERM will here be viewed as the solution adopted by the Board of Directors to address these problems.

3. A theory of enterprise risk management

A synopsis of the theory is as follows. Silos (operating units as well as corporate functions) exist and are desirable to gain from the benefits of specialization. The silos are run by agents that have incentives and/or behavioral biases that lead to suboptimal risk management decisions in the form of over-management of a certain category of risks and under-management of another category ("the agency problem of corporate risk management"). The Board of Directors is risk-neutral; represents the interests of shareholders; and pursues the goal of maximizing the long-term value of the firm. The Board is "enlightened" in the sense that it understands the nature of the agency problem of risk management. It is also empowered in that it can mobilize corporate resources. But because of the structure of decentralized decision-making, the Board lacks access to full information about the risks that the silos are exposed to and their risk mitigation actions, and consequently cannot assess the firm's overall risk profile ("the information problem of corporate risk management"). The directors therefore undertake measures to aggregate information about net risk exposures centrally in the organization. The Board adopts monitoring mechanisms and incentive systems to address the agency problems of risk management. To carry out risk governance and risk aggregation, the Board invests in new risk management capabilities in the organization. The amount of resources invested in these capabilities is proportional to the perceived costs related to agency and information problems of risk management in the firm. Thanks to the aggregation of risk information, the Board is able to deploy the appropriate amount of economic capital to support the level of risk-taking inherent in the firm's portfolio of business risks, taking into consideration interdependencies among risk exposures across the various operating units. Economic capital is costly and the Board trades off these costs against various costs related to the risk of financial distress. The theory is summed up in Figure 1.

Before proceeding, it is important to clarify the role of the Board of Directors in this theory. It treats the board as a rational and empowered entity that, on behalf of shareholders, dispassionately monitors various agents in a decentralized organizational structure and enforces sound risk management. Many observers would question that boards typically possess these attributes. The point, however, is rather to analyze how an entity that is simultaneously watching after the interest of shareholders as well as able to command

Figure 1 ERM



corporate resources would respond to the agency and information problems of risk management. In principle, top management could have performed this role so long as they are perfectly incentivized to act in the interest of the company. However, boards are structurally closer to shareholders, given their fiduciary duty to promote the company's interests (in the USA, this occurs through the Duty of Loyalty and Duty of Care in corporation law). It is widely recognized today that boards are responsible for informed risk oversight as part of this fiduciary duty, consistent with the view in academic finance that boards, as an institution, have emerged as a partial solution to the agency problem caused by the separation of ownership and control (Hermalin and Weisbach, 2003).

Another point worth observing is that the theory makes no mention of the other supposed roles of the board beyond its control function, namely to provide resources and services to the firm (Zahra and Pearce, 1989). While these aspects fall outside the scope of analysis, it is implicit that in implementing an ERM program the directors of the board would also be in a position to contribute valuable resources to such an undertaking in the form of knowledge, connections, experience, etc. Finally, the assumption that the directors are empowered and can influence the use of corporate resources does not mean they run the firm on a day-to-day basis. Rather, this influence can be thought of as stemming from their power to set agendas and create expectations that managers and committees address specific questions.

4. The information problem of corporate risk management – a closer look

4.1 Motivation

Existing theory on corporate risk management tends to assume full knowledge about all relevant decision parameters. In reality, given the complexity of firms and the fast-changing world economy, there is much evidence to suggest that managers in fact struggle to understand their own exposures. Aggregating risk information is widely acknowledged as one of the main risk-related challenges facing organizations today. Flawed risk aggregation is perceived to have contributed to some of the disasters that befell financial institutions during the crisis that erupted in 2007. In the words of the Basel Committee on Banking Supervision (2013): "Many banks lacked the ability to aggregate risk exposures and identify concentrations quickly and accurately [. . .] across business lines and between legal entities. Some banks were unable to manage their risks properly because of weak risk data aggregation capabilities [. . .]". This sentiment is echoed in reports by a large number of professional organizations. The European Central Bank (2018) concludes that: "One key lesson from the financial crisis was the need for more information on risk to make sound business decisions. IT, data architecture and related business processes were not sufficient to support the broad management of [. . .] risks".

