Risk management – a strategic advisor for a sound management of a leasing business[1]

ELENA ANDREI DRAGOMIR – ION DOBRE

Organizations face a very wide range of risks that can impact the outcome of their operations. The constantly increasing risk in nowadays global financial markets emphasizes the importance of correctly estimating future losses, therefore, the management of the leasing company needs to find a good trade-off between business risk, performance risk and financial risk and to have a good strategy to maintain and/or improve the profitability. Although leasing may not be the subject to Basel II. Capital Accord regulatory requirements, in many respects it represents best practices, reflecting a combination of the views of sophisticated lenders represented on the Committee as well as those of the major regulators. Consequently, lenders in the leasing industry frequently look to Basel for benchmarking and insights. This paper aims to illustrate the importance of risk management holistic approach in assessing the risks of a leasing company and we intend to expound that the implementation of an effective risk management process is a key requirement for a modern leasing company that has as priority the need to align profitability, risk profile and asset quality. Also, we will draw attention to the regulatory environment and recent regulatory and supervisory developments with respect to risk management practice.

Keywords: enterprise risk management, framework, risk assessment, quantification, probability, impact

1. Introduction

A recent trend in corporate governance has been the development of an integrated, enterprise-wide approach to assessing the business risks that can impact an organization's ability to achieve its business objectives and to develop programs for managing those risks (*Miccolis* et al 2001). Risk can be defined as the likelihood that the outcome from a process will not meet expectations (*Knechel* 2002). Business risks represent threats to the ability of an enterprise to execute business processes effectively and to create customer value in accordance with strategic objectives (*Bell* et al 1997).

Enterprise Risk Management (ERM) is the most recent development in the evolution of risk management. Like all modern ideas, it builds upon a foundation that started in the industrial age and moved into the knowledge age. We aim to review the risk management concepts and events that contributed to our ability to scan the horizon, identify risks broadly, and use technology to share exposures with risk owners (*Hampton* 2009).

ERM is clearly a relatively new area of academic research, since the first academic study on ERM was published in 1999, although James Lam created the term "enterprise risk management" in the mid-1990s. Academic research to date on ERM includes studies that focus on various determinants of ERM and, more recently, research has investigated the potential value associated with ERM adoption.

Early empirical work on ERM investigated why companies adopted ERM and most studies utilized survey data. The first study by *Colquitt* et al (1999) investigated the characteristics and extent of integrated risk management by surveying 397 risk managers.

[1] This article is a result of the project POSDRU/88/1.5./S/55287 „Doctoral Programme in Economics at European Knowledge Standards (DOESEC)". This project is co-funded by the European Social Fund through The Sectorial Operational Programme for Human Resources Development 2007-2013, coordinated by The Bucharest Academy of Economic Studies in partnership with West University of Timisoara.

They found that political risk, exchange rate risk, and interest rate risk were the three most common non-operational risks handled by the risk management department. Another study *Kleffner* et al (2003b) surveyed Canadian Risk and Insurance Management Society members about ERM adoption. They found that 31 percent had adopted ERM and that the primary reasons for adoption were risk manager influence, board encouragement, and stock exchange guidelines.

Other early work on ERM included a focus on the determinants of ERM. One of the first papers in this area, *Liebenberg* and *Hoyt* (2003), compared firms that appointed a chief risk officer to a matched sample. They found that firms that appoint a chief risk officer are more likely to be financially leveraged. They concluded that further research is necessary to understand ERM determinants. A related but more recent investigation was done by *Pagach* and *Warr* (2007) where they studied the announcements of senior risk officer appointments and found that such appointments are positively associated with size, leverage, volatility, and the number of business segments.

Another paper related to ERM determinants was done by *Beasley* et al (2005a) where they surveyed internal auditors and their views on factors associated with ERM implementation. They found that ERM implementation is positively associated with board independence, requests from the CEO or CFO to have internal audit involved, the presence of a CRO, the company's auditor being a Big Four audit firm, size, and industry group (banking, education, and insurance). It is interesting to note that they also found U.S.-based companies are not as advanced in ERM implementation. By the time of this study and the following study (*Beasley* et al 2005b), there had been a rising interest in ERM and added interest in ERM by many internal auditors. The data used in both of these studies was funded by the IIA Research Foundation to examine internal auditing's involvement in ERM.

2. Modern risk management perspective

As shown in the introductory chapter, despite the growing interest of practitioners in enterprise risk management (ERM) and numerous surveys by providers of ERM "solutions" (such as governance, risk, and compliance software), we may state that not enough academic research has been conducted to provide a better understanding of ERM. As an example, researchers study topics such as what ERM is (or is not), practical measurement of the degree to which ERM is implemented within different industries, factors determining ERM's implementation (or lack thereof), the effect of ERM implementation on business market values, and the interaction of ERM with overall business objectives.

