
Managing operational risk: Creating incentives for reporting and disclosing

Received (in revised form): 19th September, 2008

Sebastian Hain

is a PhD student at Goethe University, chair of business mathematics, specialising in accounting and mathematics. He also works with an association of self-employed partners, focusing on transformation consulting in Middle East countries. He has work experience in the field of risk control, trade, organisational development and change management.

Goethe University, Senckenberganlage 31, 60325 Frankfurt, Germany
Tel: +49 177 4014458; E-mail: shain@stud.uni-frankfurt.de

Abstract Operational risk management is acutely related to the management of people. This paper gives a systematic overview of the important incentive conflicts in managing and reporting operational risk to achieve internal as well as external risk transparency. Approaches from outside stakeholders and insurance companies are assessed and taken as inspiration for handling firms' internal obstacles. The paper focuses on firms' risk management, organisational architecture and possible incentive schemes to improve internal reporting. Monetary and non-monetary motivational aspects, sanctions and the level of monitoring linked to the source of risk are discussed. It is shown that these elements have to be balanced in order to let the incentive mechanism work.

Keywords: *decision making, incentive scheme, operational risk management, risk reporting, risk culture*

INTRODUCTION

The discussion regarding operational risk and its sound management has intensified in recent years. This is not solely a consequence of the new Basel II framework, but can be broadly attributed to globalisation and deregulation. Increasing dependence on technology has brought attention to this kind of risk, as the overall risk exposure has increased for firms in most market sectors. In particular, operational risk is seen as a major source of financial loss in the banking sector as of late. The last several decades have seen some spectacular incidents of operational risk

failure leading to major financial losses; the collapse of Barings Bank is a particularly illustrative example. A more recent incident highlighted operational risk concerns, when a rogue trader threw Société Générale, one of the largest banks in Europe, into turmoil. The employee executed a series of elaborate transactions that cost the company at least \$7bn. The current subprime crisis shows that incentive structures of companies often bias the behaviour of their employees towards taking risks without regard to safety regulations.

Due to tougher regulations often

based on the recommendations of the Basel Committee on Banking Supervision (BCBS), the financial industry is leading the development of systematically managed operational risk. In the course of the Basel II project, operational risk has been integrated into the regulatory capital requirements for banks. It is defined by the BCBS as 'the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk'¹. In its paper on 'Sound practices for the management and supervision of operational risk', the BCBS lists risk events that can result in substantial losses.² For instance, this classification includes the risk of (process) mistakes, incompetence, criminal acts, qualitative and quantitative unavailability of employees, failure of technical systems, and dangers resulting from external factors, such as external fraud, violence, physical threats or natural disasters as well as legal risk.

The concepts to manage market and credit risk are quite sophisticated and banks have already gained experience. Furthermore, documentation and data are readily available. In contrast, the study of operational risk has a limited history. The common methodologies to manage market and credit risk cannot be simply transferred because of the low data availability and idiosyncrasies of operational risk. Notably, operational risks are usually not taken in order to gain a particular profit. To change the poor data situation, companies have to adapt their organisational architecture and to enhance the flow of information. As shown by the Basel Committee's second quantitative impact study,³ the

human factor is the main cause of operational failures. Therefore, a sound operational risk management critically depends on the support of employees and their willingness to provide adequate and true information. Due to the fact that such support may have negative consequences for the individual, incentives have to be provided.

This paper gives a systematic overview of the important incentive conflicts in managing and reporting operational risk to achieve internal and external risk transparency. This includes a deeper discussion about the organisational architecture, which all too often remains unattended. Starting with an outside view of the company and the obstacles to accurate and complete communication, the paper follows the firm's hierarchy downwards to identify further difficulties of implementation. Incentives and sanctions used by external parties to motivate adequate management and the reporting of operational risk are assessed and taken as inspiration for firms' internal conflicts. The main part of the paper deals with the role of the communication process in operational risk management (ORM). Considerations dealing with the types of incentives are discussed. Operational risk will be treated separately from other kinds of risks, although it can often hardly be detached in practice. This is done for the purpose of understanding the idiosyncratic character of operational risk and its special treatment. Throughout the paper, banks and their environment serve as the analytical framework to discuss relevant issues.

This paper is organised as follows. The following section discusses an appropriate organisational structure for managing operational risk. The third

section introduces the first incentive conflict dealing with external disclosure of operational risk. Insurance companies and their measures to cope with moral hazard and adverse selection issues are discussed in the fourth section, before moving on to firms' internal risk management. The fifth section focuses on an incentive scheme for the line manager to manage and report the business unit's operational risk. The sixth section covers individual motivation to reveal operational risk and loss events, including the issue of employees having to confess their own misdoings. The final section concludes with a short summary and final thoughts.

ORGANISATIONAL STRUCTURE AND INCENTIVES

This section covers the following:

- a discussion of traditional siloed and centralised risk management approaches;
- an idealised risk management structure;
- an outline of the four main incentive conflicts in managing operational risk.

Recently, there has been a heightened interest in corporate governance and the pros and cons of specific risk management structures. The architecture should be designed in such a way that risk managers can have access to relevant timely information. Additionally, incentives have to be in place to alleviate conflicts at the interfaces between employees or departments. Such information hurdles are present in every organisational risk management constellation, both in communication with outside stakeholders and inside the company.