Ultimately, the information provided by risk management systems should be sufficient to enable a continuous assessment of the firm's total risk-return profile. In this section, drawing on the available literature, the elements necessary for completing this task are identified and discussed. While the deployment of economic capital is emphasized, aggregating risk information centrally has other benefits too, such as facilitating the netting of exposures, the co-ordination of risk mitigation activities and the external communication of risk management.

4.2 Description of net exposures

The first challenge is to make sure that information about risk exposures exists in the first place and is of sufficient quality (the quality criterion). To be comparable, this information must be expressed in a standardized, quantitative format (the intelligibility criterion, see Nocco and Stulz, 2006). This is normally taken to be the probability-impact dimensions of each risk, where the latter is expressed in the relevant base currency. Subsequent to

producing this information, it must reach the upper echelons of the organization through a reporting process (the timeliness-criterion). An additional challenge at this stage is to prevent information overload by overwhelming top decision-makers with data (the relevance criterion)[5]. Speier *et al.* (1999) define information overload as a situation where the amount of input into a system exceeds its processing ability.

4.3 Description of the portfolio of residual risks

The list of net exposures with their corresponding probability-impact estimates has an inherent limitation, which is that any such list will ultimately be a compilation of risks, as they were perceived at a particular point in time. While useful for many purposes, such as discussing specific risk mitigation actions, the list will not convey more than rudimentary information concerning the overall risk level that is produced by these risks when considered jointly. Since Markowitz (1952), the standard view in the finance-literature is that risks should be considered on a portfolio basis. This essentially means aggregating the characteristics of the various individual risk exposures into a single summary metric, and gauging the risk-return characteristics of this new "portfolio" instead.

A fundamental feature of a portfolio of risks is that any tendency for the individual risk factors to co-vary will impact the overall risk (Markowitz, 1952). This information is not revealed by the static list of net exposures. A firm that wishes to describe its aggregate portfolio of business risks in terms of probability-impact thus faces the additional information requirement of mapping out and assessing interdependencies, e.g. by quantifying correlation coefficients (Alviniussen and Jankensgård, 2009).

4.4 Costs and benefits of economic Capital

After a description of the probability-impact-covariation dimensions of the firm's portfolio of business risks has been put in place, the task remains to conceptualize and quantify the ability of the firm's balance sheet to absorb potential losses in this portfolio ("economic capital"). Economic capital comes with both costs and benefits that have to be gauged. To make the value-maximizing decision, the Board of Directors needs information on these various components.

Economic capital, as the term is normally applied, refers to the amount of capital needed to ensure that the firm stays solvent in a worst-case scenario (Nocco and Stulz, 2006). This framing suggests a focus on solvency and survival which is a key priority of banks and their regulators. It also implies a focus on the volatility of value: a bank is considered insolvent when the value of its assets falls below the value of its liabilities. According to Alviniussen and Jankensgård (2009), applications of the concept of economic capital in non-financial firms may be better served by a focus on contingent liquidity. The argument is that the costs of financial distress begin to accumulate well ahead of the point at which the firm is declared insolvent[6]. Experiencing liquidity shortfalls and investing below the optimal level can occur without the firm being technically insolvent. They define "risk capacity" as the amount of liquidity the firm is able to mobilize, on efficient terms, to support its cash commitments (including debt obligations and investment spending) in the event that the firm's internally generated cash flow is insufficient to cover these commitments. Risk capacity increases with the amount of liquid assets on the firm's balance sheet, spare borrowing capacity (e.g. in the form of pre-arranged lines of credit) and any derivative instruments that provide payoffs in scenarios in which cash flows are insufficient to meet cash commitments[7].

On the positive side, economic capital provides benefits in that it reduces the expected costs of financial distress. These include direct costs related to bankruptcy (Smith and Stulz, 1985), decreased product-market competitiveness (Shapiro and Titman, 1986), having to make forced asset sales at a discount to fair value (Shleifer and Vishny, 1992) and

investing below the optimal level (Froot *et al.*, 1993). These potential costs are firm-specific and have to be assessed. On the negative side, carrying economic capital comes with firm-specific costs that also need to be described (Alviniussen and Jankensgård, 2009). Using equity capital is more expensive as it means giving up the tax advantage of debt. Excess cash is costly because unproductive liquid assets are kept on the firm's balance sheet. Derivative instruments are associated with a range of costs, such as transaction costs and reduced transparency.