Many companies have completed surveys of the risks they face, and have adopted systems to control some of the risks they have found. The breadth of this analysis has varied from one company to another, depending on local factors of which we would mention the assessment by the management team and board members of the benefits that may be obtained from the risk-management approach. However, many regulators, stock exchanges, and professional bodies have encouraged companies to improve the quality of their risk measurement, and have issued guidance, so there is considerable institutional conformance pressure (e.g., *COSO* 2004, *Australia Standards* 2004).

Some insights can be gained from the COSO definition of enterprise risk management, which reads as:

> *Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives (COSO 2004).*

Most risks have limited impact. For example, they may be limited by the value of the asset whose loss they represent; others can have a large impact, but with a correspondingly small probability. The extreme value parts of such risks tend to be risk-management blind spots and are often ignored because they might occur, say, once in 200 years or less. However, most companies will have a number of such risks, so that in aggregate they can be important, as many cases demonstrate. The problem in analyzing such risks revolves around the lack of data because there may have been no occurrences of the risk in living memory. However, a body of theoretical work has been done to analyze these situations statistically. This work was pioneered by Emil Gumbel, who in the 1950s showed that you can construct a statistical distribution (the Gumbel distribution) to represent the extreme-value "tail" of many risks (*Gumbel* 1935, 1958). This was later generalized to include more risks by the introduction of the Generalized Extreme Value (GEV) distribution. This surprising result that all tails have similar shapes, and the intrinsic importance of the topic, has resulted in a body of research that is too mathematical to be covered here. A good introductory text in this area, giving many examples, is *Reiss* and *Thomas* (2001). Other references are *Embrechts* et al (1997) and *Coles* (2001).

Traditional risk management has changed into a new concept with a broader role. Modern risk management covers four areas:

1. *Hazard risk management*. Risk managers follow a five-step process to assess hazard risks. First, they seek to identify exposures. Then they assess the frequency and severity of the exposures. Step three is to identify alternatives. Step four is to choose an option and implement it. The final step is to monitor the implementation and make adjustments as needed. This process sets up both preventive and crisis risk management.
2. *Internal control*. Companies have processes, called internal controls, to provide reasonable assurance that policies are being followed. Internal control processes seek to improve effectiveness and efficiency, increase the reliability of financial reporting, and ensure conformity with laws and regulations. Elaborate systems of internal control are common in organizations, particularly in industries that are highly regulated by government agencies.
3. *Internal audit*. Internal auditors pursue assurance that internal controls are working. This is not risk management. Rather, it focuses on the cost, efficiency, and effectiveness of processes, including risk management. From a risk management perspective, internal audit focuses specifically on whether a risk is actually being avoided, reduced, or transferred. The internal audit team examines operating activities, the consistency of procedures, and compliance with directives. Then the internal auditor prepares a report for management that identifies weaknesses and failures to follow policies.
4. *Regulatory compliance*. This refers to efforts to ensure conformity with official requirements imposed by statutes, public agencies, or the courts. Examples are rules governing plant safety, the environment, reliable financial reporting, and compliance with social and economic mandates. Many organizations have a single compliance unit or officer who interprets directives, laws, and regulations, offers education and training, and recommends processes to conform to regulations (*Hampton* 2009).

3. Conceptual taxonomy of erm types

This section conceptualises ERM as an assembly of practices, which can be grouped in four ideal types with reference to their institutional origins, techniques and ambitions. Normative and technical texts are suggestive of four ideal types of risk management, all of which qualify as enterprise-wide, but vary in terms of their focus and purpose.

3.1. Type I. Risk silo management

Over the past decade there have been significant advances in the risk measurement capabilities of financial institutions (*Garside–Nakada* 1999, *Marrison* 2002). At the heart of the practitioner literature's most salient risk management ideal type is risk quantification, the rendering of an increasing number of risk types susceptible to quantification, measurement and control. The following commonly quoted definitions apply for the main risk categories (*Drzik* et al 2004).

Market risk arises from changes in the value of financial assets and liabilities due to volatility in market prices (interest rates, currencies, equities, commodities).

Credit risk arises from changes in the value of assets and off-balance sheet exposures due to volatility in default rates or credit qualities.

Banc-assurance firms and insurers add the additional category of insurance risk, which arises from volatility of insurance claims around the expected level of claims.

Operational risk has long been defined as a residual category, one that captures all of the risks not covered in the first three categories.

3.2. Type II. Integrated risk management

Risk aggregation has been a challenge to risk practitioners for a long time. This was largely due to the variety of risk measures applied to the different risk silos, and the correlations that exist between risks. The recent development of a common denominator measure for market, credit and operational risks enables firms to aggregate their quantifiable risks into a total risk estimate. The emerging common denominator of quantifiable risks is called *economic capital*. Economic capital (also known as *economic risk capital*) is a statistically estimated amount of capital that could be used to cover all liabilities in a severe loss event (given a specific confidence level), such as an unexpected market, credit, operational and/or insurance loss. The conceptual appeal of economic capital methods, as recognised recently by the regulator, is that „they can provide a single metric along which all types of risks can be measured" (*BIS* 2003).