Controversies over assigning decision rights in ORM deal with the allocation

of responsibilities in the traditional siloed approach and the centralised approach. Typically, these responsibilities include risk identification, measurement, reporting, controlling and monitoring. The traditional decentralised approach dedicates full responsibility and risk management decisions to individual business lines, accompanied by a weak corporate risk management department. In contrast, a centralised risk management approach assigns specific important duties to an established risk management function.⁴ Its role is mainly to set a common definition for operational risk, aggregate and report information, monitor the overall risk exposure of the firm and control the risk capital allocation, if applicable.

On the one hand, decentralisation has the advantage of using knowledge about risk more effectively, by linking local information to decision making. For example, a line manager should be well experienced in dealing with possible problems in the department's processes. Under centralisation, information has to be transferred upward in the hierarchy to the level which owns the ultimate decision right. Hereafter, errors or obscurities can lead to necessary follow-up questions. This process consumes time and may lead to delayed decisions. On the other hand, under a decentralised setting, local risk managers are not necessarily motivated to base decisions on the firm-wide risk level. Interdependencies might be better centrally supervised, particularly if the company employs enterprise risk management. Additionally, by managing the overall risk of a company, a central function has a better overview of the impact of different measures compared with the local view of an

individual manager. This accumulated knowledge can be used to develop enhanced risk response methods and can be transferred through guidelines to address, for example, money laundering or unauthorised trading.

One important argument in favour of the centralised ORM is the problem of data availability. As history has shown, the traditional siloed approach can encourage employees to hide operational risk events. Especially in the banking or aviation industries, recent developments are in favour of a centralised ORM. On account of this, the organisational framework used throughout this paper and described below is closer to the centralised risk management approach. It is derived from propositions of regulatory authorities and the literature as well as real-life examples (eg see BCBS,² BaFin/Deutsche Bundesbank,⁵ Reichelt-Schoelch/Kullmann⁶ and Moosa⁷). The idealised structure serves as a basis for analysing the incentive conflicts.

As shown in Figure 1, a firm can be made up from multiple business units, each with its own manager and multiple employees. The company's risk owners are the manager together with his subordinates who indulge in activities that may lead to operational risk. They represent the interface to the customer, introduce products, implement and execute processes, handle IT systems and machines, and deal with external exposure. The manager is ultimately responsible for the day-to-day operational risk management as well as the implementation of the risk strategy in his purview.

Some of the manager's tasks might be processed by an operational risk manager of the business unit. Reports

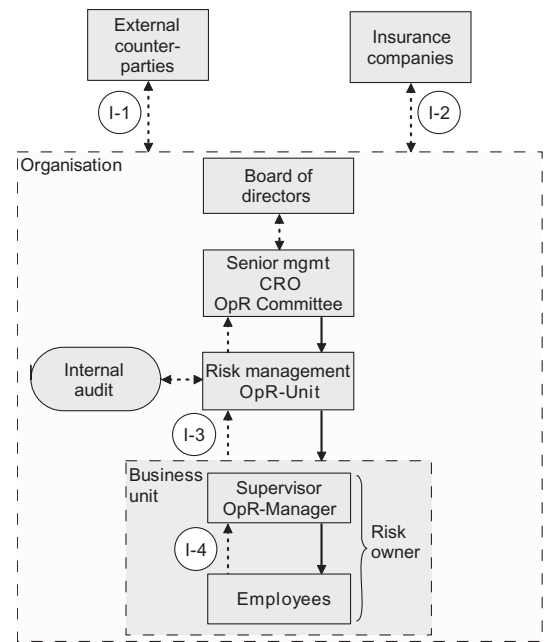


Figure 1: Organisational structure and incentive conflicts

about the operational risk exposure and occurred loss events are forwarded to a centralised operational risk unit, which may represent a subdivision of the main risk management unit. Together with the functional units, such as human resources, IT and finance, it supports the business unit in managing its risk, eg by conducting risk workshops. The internal audit unit supervises the risk management unit and offers support through the contribution of information. Senior management is ultimately responsible for setting the operational risk strategy and for implementing the management framework. Today, many firms appoint a chief risk officer, who is typically a senior manager or one level below with direct access to the CEO. Moreover, banks sometimes establish operational-risk committees to release the executive board. Finally, the board of directors approves and periodically reviews the bank's ORM framework.

Using the symbols I-1 to I-4, Figure 1 additionally indicates the four main areas of incentive conflict with respect to the management and reporting of operational risk within the organisational structure. In terms of reporting to the public, the company has a motivation to report a lower operational risk level and fewer incidents than actually have occurred in order to avoid (negative) reactions, such as increased scrutiny of the risk management processes by regulators. As communicating risk may cause consequences, reporting risk upward states a similar conflict of interest inside the firm.

The next section introduces the first of the four incentive conflicts: the difficulty of sufficient and truthful public disclosure of operational risk.

DISCLOSURE OF OPERATIONAL RISK (I-1)

This section discusses:

- the importance of disclosing risk management information in light of the legal regulations;
- senior management and external disclosure from the perspective of incentive conflict I-1;
- the market approach to resolving incentive conflict I-1.