To sum up this section, the information problem of risk management consists of organizational challenges related to collecting the appropriate data on net exposures, interdependencies and costs and benefits of economic capital and formatting these data to support decision-making. This encompasses both ensuring the supply of raw data and developing analytical capabilities.

5. The agency problem of corporate risk management – a closer look

5.1 Motivation

The agency problem refers to a conflict of interest between the principal and the agent, who is contracted by the principal to carry out a task. In the setting of a firm, it reflects the separation of ownership and control of the firm's assets (Jensen and Meckling, 1976). Managers may shirk, engage in self-dealing, seek to maximize assets under control and generally pursue "pet projects" that increase their utility. There is a wealth of empirical evidence documenting that agency costs in the corporation are real, pervasive and potentially substantial (Shleifer and Vishny, 1997).

One subset of the agency problem concerns the firm's risk-taking. On a general level, the agency problem of risk management occurs when the agent and the principal have different views on the amount of residual risk to be borne by the firm. According to Smith and Stulz (1985), managers will tend to be more risk-averse than the firm's shareholders because a larger fraction of their wealth, including their human capital, is tied to the firm's success and continued existence. Given their control over operating policies, managers have the ability to set the level of risk that maximizes their own utility, as opposed to the level that maximizes shareholder value.

The agency problem of corporate risk management can manifest itself in two different ways: either by over-managing risk or by under-managing it. The problem of under-management of risk refers to a situation where the agent omits to undertake a risk mitigation action when this would in fact be desirable for the principal. In this case, the risk mitigation has a positive net present value by itself[8]. That is, the cost of implementing the risk mitigation action is less than the expected cost of retaining the exposure to the risk. The problem of over-management of risk refers to situations in which agents undertake risk mitigation actions that are in fact undesirable from the viewpoint of a risk-neutral principal, i.e. the agent overspends resources on mitigating the risk. In this case, the principal prefers the agent to refrain from risk mitigation because the action has a negative net present value on its own terms: the expected benefits are not commensurate with the cost of implementation.

The agency problem emphasizes differing views on what is an appropriate amount of residual risk, but people also suffer from various biases that affect the quality of their decision-making. These biases create an extended agency problem of risk management[9], according to which differing incentives and behavioral biases interact to produce risk mitigation decisions that are not in the best interest of the principal. The behavioral aspect of risk management is rarely acknowledged but important, as the studies presented in the following two sections illustrate.

5.2 Under-management of risk

The under-management of risk problem generally occurs because individuals suffer from behavioral biases[10] and/or flawed incentives to undertake the appropriate risk mitigation action. I argue here that this is more liable to occur for a certain class of risks, referred to as high impact–low probability (HILP) risks. Three behavioral biases are reviewed – oversimplification, over-optimism, and overconfidence – that conjoin to produce the under-management of risk problem.

Our inability to deal well with HILP risks is a famous theme in Taleb's (2007) book *The Black Swan*. According to Taleb, the human mind copes poorly with randomness, and we are notoriously bad at predicting, or even granting the possibility of, those highly unlikely but highly consequential events that disproportionally affect the world around us. As information is costly to obtain, store and retrieve, humans search for simplifying rules that reduce the dimensions of the issue at hand. Because of this excessive simplification, we leave ourselves vulnerable to "Black Swans": events that lie outside the realm of regular expectations but can have a large, or even extreme, impact[11].

Our tendency to over-simplify matters, and thus become blind to the potential impact of unlikely events, is joined by over-optimism in creating the problem of under-management of risk. According to Kahneman and Tversky (1979), people tend to produce plans and forecasts that are unrealistically close to best-case scenarios, and which could be improved upon by checking the statistics of similar cases in the past ("the planning fallacy"). The planning fallacy is the consequence of a pervasive optimistic bias, because of which most of us tend to view the world as more benign than it really is (Kahneman, 2011). This bias has major consequences for corporate risk taking. Kahneman (2011) summarizes, "The evidence suggests that an optimistic bias plays a role – sometimes the dominant role – whenever individuals or institutions voluntarily take on significant risks. More often than not, risk takers underestimate the odds they face, and do not invest sufficient effort to find out what they are".