Economic capital, as the common denominator for the measurable risk types, creates a consistent and comprehensive framework, or at least the appearance of it, in which risks can be compared and aggregated, enterprise-wide. Further, economic capital can be set to constrain the risk capacity of business initiatives and profit centres, serving as a tool for limit setting and control.

The economic capital framework gives rise to a new risk management ideal type, *integrated risk management*. It is defined here as a risk management approach that applies the economic capital framework for the measurement, comparison, aggregation and control of risks.

Although leasing may not be the subject to Basel Capital Accord regulatory requirements, in many respects it represents best practices, reflecting a combination of the views of sophisticated lenders represented on the Committee as well as those of the major regulators. Consequently, lenders in the leasing industry frequently look to Basel for benchmarking and insights.

3.3. Type III. Risk-based management

Relatively recent works in the risk management literature support the idea of using risk-based internal capital allocations for performance measurement and control. The possibility of introducing risk-based *performance measurement* in banks and leasing companies has emerged as a result of developments in risk quantification and risk aggregation. It also

appears to coincide with the rise of the shareholder value concept in corporate writing (*Arnold–Davies* 2000).

The type of risk management that is able to feed these ambitions has gone well beyond the original sphere of risk silo management or even that of integrated risk management. It is put forward as the third risk management ideal type, *risk-based management*, its characteristic aspect being a strong shareholder value rhetoric.

3.4. Type IV. Holistic risk management

We have seen how the ascent of the shareholder value concept gave rise to a specific ideal type of risk management, risk-based management. This section focuses on the impact of another powerful notion, proclaimed by corporate governance advocates, that of risk-based internal control. The Treadway Commission (*COSO* 2004) advocates ERM as a framework for capturing risks that are material from the point of view of the achievement of the strategic objectives of the enterprise. Apart from the measurable risk silos, this conception of ERM encompasses risks that cannot be readily quantified or aggregated. These non-quantifiable risks include, for example, the risks of strategic failure, environmental risks, reputational risks and operational risks that materialise only rarely. Recent developments in corporate governance have emphasised the importance of monitoring and managing these risks.

4. ERM framework and risk universe

4.1. ERM framework

The importance of risk management is recognized by the publication in 2009 of an International Standards guide, ISO 31000 Risk Management - Principles and Guidelines, developed by a work group of international experts from more than 30 countries.

The ISO framework is current best practice for risk management frameworks. It incorporates best practice from COSO, PMI (Project Management Institute), the Australian and New Zealand Standard (AS/NZS 4360:2004) and other leading international risk management standards.

ERM framework has seven components:

1. Mandate and commitment to the ERM framework.
   a) Agreement in principle to proceed with ERM.
   b) Gap analysis.
   c) Context for framework.
   d) Design of framework.
   e) Implementation plan.
2. Risk management policy
   a) Policies for the ERM framework, its processes and procedures.
   b) Policies for risk management decisions:
      – Risk appetite.
      – Risk criteria.
      – Internal risk reporting.
3. Integration of ERM in the organization.
4. Risk Management Process (RMP).
   a) Context.
   b) Risk assessment (identification, analysis, and evaluation).
   c) Risk treatment.
   d) Monitoring, review, and actions.

e) Communications and consultation.

5. Communications and reporting.
6. Accountability.
   a) Risk ownership and risk register.
   b) Managers' performance evaluation.
7. Monitoring, review, and continuous improvement.
   a) Responsibility for maintaining and improving ERM framework.
   b) Approach to risk maturity and continuous improvement of ERM framework.

Figure 1 illustrates a typical framework for an organization to implemented ERM according to ISO 31000. It shows in addition to the main components of an ERM framework, other processes and functions necessary for implementation and continuous improvement. It is expected that each organization will customize the ISO framework to suit their organization's structure, roles, and responsibilities, with a view to making integration of risk management easier and more effective.

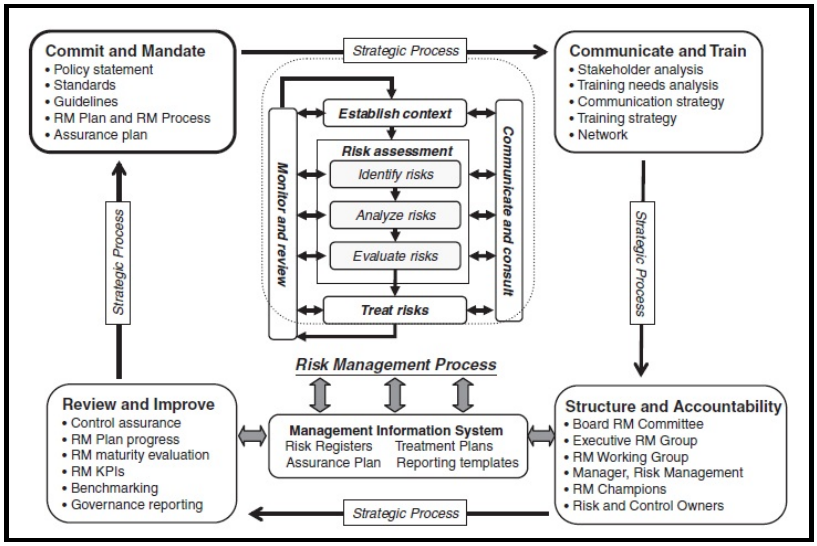
Figure 1 illustrates the traditional set of risk management tasks to support and assist decision making by any manager anywhere in the organization.