The motivation of external parties as regards monitoring corporate decisions differs among stakeholders. For example, regulatory authorities focus on social welfare, the capital market requires information for investment decisions, insurance companies try to calculate fair premiums, and rating agencies as well as public accounting firms assess firms as part of their business. Driven by

experience, the disclosure of risk management details has recently become a cornerstone of monitoring by outsiders. If operational risk represents a serious part of the accumulated risk exposure of a firm, external parties should demand to be informed. The basic idea is that higher transparency leads to improved risk management of the firm.

In Germany, the Control and Transparency in Business Act 1998 requires corporations and limited companies to reveal all relevant risks in their annual statements. Likewise in the USA, the Sarbanes-Oxley Act 2002 aims to make corporate decisions and actions more transparent. Section 404 requires reporting on internal control aspects, including an assessment on risk management. As stated above, however, the banking industry is leading developments in risk management as a result of the second Basel Accord.

Basel II is composed of three pillars.¹ The objective of the third pillar is to foster market discipline through comprehensive and detailed disclosure of risk management details. The amount of disclosure should enable counterparties to determine the operational risk level and highlight whether a bank effectively manages it. Publications can be done within the scope of the financial disclosure and other media such as the internet or via direct communication to the regulators. A possible way to communicate senior management's assessment of the risk level could be classification into different intervals. For example, a company could announce and explain in detail whether it is exposed to 'no risk', 'slight risk', 'medium risk', 'high risk' or 'very high risk'.

Supported by some examples of the past, one can assume that senior management has a motivation to minimise the risk level or hide loss events from the public (incentive conflict I-1). A high level of operational risk or a great loss may induce bad publicity or influence competition, which in turn affects senior management's reputation. Another aspect is that the disclosure of the firm's real risk exposure allows market participants to price and deal appropriately. The higher the risk level, the more expensive it is to deal with some external parties, such as in the case of lending capital or insuring risks. This may indirectly affect the bonus payment of the firm's management. One source of the problem is that management decisions are often based on a short-term view on risk issues. Executives' contracts are mostly temporary and there is a possibility that the consequences of operational risk arise never or too late. Thus, some senior managers may not see the necessity of disclosing the risk level honestly, particularly if external parties cannot verify the information.

Possible countermeasures by external parties deter senior management from manipulating information arbitrarily. The lack of monitoring resources and asymmetric information, however, decrease the probability of revealing all major misinformation about operational risk. In their paper on optimal law enforcement, Kaplow and Shavell quote that parties are likely to report events only if they fear more severe treatment compared with remaining silent.⁸ For example, it is normal for firms producing chemicals to voluntarily report environmental and safety violations to an enforcement authority as they are aware of the more negative

consequences should they attempt to hide them. This all comes down to a mechanism that induces those who report a harmful event to pay a certain sanction equal to or less than the sanction should the (unreported) event be revealed by a third party. This leads to a situation where market participants face clear expected treatment in their decision whether to disclose their risk level truthfully.

In fact, the market and its regulators primarily use adverse consequences and monitoring to encourage sound reporting. Possible investigations by regulators can lead to bad publicity or mistrust by market participants. Furthermore, the threat of major loss events, which can hardly be hidden from public awareness, also fosters the discipline. Rating agencies and auditing companies play an important role in this monitoring process. As noted by the BCBS, however, corporate scandals such as WorldCom have generated concern about whether these institutions are always sufficiently independent to do so.⁹

INSURANCE FOR OPERATIONAL RISK (I-2)

This section considers:

- the rationale for insuring operational risk;
- senior management and operational risk insurance from the perspective of incentive conflict I-2;
- the insurance company's approach to resolve incentive conflict I-2.

This section draws special attention to the interaction between organisations and insurance companies. Insurance is an important tool for companies to

mitigate the financial impact of losses due to operational risk. With respect to banks, Moosa points out that insurance has emerged as a valuable risk transfer tool in recent years.⁷ The purchase of insurance provides a measure for companies to substitute possible random fluctuation in the cash flows for a certain periodical premium, eventually raising market value. Basically, insurance is profitable for a company if the marginal benefits are lower than the marginal costs, ie the premium is lower than the capital costs in cases where the risk is internally financed. This is usually the case for low-frequency/high-severity operational risk. Furthermore, a company gains knowledge from the risk management experience of the insurance industry, which it has gathered from access to a multiplicity of clients in various sectors. Today, a wide range of insurance is available, ranging from peril-specific insurance products (eg property insurance, directors and officers insurance, and fidelity bonds) to multiperil products for operational risk.

The incentive conflict I-2 is well known to the insurance industry as moral hazard and adverse selection. Moral hazard arises because the company does not bear the full consequences of its actions. The insurance protects the firm — and therefore its senior management — against the financial consequences of losses due to operational risk, thus reducing the incentive to invest in control activities. For example, a company taking out insurance on internal fraud may have less motivation to implement or enforce precautionary measures, eg taking care of the fidelity of employees or adequate monitoring. A quite common procedure to prevent

moral hazard is that insurance companies monitor the risk management activities of the policyholder both *ex ante* for constraining opportunistic behaviour and ensuring compliance as well as *ex post* for determining whether the company engaged in behaviour that unreasonably increased risk. Another popular approach to overcome moral hazard issues is that the firm retains some risk through certain deductibles and/or upper limits. These measures align the interests of the counterparties to avoid losses. In this vein, insurance may lead to an improved ORM in the firm as the insurer can push the policyholder to adopt sophisticated risk management tools. Measures of the insurer to enforce its requirements include increasing the premium, limiting or cancelling cover, or raising the deductible.