Overconfidence is a third behavioral bias that bears on the problem of under-management of risk. In this case, humans are prone to overrate their own abilities (the above-average effect, Svenson, 1981) and the level of control they have over a situation (Langer, 1975). Plous (1993) argues that a large number of catastrophic events, such as the Chernobyl nuclear accident and the Space Shuttle Challenger explosion, can be traced to overconfidence. He offers the following summary: "No problem [. . .] in decision-making is more prevalent and more potentially catastrophic than overconfidence". According to Moore and Healy (2008), overconfidence has been used to explain a wide range of observed phenomena, such as high entrepreneurial entry and trading in financial markets, despite available data suggesting high failure rates.

To sum up this section, the available evidence suggests that organizational man is psychologically biased *against* managing HILP risks.

5.3 Over-management of risk

Over-management of risk tends to happen for another category of risks, which I refer to as "high probability-high salience" (HPS) risks. HPS risks are characterized by being comparatively easy to observe by the agent and by appearing imminent and important. HPS-risks also tend to have a relatively unambiguous link to the performance metric used to decide the agent's compensation.

Salient factors are factors that command attention (Plous, 1993). Research in psychology shows that the more salient an event is, the more probable and causal it will appear. A salient risk is therefore a risk for which the exposure appears reasonably clear and imminent to the agent. Risk exposures may gain salience for a number of reasons and trigger our

natural risk aversion. Risk aversion is a fundamental property of human behavior, whose widespread observance suggests evolutionary advantages (Zhang *et al.*, 2014). It is the base assumption of economic behavior, which features prominently in many attempts to understand decision-making under uncertainty (Zhang *et al.*, 2014). When risks become salient, for whatever reason, our tendency toward risk aversion makes us liable to over-manage them.

Most market risk exposures (commodities, exchange rates, and interest rates) fall within the HPS-category. Take the example of currency risk. Once such an exposure gets established, say by initiating exports, the agent will typically have a keen appreciation of the magnitude of the exposure. Currency risk also tends to affect the financial performance of the business unit in a relatively straightforward way, and exchange rates are known to fluctuate significantly. Therefore, it is also "high-probability", the second property of HPS-risks. Another way risk exposures can become salient is through the use of personal scorecards ("key performance indicators"). Moreover, according to Lynch (2008), managers typically overreact to recent failures and accidents: once a negative event has occurred, it receives undue focus and attention (i.e. becomes salient), leading to too many resources being spent on mitigating the risk of a re-occurrence.

To sum up this section, the evidence suggests that organizational man is psychologically biased to over-manage HPS risks.

6. Enterprise risk management as a solution

6.1 Risk governance

Addressing the agency risk management problem can appropriately be labeled "risk governance". Shleifer and Vishny (1997), in their seminal survey of corporate governance, state that their view on corporate governance is a "straightforward agency perspective. We want to know how investors get the managers to give them back their money". Echoing this, my perspective on risk governance is an equally straightforward agency perspective: I want to know how principals, as represented by the Board of Directors, get managers, at all levels of a decentralized organization, to undertake risk management decisions that maximize long run firm value. Risk governance is accordingly defined as a set of mechanisms by which the Board of Directors ensures that managers, at all levels of a decentralized organization, undertake the risk management decision that are in the best interests of the company. Successful risk governance implies that the incentives and behavioral biases of managers do not cause risk management decisions that detract from the goal of long run value creation.

What are the mechanisms that the Board of Directors may consider to achieve good risk governance? The requirement to report risks is a pillar of ERM-programs. Operating units are asked to collect and compile information about their most important risks and pass it on to headquarters. For example, in Equinor ASA (formerly Statoil) units are expected to deliver updated risk information to headquarters on a biannual basis, including discussions and justification of assumptions (Alviniussen and Jankensgård, 2015). This effectively amounts to monitoring the units' diligence in identifying risks. Alternatively, a corporate risk function carries out interviews and workshops to obtain this information as a basis for further conversations about possible risk mitigation actions (Fraser, 2014).