Context sets the stage for the decision or activity requiring risk management; *risk assessment* identifies, analyzes, and evaluates the risks; *risk treatment* enhances the likelihood of positive consequences and reduces the likelihood of negative consequences to acceptable or tolerable levels; *monitoring and review* keeps close watch over the risk and the controls implemented to modify the risk; and *communication and consultation* is continuous to ensure that the stakeholders are engaged and contribute to the management of risks.

The Risk Management Process (RMP) is the first framework component presented because it is used for all decisions in the organization. RMP is a method to modify risks to create value. The ERM framework exists primarily to facilitate application of the RMP everywhere in the organization.

The RMP in Figure 1 is not a flow chart but a relational diagram that must be tailored to the individual organization before implementation as a process flow chart. The tailored implementation ensures that risk management is both practical and aligned with the organization's structures, processes, and objectives *Shortreed* (2010).

Figure 1. An ISO 31000 Compatible Framework for Implementing ERM Including the Risk Management Process



Source: *Shortreed* (2010) taken from Broadleaf Capital International Pty Ltd., 2008, www.Broadleaf.com.au.

4.2. Risk universe

Before taking further steps into detailing methods for measuring and predicting the risk faced by financial institution we consider that it would useful to identify and classify the risks.

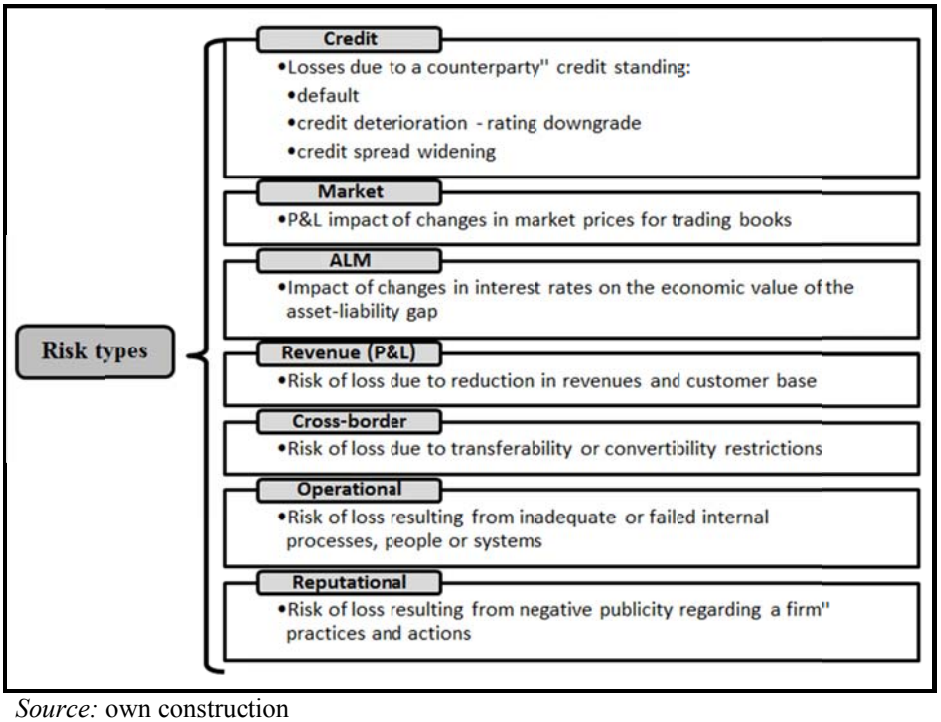
Risk can be defined as the likelihood and severity of events that lead to loss of capital and/or less-than expected returns. How an institution interprets this definition helps to determine what the strategic goals of risk management are.

Risk can be idiosyncratic or systemic. *Idiosyncratic risk* is the risk of price change (or default on debt) due to the unique circumstances of a specific security (obligor), as opposed to the overall market. In terms of unexpected loss, this risk may be virtually eliminated from a portfolio through diversification, as losses converge on their expected value. In this case, it is called *diversifiable risk*. In contrast, *systemic risk* affects an entire financial market or system, and not just specific participants or obligors (for example, the exposure to credit cycles or industry downturns). In practice, financial institutions may be unable to completely eliminate systemic risk through diversification, making it a *non-diversifiable risk*.

In the case of credit risk, for example, diversification (across asset classes as well as obligor names, regions, sectors, and so on) can lower the variance of expected losses, but diversification cannot eliminate idiosyncratic risk in the same way as it does for market risk. First, because of the asymmetry of returns associated with most types of bank lending and debt issuance, improving credits cannot precisely offset losses on idiosyncratic defaults. Second, the concept itself is not an accurate analogy to the market risk case because the idea that a particular firm is forced to default because of changes in aggregate credit risk (and for no other reason) is debatable.