Adverse selection is closely related to I-1. The corporation seeking insurance is motivated to reduce its risk level before signing a contract to minimise the premium or to obtain insurance at all. For instance, a constant premium for computer abuse insurance has the highest appeal for those companies with greater than average IT risk. As insurance companies cannot simply distinguish between the different customer types, the average premium will increase as a rule. The incentive problem is usually reduced by the clever design of contracts. The insurance company offers a menu of policies with different deductibles and prices that motivates self-selection of the prospective policyholder. As a tendency, a firm that is exposed to low risk will demand low insurance and vice versa. Furthermore, the insurer might be able to become well informed either through screening the company or receiving valuable signals from it.

MOTIVATING THE MANAGER FOR SOUND OPERATIONAL RISK MANAGING AND REPORTING (I-3)

This section considers:

- internal reporting of operational risk;
- incentives for the line manager to incorporate risk in his business decisions, risk-adjusted performance measures and associated problems;
- risk reporting by the line manager analysed from the perspective of incentive conflict I-3;
- the firm's approach to resolve incentive conflict I-3 — monetary incentives, sanctions and monitoring;
- the model approach to improve risk reporting.

This section starts to focus on the firm's internal incentive conflicts. Gathering risk information and communicating it inside the institution supports effective risk management, allows for the consideration of risk in business decisions, and is the basis for reporting the firm's operational risk to stakeholders. Various organisational units need different types of information on risk management. For this purpose there are a number of obstacles to overcome. For a number of decades, it was the usual practice to hide loss events and potential problems if possible, leading to serious intransparency. In observing this fact, Levitt and Snyder state that effective information transmission upward through the company is especially unlikely when the news is considered 'bad'.¹⁰ Indeed, this is often the situation when the information is most valuable for risk management, such as in the case of near misses.

The firm's policy towards risk is

defined by the senior management and the board of directors. The line manager can influence the operational risk level partly through his choice of projects and strategy. However, the obligation to deal with operational risk is not just a matter of responsibility: if an identified risk or loss event is important for the company's risk management and the manager is aware of it, he should report it anyway. In general, the frequency and scope of operational risk reports depend on the addressee and the urgency.

Intrinsic and extrinsic incentives should be provided to ensure that the line manager is motivated to care about the risk associated with his decisions. Intrinsic motivation describes the fact that people engage in activities without obvious external incentives — the motivation arises from 'inside'. However, the potential for intrinsic motivation is limited. Additionally, extrinsic incentives have to be provided explicitly for good risk management decisions. Forms of extrinsic incentives include recognition, bonuses, salary revisions and promotions. The counterpart of extrinsic motivation is sanctions such as reprehension, firings or other penalties.

To link the incentives to the employee's performance, a performance measure has to be in place. It should be based on inputs and on outputs. Input-based performance measures for ORM include controlling of the manager's activities and his influence on the risk level. A clear risk management framework, including a description of the risk appetite and guidance on how to weigh potential operational risk against expected profits, is a precondition for efficient management and controlling. As a consequence of asymmetric

information, however, it is often difficult to assess how a staff member deals with operational risk. Therefore, output-based performance measures should also exist in the firm. These measures are linked to the consequences of ORM, for instance, to the risk level or actual loss events. This kind of remuneration leads to the situation where not reporting or considering a risk can influence future performance evaluations.

Profit-sharing through financial ratios is a common way of motivating managers. By means of aligning the interests of the manager and the company on risk issues, this approach is quite similar to the way insurance companies overcome moral hazard issues. In particular, risk-adjusted performance measures (RAPMs) have become increasingly popular.¹¹ These ratios can be used to assess projects, business units or even whole enterprises *ex ante* and *ex post* with a focus on both profitability and risk. Today, an often used measure is the risk-adjusted return on capital (RAROC), which confronts financial performance with the required risk capital. With other things being equal, the higher the risk, the more economic capital is assigned to the division that lowers this performance measure. It can be assumed that a line manager would incorporate the risk of a certain project or strategy in his decisions if the performance measure influences his appraisal.

Unfortunately, new problems emerge whatever performance measure a company introduces to include operational risk in its business decisions. The dilemma is that the evaluated manager can distort the performance measure not only through raising profits or limiting risk, but also through

influencing the risk identification and measurement process in his purview (incentive conflict I-3). Hence, the manager's output is not observable, causing the incentive mechanism to be diluted. Ironically, history shows that cheating on incentive schemes has been rewarded in many cases where unusual risk/return ratios have not been queried.

The supervisor can neglect his duty to report identified operational risk and hope that losses do not occur — at least not until he has left the unit. The time factor is an important enabler for such behaviour: the reporting period for measuring a business line's RAROC is often limited to one year. Taking this into account, the problem for the low-frequency type of operational risk is obvious. The manager taking such a risk has a high probability of never being called to account. The hurdles to report increase by the time the manager fears a negative reputational impact because of carelessness, inappropriate decisions, shirking or fraud. For instance, he might be aware that his managerial style demanded excessive labour by his subordinates, thereby causing serious losses. Assuming a short-term view of the line manager, the bottom line is that the truth-telling is perceived as negatively affecting the performance measure. Consequently, risk-adjusted assessments can lead to distorted incentives and possibly a wrong impression as regards risk exposure. Firms using RAPM to assess the performance of their business units or projects might allocate their capital suboptimally.