Closely linked to the reporting requirement is the practice of assigning "risk ownership" to the risks that have been identified. ISO 31000 (2009) defines a risk owner as "a person or entity that has been given the authority to manage a particular risk and is accountable for doing so". The intention behind designating risk owners is to increase accountability, so that bad outcomes do not occur simply because no one assumed responsibility for the activity that caused it. Explicit incentives may also come from building expectations about

maintaining risk management processes into the roster of so-called "key performance indicators" to which bonuses are tied.

What are the available mechanisms that deal with behavioral biases that affect risk management? Shefrin (2008) uses the term "debiasing" to describe procedures that address behavioral biases. Specific debiasing techniques to counter overconfidence and overoptimism include keeping good records of the history of a particular activity, developing explicit "failure scenarios" and requiring managers to incorporate past experiences into their current task resolutions. Lynch (2008) suggests training staff in risk management principles to foster a risk-conscious culture. On the whole, training to induce awareness is one of the main methods for countering behavioral biases, as opposed to traditional agency problems where incentives and monitoring are the main mechanisms. Certainly, workshops and similar sessions that aim to increase risk awareness appear to be plentiful. Evidence is scarce, however, that firms systematically institutionalize practices with the purpose of correcting behavioral biases.

6.2 Risk aggregation

Risk aggregation is defined as a set of mechanisms used to ensure that high-quality information about risk is aggregated in a timely, intelligible and relevant format to support centralized decision-making regarding the deployment of economic capital. Successful risk aggregation implies that the Board of Directors has all the relevant information to select an overall risk profile compatible with the goal of long run value maximization.

The most basic and commonplace risk aggregation practice observed is the so-called "risk register". At least judging by its widespread adoption the register must be one of the greatest impacts ERM initiatives have had so far on corporate practice. The risk register is a compilation of the risks that have been identified in the risk reporting process, usually accompanied by estimates of probability and impact to make them comparable. What reaches the directors of the board is usually a condensed list consisting of the organization's top risks or some visualization thereof ("the risk map").

The risk register, while presumably achieving the basic goal of informing the board of the firm's main risks, falls short of expressing what this compilation of risks means for the magnitude of potential gains and losses for the firm as a whole. The arsenal of techniques to deal with inter-related risks on a portfolio basis includes creating scenarios, stress-testing and Monte Carlo simulations of firm performance to derive various aggregate-level risk statistics (Alviniussen and Jankensgård, 2009). For non-financial firms we are confronted with the observation that ERM in practice often appears to "stop" at the level of the risk register. Some non-financial firms are known to have implemented analytical methods involving simulations and the estimation of economic capital (Nocco and Stulz, 2006; Alviniussen and Jankensgård, 2009, 2015) but they appear to be the exceptions to the rule. At the present time, ERM programs are therefore still contributing little or nothing to discussions about the firm's aggregate risk and the suitable level of economic capital.

6.3 Discussion

While accounting for many common risk management practices, the theory also brings emphasis to a set of factors not commonly highlighted in current ERM programs, including the importance of behavioral biases affecting risk management decisions. The theory also places much greater emphasis on the conflicting incentives between players at various levels in the organization than the more harmonious representations of ERM in existing frameworks. Rather than sorting risks into the usual categories of operational, strategic, and market risks, the theory encourages directors of the board to classify risks according to where the problems of over- and under-management of risk may be the most severe.

As noted, another prediction of the theory that finds weak support in actual practice is the idea that ERM should facilitate the task of optimizing the firm's deployment of economic capital. Why is ERM not living up to its potential in this regard? For non-financial firms a major part of the answer to that question is the absence of regulatory pressure. Many regulated banks have developed the internal risk management capabilities necessary to execute this task simply because they have been under pressure to do so. For non-financials, the benefit of meeting the regulators' expectations is lacking in the cost-benefit analysis. Higher-level risk analytics are for the most part neither easy to implement nor understand. According to Alvesson and Spicer (2012), sophisticated thinking and use of advanced knowledge are not core characteristics of the administration of contemporary organizations. Reflecting about potentially disastrous risks and diagnosing behavioral biases are exercises that fit poorly into most organizational structures, and are hence seen as distractions from the effective administration of the company.