For operational and reputation risks, the situation may even be reversed, in that risks may compound as business activities expand in scope. Clearly, one of the primary problems in quantitative risk management is that of classifying the various types of risks faced by the institution, and establishing a consistent set of metrics for each. Regulators, financial institutions, and rating agencies usually group risks in a handful of broad types, which are detailed underneath the Figure below.

Figure 2. Main types of risks currently faced by financial institutions



Source: own construction

a) Credit risk

Credit risk encompasses both the possibility that a borrower will default by failing to repay principal and interest in a timely manner, and the possibility that the credit quality of the obligor will deteriorate, leading to an economic loss. Sometimes the risk faced by an institution is not related to the instrument itself but to a third party responsible for some aspect of the transaction. The risk that this party will prevent the settlement of the obligation for full value, either when due or at any other time thereafter, is called counterparty risk.

Statistical models for assessing credit risk at the facility, obligor, and portfolio level have been available for decades. However, only recently financial institutions and vendors of risk management solutions have been able to collect and process sufficiently rich and timely flows of data to make model implementation feasible for supporting quantitative capital management and allocation strategies. Whether obligor risk measures are based on commercial models, internally developed models, or other methodologies, institutions will still need to perform model validation and data reliability tests to verify the benefits and limitations of the different approaches and the impact on their businesses. Thus, quantitative expertise and the ability to implement and validate mathematical modeling tools are now major concerns for most institutions.

b) Market risk

Market risk results from the possibility that the price of an asset may decline or the value of obligations (such as swap exposures, options, or futures contracts) may grow over a given time period simply because of economic changes or other events that impact the market price of securities, commodities, and interest rates. Market risk is somewhat unique in that it can be largely hedged using an array of market products designed specifically for this purpose, including options, futures, and other derivatives.

Because assets are acquired with a specific purpose in mind, market risk is often associated more with "potential" loss as opposed to "expected" loss, in that day-today fluctuations in asset prices create losses only when those assets must be liquidated on a day-to-day basis. Buy-and-hold investors can ignore short-term price movements except insofar as a crisis situation may force assets to be sold on short notice. Therefore, institutions must make sensible links between how they interpret standard market risk measures, and how they characterize "normal" versus "stress" scenarios in their broader risk management and capital allocation practice.

c) Asset-liability management risk, also called in other papers Liquidity risk

ALM risk is the risk that a mismatch between assets and liabilities will cause a liquidity shortfall, or necessitate loss-generating balance sheet adjustments to avoid a liquidity shortfall. For most firms, ALM risk is dominated by the risk that changes in the level of interest rates or their term structure will negatively affect the asset/liabilities balance, leading to a shortage of cash to meet current obligations. However, the tenor and structural cash flow relationships between assets and liabilities can become unbalanced due to inattention, failed speculation, and operational risks. Banks and other financial institutions are sensitive to all of these ALM risks due to the particular nature of their business (often borrowing short term from depositors and lending long-term loans to borrowers).

d) P&L (Revenue) risk

Here the risk is not that the tenor or expected cash flows from assets will not match with those required by liabilities, but that unexpected volatility in revenues may precipitate such a mismatch, especially in businesses with significant fixed costs. For banks and other financial

institutions, most shocks to revenue are the result of changes in market conditions; for example, falling interest rates combined with sluggish economic growth.

Other disturbances to revenues may result from political and reputation crises that can result in loss of customer confidence, customer volume, or market share. As a result, there is considerable overlap between P&L risk and other classes of risk that are already being measured and managed by the firm. Nevertheless, revenue volatility can be reduced by careful management of the products and services being offered.

e) Cross-Border Risk

Cross-border risk is the risk of loss due to transferability or convertibility restrictions in different countries. This type of risk affects primarily institutions that do businesses in multiple markets and countries.

f) Operational Risk

Generally speaking, operational risk is the risk of loss resulting from inadequate or failed processes (internal or external), people, and systems or from external events (that is, a potential failure in a business). Classic examples of operational failures include massive losses due to unauthorized "rogue" trading, internal and external fraud, and criminal mismanagement and corporate theft. However, failures to the physical plant and equipment of the firm also present significant operational risks.

If electronic trading, clearing, or wire transfer systems fail, trading and legal liability losses can be substantial. Declining profitability may also increase risk when management places heavy burdens on business heads to meet aggressive or unrealistic profit targets. Here, quality controls may be ignored in an environment myopically focused on short-term performance. Regulatory compliance requires that banks track and categorize operational risk "events," so the raw data for more quantitative research will continue to accumulate going forward.