To alleviate I-3, additional incentives have to be provided for reporting risk. In addition, these must be supplemented with consequences for not exposing or

warning. For this reason, the risk identification and measuring process of the business unit as well as risk management decisions of the line manager need to be monitored. By analysing internal and external data, the firm gains knowledge about the features of its operational risk. Especially for the high-frequency type of risk (eg routine processing errors in a high-volume business), there should be conceptions about the risk capital of particular business units. Possible measures for increasing the monitoring level might be, for instance, the obligation that critical risk management decisions are double-checked by another person. Through internal audit, it is possible to ensure the validity of the business units' own risk assessments. Similarly, the risk management unit can work with individual business units in risk workshops and other risk identification processes, and check the business unit's reports against their own assessments. Some enterprises can also consider the reports of external auditors. However, perfect monitoring is not desirable due to feasibility considerations and high costs. Furthermore, it reduces the trust in co-workers and can lead to an unproductive work environment with low mutual support. By contrast, with no controls, the company could just hope that the reports are true as a result of the manager's intrinsic motivation or other circumstances. Hence, the monitoring level has to be balanced. The level depends on the choice of incentives and the type of risk.

Economic theory suggests that individuals make decisions based on subjective expectations of marginal costs and benefits as they perceive and value them. Following the earlier argument

regarding I-1, the incentive mechanism must be designed as follows: the expected utility of reporting the operational risk has to be higher than the expected utility of concealment. Employing incentives and sanctions, the mechanism has to be carefully and thoroughly designed to induce sound risk management and reporting. Incentives refer to rewarding proper risk management and true reporting. In contrast, punitive measures punish divergence from a firm's risk policy. The basic mechanism of such an incentive-oriented procedure will be illustrated in the following simple economic model.

A MODEL FOR IMPROVING RISK REPORTING

In this section, it is assumed that the manager has comprehensive and accurate knowledge about the risk exposure of the business unit. As such, there is no incentive conflict between the supervisor and his staff. The level of operational risk is given, so the line manager has already decided on strategy and projects. He himself is not a source of operational risk with respect to deliberate actions. In the model, the line manager has to decide rationally which level of operational risk is reported to the central risk management function, eg the risk of losing business-relevant data or the failure of productive systems. The business unit is rated by the RAROC performance measure, which is also part of the manager's variable compensation scheme. A higher risk level leads to lowering the RAROC, which reduces the manager's remuneration and vice versa.

For analysing an accurate incentive mechanism one starts with utility

considerations. As stated above, the utility for the manager of truthfully reporting the operational risk level $U(R)$ has to be higher than a wrongly reported exposure $U(NR)$. In other words:

$$U(NR) \leq U(R) \quad (\text{A.1})$$

It is assumed that the manager's utility is on a par with his year-end bonus. Thus, one can focus on monetary incentives and disregard possible influences due to intangible aspects. In simple terms, the RAROC formula can be written as follows:

$$R = \text{RAROC} = \frac{\text{Risk-adjusted net revenue}}{\text{Risk capital}} \quad (\text{A.2})$$

The line manager has the option to accurately report the risk level, which yields the RAROC R_R , or to distort the provided information. In the latter case, one assumes that he tends to reduce the risk level or cover up loss events, which leads to a lower risk capital and eventually to a higher RAROC. With a probability of P_D , the true risk level is discovered and the business unit's RAROC is manually changed to R_D . Consequently, the probability of not detecting a manager's wrong report leading to R_{NR} is $(1 - P_D)$. To sum up, the incentive mechanism can be written as follows:

$$R_{NR} \cdot (1 - P_D) + R_D \cdot P_D \leq R_R \quad (\text{A.3})$$

Note that if assuming $R_{NR} \geq R_R$ (otherwise, there would be no incentive conflict), the incentive mechanism only works when $R_{NR} \geq R_R \geq R_D$.

The company can use R_D as a penalty measure and decide on the level of P_D .

R_{NR} is only known by the line manager and cannot be directly influenced by risk management. Normally R_R is given through the choice of projects and strategy. However, the firm can employ R_R strategically to motivate for accurate reports and support an open-risk culture. For example, voluntary disclosure can be rewarded by considering a lower risk capital to calculate manager compensation than the risk capital that is actually taken for calculating the economic capital. In this regard, it is very important to note that the manager's expectations about the variables decide on the functionality of the incentive scheme. For instance, it is not important to actually increase the level of P_D but to let the manager think so. However, real circumstances should normally meet the manager's expectations not to provoke distrust. Similarly, the manager possibly calculates with a different P_D compared with the firm because of the previously mentioned short-term view.