The theory's poor fit with data in these cases may of course also be put down to the assumptions about "enlightened" and empowered directors who understand the nature of the organization's risk management problems and are able to direct the firm's limited resources towards addressing it. While there certainly has been important progress made in terms of raising board awareness about the importance of risk oversight, it seems fair to say that directors are still in an early phase when it comes to developing an understanding of formal risk management (Brancato et al, 2006). In addition, the basic premise of the theory – that the Board of Directors is fully incentivized to serve the best interests of shareholders – is shaky. Bebchuk and Fried (2004), in particular, have been vocal in expressing the view that directors are generally more concerned about their own career prospects and remaining on good terms with the CEO than actually promoting shareholder interests. Of course, the Board of Directors is not a homogenous unit. Boards vary greatly in terms of size, educational background, degree of independence, and so on (Adams *et al.*, 2010) all of which are factors that affect the relative power and ability of the Board. There remain rich opportunities for empirically examining how various board arrangements, and corporate governance arrangements more generally, influence on the extent of ERM implementation.

7. Conclusions

This paper provides a theoretical analysis of ERM. Rather than describing ERM in terms of a process aimed at meeting corporate objectives, it proposes to view ERM as a solution, i.e. a set of mechanisms, to address two general risk management problems faced by the firm. These are the agency and information problems of risk management, respectively. The theory is predicated on the observation that there are *internal* agency problems and information asymmetries in firms with decentralized decision-making authority. It therefore complements existing corporate risk management theory, which tends to focus on frictions between the firm and *external* actors. It challenges both the presumption of a harmonious relationship between various actors in the ERM-process, as well as the suggestion that ERM should be viewed primarily as an evolving set of practices that will eventually become codified.

Notes

1. How firms trade off costs and benefits of different risk profiles is covered by existing theories of capital structure and corporate risk management. We consequently do not need ERM to explain the existence of this activity. ERM is instead concerned with overcoming internal agency and information problems related to the risk management process. Hence the boundaries of ERM are demarcated.
2. The micro-benefits include the improved decision-making that comes about when business units factor the effects of firm-wide risk into their capital allocation decisions. Such a risk-based capital

allocation system takes into account the marginal contribution to firm-wide risk when evaluating the units' performance.

3. In this context, it should be mentioned that larger firms may have access to more resources and managerial competence, which may also be factors conducive to ERM implementation. Furthermore, large firms in the financial sector are subject to substantial regulatory pressure to document risk management processes.
4. COSO is a joint initiative by the following five organizations: Institute of Internal Auditors, the Association of Accountants and Finance Professionals in Business, Financial Executives International, American Institute of CPAs and American Accounting Association.
5. Consider a verbal description of a few hundred different risks from various different departments and this point can be appreciated.
6. In this line of reasoning, residual business risk is financed essentially by contingent liquidity. This obtains because liquidity shortfalls are costly and firms are financially constrained. If one uses economic capital (equity depletion), too many risks would be retained because default is typically remote. Such a company would suffer more-than-optimal liquidity shortfalls.
7. The link between value and contingent-liquidity notions of economic capital is that spare borrowing capacity is typically a function of the firm's solvency: the higher the solvency (the excess of asset value over liability value), the better the firm's refinancing opportunities will tend to be.
8. This net present value-rule is the appropriate framework for well-diversified investors who are risk-neutral with respect to idiosyncratic risks.
9. An agency problem typically refers only to diverging interest, not behavioural fallacies. To keep terminology at a minimum, however, I include the latter in the "extended" agency problem rather than introducing a separate "behavioral problem of corporate risk management."
10. Shefrin (2008) has defined a behavioral bias as a predisposition toward making a psychological mistake in a decision situation.
11. A third feature of Black Swans, according to Taleb, is that our capacity for constructing logically coherent narratives make these events seem plausible and predictable *after* they have happened.

References

Alvesson, M. and Spicer, A. (2012), "A stupidity-based theory of organizations", *Journal of Management Studies*, Vol. 49 No. 7, pp. 1194-1220.