g) Reputational risk

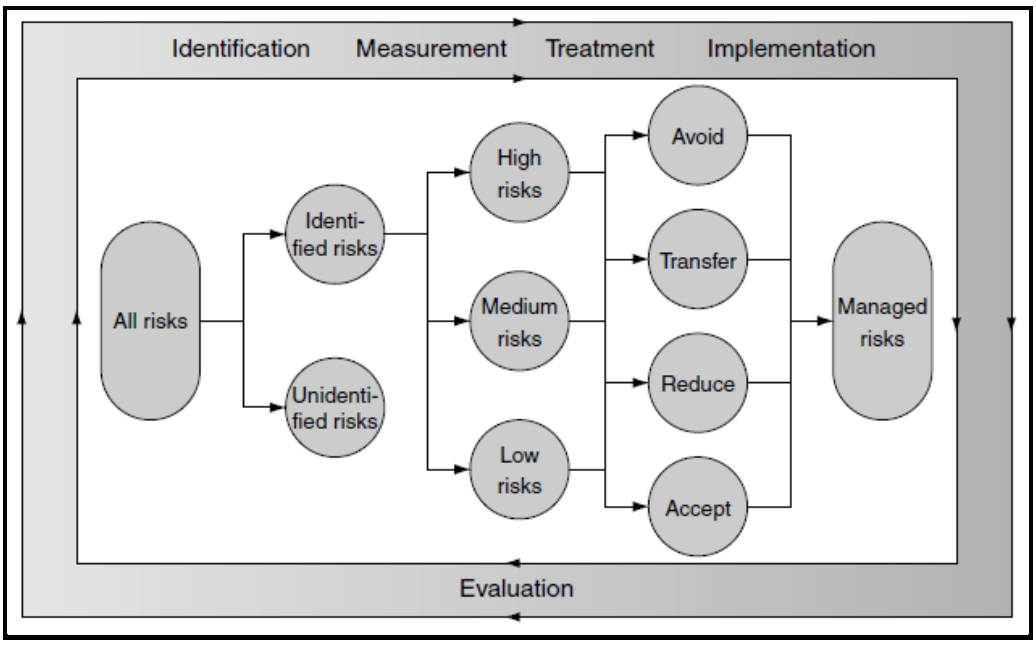
Reputation risk is the potential that negative publicity regarding a firm's practices and actions will cause a decline in the customer base, costly litigation, revenue reduction, liquidity constraints, or significant depreciation in market capitalization. Reputation is one of the most valuable assets a company can have, and one of the most difficult to protect.

Certainly, the avoidance of events that may damage a firm's reputation lies properly in the sphere of operational risk. However, most large firms engage in reputation enhancing efforts that are effectively hedges against future damage, and these hedges can be evaluated on a cost benefit basis. Moreover, the firm's response to actual reputation damage can be organized and rational, and could potentially make use of a formal modelling approach. The crucial components required to support an active reputation risk management regime include the identification and ranking of constituents, in terms of the benefits of remediation, and an identification and ranking of information flows available for remediation in terms of cost and efficacy. Despite its importance to a firm's survival, the quantification of reputation risk is still in its infancy.

5. Risk management process

The main steps in a risk management process are presented in Figure 3 and described below.

Figure 3. Steps of continuous risk management process



Source: Van Gestel–Baesens (2009)

a) Identification

Within a defined perimeter and scope of the risk management process, one identifies all potential risks. The identification can start by analyzing sources of potential risk (e.g., lower housing prices may result in lower recoveries and higher losses on a mortgage loan) or identifying threats (e.g., which factors would result in higher losses on a mortgage loan). The identification of all the risks requires a good knowledge of the financial products. A main risk is the lack of identification ability in the organization, e.g., due to insufficient competencies.

b) Measurement

Given the identified sources of risk, one needs to quantify the risk. For credit risk, this means, e.g., that one needs to determine the actual default probability and how much a change of the risk drivers (e.g., profitability of a firm) impacts the default probability. How much will the loss given default increase if housing prices reduce by 10%? Risk measurement requires thorough statistical analysis of past events. When in case past events are only available to a limited extent, one applies theoretical models and expert knowledge to quantify the risk.

c) Treatment

Risk can be treated via one of the following four ways (*Dorfmann* 1997):

Risk avoidance: A simple way to treat risk is to avoid risk. This implies that one does not invest in products that are too risky or for which the risk is not well enough understood. Avoidance does not mean that one avoids all risk, a strategy may consist of selecting the good counterparts and not investing in counterparts with too high default, loss or exposure risk. Alternatively, one may decide to invest only small proportions in such counterparts; one limits the exposure on risky investments. This reduces the concentration risk.

Risk reduction: Risk reduction or mitigation implies that one takes a part of the risk, but not the full part of it. For high-risk counterparts, one may require collateral that the bank can sell in the case of a default. The value of the sold collateral reduces the actual and hence the risk for the bank. One may also ask guarantees from a family. Risk reduction may not always be feasible.

Risk acceptance: One accepts or retains the risk that one has to take as part of the business strategy. Risk acceptance is typically applied for low-risk assets. Risk is more easy accepted when it is well diversified: investments are made in various sectors and countries, where it is unlikely that high losses will occur simultaneously in all sectors and in all countries.