Taking a deeper look at the formula A.3 yields the following: the higher R_R and therefore the closer to R_{NR} , the higher the encouragement to report truthfully in the first place. Consider an example where the firm uses R_R strategically. Assume that the probability of discovering misinformation is $P_D = 20$ per cent. Due to a lack of resources and cultural aspects, a higher level of monitoring is not feasible. The risk management function receives a report about the risk level of a business unit, which yields $R_{NR} = 15$ per cent, but the risk managers feel it should be lower at around 10 per cent. Figure 2 illustrates the mechanism which would induce a true report.

The figure shows that only $R_D \leq -10$

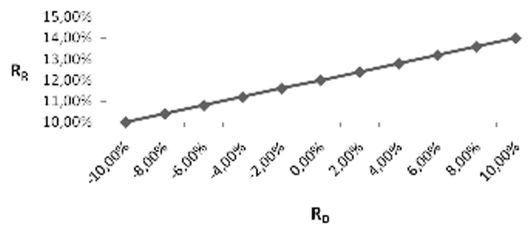


Figure 2: Incentive mechanism with R_R subject to R_D

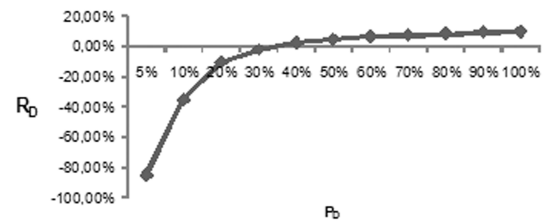


Figure 3: Incentive mechanism with R_D subject to P_D

per cent guarantees a report of $R_R = 10$ per cent. If it is not possible for the firm to punish through a negative RAROC, the role of R_R becomes obvious: the firm should add a bonus to the real RAROC to receive true reports. In this example, when R_D is fixed to 0 per cent, the company should guarantee that $R_R \geq 12$ per cent, even if the true RAROC turns out to be 10 per cent.

The following assumes that the firm wants to calculate and use the risk capital correctly and is not willing to change R_R artificially. If the difference between R_{NR} and R_R is high, because the manager considers suppressing serious risks, P_D has to be sufficiently high and R_D sufficiently low to let the mechanism work. The interaction between P_D and R_D can be illustrated by rearranging the formula A.3:

$$\frac{R_R - R_{NR}(1 - P_D)}{P_D} \geq R_D \quad (\text{A.4})$$

As $0 \leq R_{NR} \leq 1$, a lower P_D leads to an increase of R_D . This means that a low monitoring level (or high information asymmetries) has to be compensated with a higher punishment (lower R_D) in the event that the information submitted is identified as incorrect. R_D also decreases in the spread between the R_R and R_{NR} . Figure 3 illustrates the incentive mechanism for constant $R_{NR} = 15$ per cent and $R_R = 10$ per cent (more general $R_{NR} = \frac{3}{2} \cdot R_R$). It shows

that R_D has to be negative when the monitoring level is low. If a negative RAROC is not possible, the disclosure rate has to exceed one-third.

The incentive mechanism illustrates the possibilities of the risk management function to influence the manager's decision whether to reveal operational risk information. However, the mechanism would have to be embedded in an overall compensation scheme that incorporates other kinds of risks and other aspects of a manager's duties. The analysis of the multitask principal-agent model suggests that incentive pay serves also to direct the allocation of the manager's attention among his various tasks.¹² Aspects which are not incorporated in the compensation contract or are hardly measurable run the risk of being neglected. In addition, the compensation scheme should cope with the problem of a short-term view on risk issues. Techniques derived from the idea behind bonus banks can help to solve the problem. Compensation linked to the operational risk of a certain fiscal year should be paid out in a delayed manner as risk materialises over time.

A particular problem remains for low-frequency/high-severity operational risk, which may even endanger the survival of the enterprise. Major loss events occur extremely rarely, but may happen to many firms over time. If P_D is low, the motivation to report such a

risk is weak and the incentive mechanism may not work. This is why the framework conditions for managing and reporting operational risk have to be supportive for an open-risk culture. For example, if a manager anticipates compensational disadvantages for reporting a low-frequency/high-severity operational risk in a project, then at least he should not fear a serious loss of reputation. Aspects related to this kind of motivation are analysed in the next section.

MOTIVATING THE EMPLOYEE FOR REPORTING OPERATIONAL RISK (I-4)

This section considers:

- risk identification by employees from the perspective of incentive conflict I-4;
- risk culture and influences on risk information flow;
- the employee's personal decision process to reveal a risk;
- the firm's approach to resolve incentive conflict I-4 — non-monetary incentives, sanctions and monitoring.

This section is concerned with the source of operational risk, the employee, and non-monetary incentives to reveal identified risk. It is assumed that the line manager seeks to be accurately informed about the risk level in the business unit. In doing so, he strongly relies on his subordinates, which can cause the incentive conflict I-4. One important aspect of sound ORM is that the line manager motivates the employees to report risk and loss events to him or directly to the risk management function. The requirement to report has to be independent from the question of responsibility. To perform the risk

identification process more systematically, best practice instruments have recently emerged in the banking sector: self-assessments, loss databases, scenario analyses and key risk indicators can be used to discover operational risk in business units, processes or projects. In particular, tools such as self-assessment in the form of risk workshops, scenario analyses or input for the loss database, rely on the support of employees. Subordinates who deal with the company's business processes every day are often in the best positions to recognise problems as they arise. For example, purchasing personnel may be offered improper and illegal incentives from a supplier to receive a tender. Stopping business connections at an early stage could reduce potential harm to the company. However, exposing the risk might have negative consequences for the whistleblower.