Alviniussen, A. and Jankensgård, H. (2009), "Enterprise risk budgeting: bringing risk management into the financial planning process", *Journal of Applied Finance*, Vol. 19 Nos 1/2, pp. 178-192.

Alviniussen, A. and Jankensgård, H. (2015), "Value and risk: enterprise risk management in Statoil", in Fraser, J.R.S., Simkins, B.J. and Narvaez, K. (Eds), *Implementing Enterprise Risk Management: Case Studies and Best Practices*, John Wiley & Sons, Hoboken, NJ.

Aven, E. and Aven, T. (2015), "On the need for rethinking current practice that highlights goal achievement risk in an enterprise context", *Risk Analysis - An International Journal*, Vol. 35 No. 9, pp. 1706-1716.

Basel Committee on Banking Supervision (2013), *Principles for Effective Risk Data Aggregation and Risk Reporting*, Bank for International Settlements, Basel.

Bebchuk, L. and Fried, J. (2004), *Pay without Performance: The Unfulfilled Promise of Executive Compensation*, Harvard University Press, Cambridge.

Bogodistov, Y. and Wohlgemuth, V. (2017), "Enterprise risk management: a capability-based perspective", *The Journal of Risk Finance*, Vol. 18 No. 3, pp. 234-251.

Brancato, C., Tonello, M., Hexter, E. and Newman, K.R. (2006), "The role of US corporate boards in enterprise risk management", *The Conference Board Research Report No. R-1390-06-RR*.

COSO (2004), *Enterprise Risk Management-Integrated Framework: Executive Summary*, COSO, New York, NY.

COSO (2016), "*Enterprise Risk Management-Aligning Risk Management with Strategy and Performance*, June Edition, COSO, New York, NY.

Daud, W.N.W., Haron, H. and Ibrahim, D.N. (2011), "The role of quality board of directors in enterprise risk management (ERM) practices: evidence from binary logistic regression", *International Journal of Business and Management*, Vol. 6 No. 12, pp. 205-211.

European Central Bank (2018), *Report on the Thematic Review on Effective Risk Data Aggregation and Risk Reporting*, European Central Bank, Frankfurt am Main.

Fraser, J.R.S. (2014), "Building enterprise risk management into agency processes and culture", in Stanton, T. and Webster, D.W. (Eds), *Managing Risk and Performance: A Guide for Government Decision Makers*, John Wiley & Sons, Hoboken, NJ.

Fraser, J.R.S., Simkins, B.J. and Narvaez, K. (2015), "Enterprise risk management case studies: an introduction and overview", in Fraser, J.R.S., Simkins, B.J. and Narvaez, K. (Eds), *Implementing Enterprise Risk Management: Case Studies and Best Practices*, John Wiley & Sons, Hoboken, NJ.

Froot, K.A., Scharfstein, D.S. and Stein, J.C. (1993), "Risk management: coordinating corporate investment and financing policies", *Journal of Finance*, Vol. 48 No. 5, pp. 1629-1658.

Gates, S. (2006), "Incorporating strategic risk into enterprise risk management: a survey of current corporate practice", *Journal of Applied Corporate Finance*, Vol. 18 No. 4, pp. 81-90.

Gatzert, N. and Martin, M. (2015), "Determinants and value of enterprise risk management: empirical evidence from the literature", *Risk Management & Insurance Review*, Vol. 18 No. 1, pp. 29-53.

Harris, M. and Raviv, A. (1996), "The capital budgeting process: incentives and information", *Journal of Finance*, Vol. 51 No. 4, pp. 1139-1174.

Hermalin, B.E. and Weisbach, M.S. (2003), "Boards of directors as an endogenously determined institution: a survey of the economic literature", *Economic Policy Review*, April issue, pp. 7-26.

Hoyt, R.E. and Liebenberg, A.P. (2011), "The value of enterprise risk management", *Journal of Risk and Insurance*, Vol. 78 No. 4, pp. 795-822.

ISO 31000 (2009), *ISO Risk Management-Principles and Guidelines*, International Organization for Standardization, Geneva.

Jankensgård, H. (2015), "Does centralisation of FX derivative usage impact firm value?", *European Financial Management*, Vol. 21 No. 2, pp. 309-332.