Risk transfer: One transfers the risk to another bank, insurance or company. Insurance companies, called financial guarantors, exist that provide guarantees to credit risk. A specific type of credit derivatives, a.o., credit default swaps are a type of option contract in which the buyer of the contract is reimbursed in the case of the default of the underlying counterpart.

d) Risk management strategies

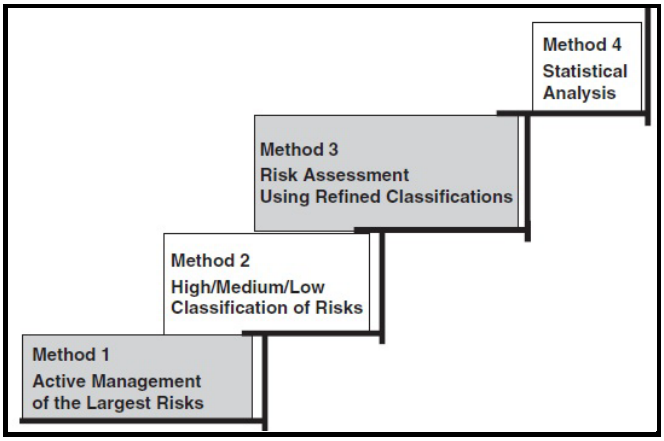
Implementation: Once the risk management strategy has been defined, it is implemented. People, statistical models and IT infrastructure evaluate the risk of existing and new investments. Guidelines for the risk treatment define in which counterparts does one invest and in which one does not; which exposure limits are used for the most risky products; whether collateral for specific loans is mandatory or whether one buys protection from a financial guarantor. The risks of the bank are continuously reported and monitored. The implementation is supervised by senior management.

Evaluation: The effectiveness of the risk management strategy is evaluated frequently. One verifies whether the resulting risk taking remains in line with the strategy and applies corrections where necessary. This involves evaluation of the relevant risk drivers, the measurement process is evaluated, in back-testing procedures, the result of the risk treatment plans and the actual implementation.

6. Alternative approaches of risk assessment

When deciding the most appropriate method of evaluating an organization's risks, there is a choice between several broad alternative approaches, that are illustrated in Figure 4. The appropriate choice between them depends on cultural and environmental considerations, and on the industry concerned. In this paper, we consider mainly strategic risks and managerial situations where financial risks are not dominant. It is worthwhile to examine the four main alternative methods for the assessment of strategic risks, and to consider issues that contribute to the choice between them.

Figure 4. Methods of quantifying risk



Source: Hargreaves (2010, p. 223.)

6.1. Active management of the largest risks

Companies' executives will often claim that they are already aware of the main risks that their organizations face. Thus, they would argue that the most important risk-management task is to manage these risks well. This attitude is justified by the fact that about 80 percent of the total risk facing an organization is usually concentrated in the top dozen risks.

In organizations that are beginning the implementation of risk management, and in those going through crisis situations, the resources available to control risk may be limited. In such circumstances it may be best to concentrate initially on the effective management of key risks. This avoids spreading the management effort too thinly and less effectively.

There are large differences in risk probabilities. Some risks occur rarely and others happen quite frequently. Nevertheless, to uncover the top dozen risks with confidence it is usually necessary to consider at least twice that number of risks. This analysis often reveals a couple of large risks that have been underestimated by management.

It is sensible to take advantage of the effect of large differences in risk impact and probability through the adoption of an "Active" style of risk management (Table 1.). It is certainly better to actively manage the top 12 risks than to make a long list of risks and do little about any of them!

Table 1. The necessity to tackle top risks first

Probability	Impact	Action
High	High	Immediate
High	Low	Consider steps to take
Low	High	Consider steps to take and produce a contingency plan
Low	Low	Keep under review

Source: Hargreaves (2010, p. 223.)

The idea of concentrating on the top risks is good as a first approach to risk evaluation. Often it is also appropriate in a transitory situation where an organization is going through a process of rapid change. However, it is not an adequate basis for confident risk management in the medium term.

Active management of the top risks suffers from the drawback that it is not comprehensive. The business world is littered with examples of infrequently occurring risks that have led to the downfall of organizations. Sector regulators seek to ensure that companies do not overlook any risks that may have significant adverse impacts, but recent experience tells us that this is difficult to achieve in practice. However, favourable experience of the savings or risk reductions made by good management of the important risks indicates the benefits of extending management attention to the less significant risks as well.

6.2. The two-dimensional risk map: "High/Medium/Low" classification of risks

A more complete coverage of risks may be obtained by using the two-dimensional risk map approach illustrated in Table 2 Following this approach, a detailed list of risks is drawn together that, as far as possible, covers all the company's activities. For each risk, estimates of the probability of the risk occurring and the impact of the risk are made. These estimates are expressed in terms of High/Medium/Low categories (for example) and plotted on a risk map to illustrate graphically the relative rankings of their respective probabilities and impacts (*Risk Management Standard* 2002).

It is common in this sort of approach to use traffic-light colour highlights (i.e., red, orange, and green), in reports to distinguish high, medium, and low risks. Noncritical risks

that are being managed satisfactorily are signified by a "Green Light" signal, and conversely high-risk situations that are causing concern are indicated by a "Red Light" signal.