Detrimental to proper risk information flow is an environment where the suppression of bad news is encouraged more than open dialogue. Strictly following orders without questioning and always being a team player can be of advantage for some aspects of corporate business but may hinder an open dialogue on risk issues. Indeed, employees might even cause an operational risk when the firm's incentive system indirectly motivates them to do so. For instance, dishonest or unethical acts can be provoked through undue emphasis on increasing sales or profits in the short term at any cost. A key issue for overcoming these obstacles is the frequently cited, but rarely analysed operational risk culture. This often turns out to be a weak point of companies. This culture encompasses the ways risk management and

responsibilities are organised, the ways people receive incentives for proper management, how the people are monitored, the attitude towards and perception of risk, as well as how people respond to identified risk. These aspects can be referred to as 'soft elements' of the organisation, in contrast to 'hard elements' such as the previously discussed incentive scheme. If used properly, these soft elements can support the communicating of the firm's risk management framework to employees. Moreover, it can help to form employees' expectations of how their co-workers, managers or other members of the firm will respond to their manner of handling operational risk. Clear rules and statements are a valuable guideline on how to react in certain situations, as not every aspect of operational risk and possible countermeasures can be defined beforehand.

If it is not possible or desired to pay people for the general risk management performance of their business unit, intangible incentives and subjective performance measurement have to be taken into consideration. It should be clear that the best motivational factor for an employee to follow a firm's policy is satisfaction with the job, colleagues, supervisors and other aspects of the firm's environment. Nevertheless, particular incentives are a proper way to induce sound risk management and reporting. As shown in the previous section, the perceived net cost of reporting is important for an individual's judgment regarding whether to communicate an operational risk or loss event. Generally, two different situations should be distinguished that influence the decision process of an employee: on the one hand, the operational risk or a

loss event is identified by the employee, but he is not responsible (case 1). On the other hand, the employee himself may have been partly or fully responsible for an error (case 2). The hurdles to report intensify with an employee's degree of responsibility for the operational risk in question.

Starting with case 1, the person gains no monetary advantage by not reporting (it does not change his remuneration). However, he will consider the disutility of revealing the risk. Among other things, the disutility can manifest as time-consuming questions, follow-up processes or being labelled as defeatist by colleagues and supervisors. An aggravating factor emerges when a colleague's action leads to the risk and there is a kind of solidarity in the team — sometimes referred to as 'groupthink' or 'herding'. Reporting tends to be more unlikely the more benefits everyone receives through cooperation in the team. Furthermore, if the supervisor's action led to the event, career concerns can also influence the reporting decision. As an example, a staff member recognises that the company's data security procedures are not adequately explained to new employees. If he reports this circumstance to the risk management function, his colleagues may blame him for increasing the amount of work for the business line. To change this culture, people have to understand the necessity of ORM. Such support can be fostered through training and seminars, in which risk managers can additionally create an understanding for problem areas and the risk management approach. Moreover, simply giving feedback to the employee who reported an operational risk is powerfully motivating. A good

reporting mentality should be rewarded through intangible incentives such as praise and official announcements. The performance in risk assessments and scenario exercises can be part of the agreement of objectives between supervisors and subordinates, and eventually considered in career path development. To simplify the reporting process, clear roles and user-friendly reporting systems are important. The expenditure of time for reporting has to be kept to a minimum. The employee has to be offered security and trust so that he does not have to fear being laid off. In addition, there should be the option to report a risk or loss event anonymously. This significantly lowers the barriers to revealing important information. In contrast, there must be consequences if a person knew about a risk which materialised as a result of not reporting an event, perhaps because he did not want to blame a colleague. As argued in the previous section, monitoring is necessary to let the incentive mechanism work.

The incentive conflict is different in case 2, because an employee can hardly be positively rewarded for reporting his own mistake. For example, providing monetary incentives for confessing personal wrongdoings could even lead people to take unnecessary risk. Compared with case 1, it is generally harder to reveal the information. Clear rules depending on the degree of deliberateness of the event are necessary to provide security to personnel. A classification of unintended errors (eg slips, lapses or mistakes), negligent actions and deliberate errors seems reasonable. In practice, there should be smooth transitions between these partitions. The basic incentive

mechanism focusing on the outcome for the employee is illustrated in Figure 4.

As shown in the figure, self-incrimination should always be rewarded in preference to the risk or loss event being revealed through a third party. This conclusion coincides with the findings of analysing I-3. The disutility can be interpreted as a consequence of the operational risk or loss being revealed, such as embarrassment, annoying questions, reprimand by a supervisor, a warning letter, or dismissal. In the event of an unintended error that did not result in serious negative consequences, the company should consider waiving the disciplinary actions against the voluntarily reporting person. Therefore, a line between unacceptable behaviour (closer to deliberate errors) and blameless acts (closer to unintended errors) has to be drawn. Incidents in the grey area between must be decided upon case by case. This is common practice within the aviation industry. To reduce accidents by learning from incidents, pilots are thus motivated to report any mistakes they may have made during a flight. Introducing this kind of firm policy will particularly increase the