Jensen, M.C. and Meckling, W.H. (1976), "Theory of the firm: managerial behavior, agency costs, and ownership structure", *Journal of Financial Economics*, Vol. 3 No. 4, pp. 305-360.

Kahneman, D. (2011), *Thinking Fast and Slow*, Farrar, Straus and Giroux, New York, NY.

Kahneman, D. and Tversky, A. (1979), "Intuitive prediction: biases and corrective procedures", *TIMS Studies in Management Science*, Vol. 12, pp. 313-327.

Langer, E. (1975), "The illusion of control", *Journal of Personality and Social Psychology*, Vol. 32 No. 2, pp. 311-328.

Lynch, G. (2008), *At Your Own Risk: How the Risk-conscious Culture Meets the Challenge of Business Change*, John Wiley & Sons, Hoboken, NJ.

Markowitz, H. (1952), "Portfolio selection", *Journal of Finance*, Vol. 7 No. 1, pp. 77-91.

Mikes, A. and Kaplan, R. (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.

Moore, D. and Healy, P. (2008), "The trouble with overconfidence", *Psychological Review*, Vol. 115 No. 2, pp. 502-517.

Nagar, V., Nanda, D. and Wysocki, P. (2003), "Discretionary disclosure and stock-based incentives", *Journal of Accounting and Economics*, Vol. 34 Nos 1/3, pp. 283-309.

Nocco, B.W. and Stulz, R.M. (2006), "Enterprise risk management: theory and practice", *Journal of Applied Corporate Finance*, Vol. 18 No. 4, pp. 8-20.

Plous, S. (1993), *The Psychology of Judgment and Decision Making*, McGraw-Hill, New York, NY.

Power, M. (2009), "The risk management of nothing", *Accounting, Organizations and Society*, Vol. 34 Nos 6/7, pp. 849-855.

Shapiro, A.C. and Titman, S. (1986), "An integrated approach to corporate risk management", in Stern, J.M. and Chew, D.H. (Eds), *The Revolution in Corporate Finance*, Basil Blackwell, Oxford.

Shefrin, H. (2008), *Ending the Management Illusion: How to Drive Business Results Using the Principles of Behavioral Finance*, McGraw-Hill, New York, NY.

Shleifer, A. and Vishny, R.W. (1992), "Liquidation values and debt capacity: a market equilibrium approach", *Journal of Finance*, Vol. 47 No. 4, pp. 1343-1366.

Shleifer, A. and Vishny, R.W. (1997), "A survey of corporate governance", *Journal of Finance*, Vol. 52 No. 2, pp. 737-783.

Smith, C.W. and Stulz, R.M. (1985), "The determinants of firms' hedging policies", *Journal of Financial & Quantitative Analysis*, Vol. 20 No. 4, pp. 391-405.

Speier, C., Valacich, J.S. and Vessey, I. (1999), "The influence of task interruption on individual decision making: an information overload perspective", *Decision Sciences*, Vol. 30 No. 2, pp. 337-360.

Svenson, O. (1981), "Are we all less risky and more skillful than our fellow drivers?", *Acta Psychologica*, Vol. 47 No. 2, pp. 143-148.

Taleb, N.N. (2007), *The Black Swan: The Impact of the Highly Probable*, Random House, New York, NY.

Tufano, P. (1998), "Agency costs of corporate risk management", *Financial Management*, Vol. 27 No. 1, pp. 67-77.

Zahra, S.A. and Pearce, J.A. (1989), "Boards of directors and corporate financial performance: a review and integrative model", *Journal of Management*, Vol. 15 No. 2, pp. 291-334.

Zhang, R., Brennan, T.J. and Lo, A.W. (2014), "The origin of risk aversion", *PNAS Proceedings of the National Academy of Sciences of the United States of America*, Vol. 111 No. 50, pp. 17777-17782.

Further reading

Myers, S.C. (1977), "Determinants of corporate borrowing", *Journal of Financial Economics*, Vol. 5 No. 2, pp. 147-175.

Corresponding author

Håkan Jankensgård can be contacted at: hakan.jankensgard@fek.lu.se