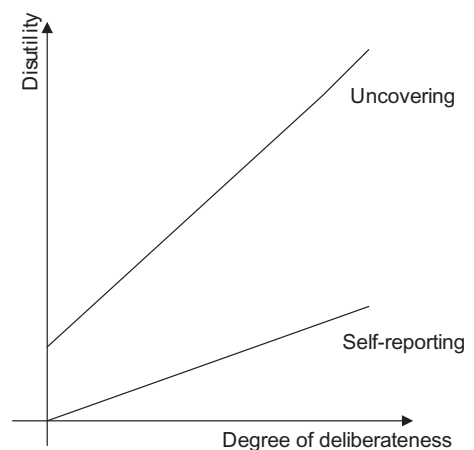


Figure 4: Utility considerations

reporting of high-frequency/low-severity events. Some of the information can be used as warning indicators and signals to learn more about the firm's operational risk, especially the low-frequency/high-severity type. The consequences of uncovering mistakes through a third party should increase disproportionately to the degree of deliberateness, in order to give people additional incentives to think before acting. As many operational risks such as attempts to defraud are originated or at least known by more than one person, whistleblowing policies offer an effective way to encourage the reporting of deliberate actions.

CONCLUSION

It was shown that the balance of positive incentives and sanctions accompanied by an adequate level of monitoring is very important for the reporting of operational risk. Incentives can be employed as substitutes to reduce disciplinary actions and control. In the personal decision process, truth-telling has to yield an advantage to let the incentive mechanism work. The widespread short-term view on risk issues of employees has to be taken into consideration. If misbehaviour has caused the operational risk or loss event, then special treatment is necessary to motivate voluntary reporting. Especially for unintended errors, the consequences for the confessing employee should be very low. Human error will never be fully eliminated, thus organisations should deal with it appropriately. However, changing the risk culture needs time as well as strong support and commitment from upper management.

The analysed incentive mechanism can only work properly if the

methodologies for measuring operational risk are quite sophisticated. Moreover, as a particular operational risk can affect different units of a company at one time, it is often a challenge to assign it fairly. The development of techniques should improve over time in order to foster employees' acceptance. During this period, the firm should introduce its operational risk management and employ objective and subjective performance measures linked to its risk management framework. The performance standards should be improved from year to year. As shown in this paper, incentive conflicts have to be solved at the interfaces to improve the poor data availability of operational risk. A better data basis enables researchers and practitioners to measure risk and identify the causes and consequences. The bottom line is that a better risk transparency develops a firm's risk culture and leads to improved operational risk management. This improvement supports the management of market and credit risk.

ACKNOWLEDGMENT

The author thanks Professor Dr Heinrich Rommelfanger and participants of the semi-annual doctoral colloquium for valuable discussions and comments.

References

- 1 BCBS (2006) 'International convergence of capital measurement and capital standards', available at: <http://www.bis.org/publ/bcbs107.pdf?noframes=1> (accessed 12th July, 2008).
- 2 BCBS (2003) 'Sound practices for the management and supervision of operational risk', available at: <http://www.bis.org/publ/bcbs96.pdf?noframes=1> (accessed 12th July, 2008).

- 3 BCBS (2002) 'The quantitative impact study for operational risk: overview of individual loss data and lessons learned', available at: <http://www.bis.org/bcbs/qis/qisopriskresponse.pdf> (accessed 12th July, 2008).
- 4 Brickley, J., Smith, C. W. and Zimmerman, J. (2007) 'Managerial Economics and Organizational Architecture', McGraw-Hill/Irwin, New York.
- 5 BaFin/Deutsche Bundesbank (2005) 'Bericht über die Industrieaktion AMA operationelles Risiko 2005', available at: <http://www.bundesbank.de/download/bankenaufsicht/pdf/ama/abschlussbericht.pdf> (accessed 12th July, 2008).
- 6 Reichelt-Schoelch, I. and Kullmann, A. (2006) 'Implementierung eines Operational Risk Managements', *Risiko Manager*, Vol. 18, pp. 10–13.
- 7 Moosa, I. A. (2007) 'Operational Risk Management', Palgrave Macmillan, New York.
- 8 Kaplow, L. and Shavell, S. (1994) 'Optimal law enforcement with self-reporting of behavior', *The Journal of Political Economy*, Vol. 102, No. 3, pp. 27–51.
- 9 BCBS (2002) 'Supervisory guidance on dealing with weak banks', available at: <http://www.bis.org/publ/bcbs88.pdf?noframes=1> (accessed 12th July, 2008).
- 10 Levitt, S. and Snyder, C. (1997) 'Is no news bad news? Information transmission and the role of early warning in the principal-agent model', *RAND Journal of Economics*, Vol. 28, No. 4, pp. 641–661.
- 11 Hull, J. C. (2007) 'Risk Management and Financial Institutions', Pearson Prentice Hall, Upper Saddle River, NJ.
- 12 Holmstrom, B. and Milgrom, P. (1991) 'Multitasking principal-agent analyses: Incentive contracts, asset ownership, and job design', *Journal of Law, Economics, and Organization*, Vol. 7, special issue, pp. 24–52.

Copyright of *Journal of Risk Management in Financial Institutions* is the property of Henry Stewart Publications LLP and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.