Table 2. Example of a two-dimensional risk map

		Impact		
		Limited	**Some**	**Significant**
Likelihood / Probability	**High**	M	H	H
	Medium	L	M	H
	Low	L	L	M

Source: Hargreaves (2010, p. 224.)

The High/Medium/Low approach can work quite well if the risk analysis is done mainly by one person. However, if the risks are to be tackled at all levels of the organization, a number of people will need to be involved and there will be different views of specific risks. The High/Medium/Low classification suffers from the deficiency that it is a crude gauge. It does not register graduations of risk other than within the three-fold classification. So, if management expends effort to reduce a particular risk, it may well continue to register as "high." Thus, a system with only three graduations may be difficult to use for control purposes and at lower levels of the organization most risks would be classified as low. Thus, although this methodology meets the needs of some standards and regulators, we do not recommend it since, for a relatively small additional effort, a slightly more sophisticated methodology on the lines of Method 3 described below will be much more effective.

6.3. Risk assessment using refined classifications

A possible solution to a simple but more effective risk management methodology is to employ a more refined classification of probabilities and impacts. For example, the graduations may be increased to five classifications such as Very High, High, Medium, Low, and Very Low, as recommended in the Australian and New Zealand Standards (*Australian Standards* 2004).

If we have more scale graduations, it is more important to define exactly what we mean by each one. In order to achieve uniformity, numeric bands are established both for impact and probability. Thus, for a medium-sized company we might define a very high financial impact to mean an impact of more than say $1 million. Managers may not initially feel confident in making quantified probability estimates. However, in practice they are usually happy to estimate a probability using the probability scale as shown in Table 3 In this scale, there is an approximate tripling of probability between one level and the next this level of accuracy works well for many risk-management purposes, except for the most important risks that may need to be examined in detail.

Table 3. An example of a probability scale

Probability Score	Description	Range
5	Very High	More than 90%
4	High	31% to 90%
3	Medium	11% to 30%
2	Low	3% to 10%
1	Very Low	Less than 3%

Source: Hargreaves (2010, p. 226.)

In a situation where a risk is present with an associated set of controls, the question arises as to which probabilities we should assess. In particular, we normally assume that the existing controls are in place, and assess the probability that the risk will occur either in the following year or over the course of a short planning period. Some practitioners, in particular those with an internal audit background, try to estimate also the probability that the risk would occur without the controls in place. This provides information on the value of the existing controls.

6.4. Statistical Analysis

So far this paper has examined the use of bands or single "best guess" estimates of the impact and probability of each risk to represent its importance. However, this is a simplification of reality because in practice we may be uncertain of the probability estimates and the possible impact of the risk may vary continuously from almost zero to a high figure.

Sometimes we may want to examine the impact of a number of risks together, for example, because their incidence is strongly interconnected. In such cases one might be able to make some progress by examining a set of "what if" scenarios, making a range of assumptions for each risk. However, there may be too large a set of possibilities for this to be practical, in which case a more exact model can be created using Monte Carlo simulation techniques. The Monte Carlo approach is similar to the "what if" scenario method because it generates possible scenarios, but the number of scenarios examined is large and the variables used to generate the scenarios are weighted by the probability of their occurrence. Thus, each risk can be represented by a probability distribution rather than as a single value. The objective of the simulation model is to calculate the combined impact of the various uncertainties to obtain a probability distribution of the total outcome, perhaps at total-organization level. In practice this is easier to accomplish than one would think, because all the relevant technical aids are available in a spreadsheet-based form that is not difficult to use (*Hargreaves* 2010).

6.5. Aggregating probabilities and impacts

An example is shown below to demonstrate the logic of risk aggregation using two risks. In the example, the two risks lead to only four possible combined outcomes. In practice there will be a number of risks and each will have range of outcomes. Combining these together cannot be done manually, but cheap spreadsheet-based models are commercially available and these are not difficult to use.

Risks do not "add up" in a straightforward manner, but can be aggregated using statistical techniques. This may be illustrated by the below two-risk example. The example assumes two maintenance risks in a housing association's content. The two risks happen independently of one another.

Risk A. As a consequence of a lack of quality maintenance contractors there is a risk that maintenance may not be of suitable quality due to allocation of work to an incompetent contractor. The risk has an assessed probability of 25% per annum and impact of €30,000.

Risk B. There is a risk that taking legal proceedings against a maintenance contractor to achieve agreed performance may be disproportionately expensive due to slow court procedures. The risk has an assessed probability of 50% per annum and impact of €20,000.

In this way the average cost (often called the "expected loss") of each risk can be easily calculated. They can be simply added up to get the average cost for the whole organization.

In order to calculate what might happen in a particular year we need to enumerate the combinations of possibilities. The table gives the distribution of combined impacts for the year. For example, there is a 12.5% probability of a combined loss of €50,000, but on the

other hand a 37.5% probability of no loss at all. This illustrates that in practice it is more important to know the distribution of out-turns than it is to know the average cost of the risks.

Example 1a. Adding expected losses

Then the average cost of Risk A over a number of years will be 25% of €30,000 per year or	€7,500 per year
and the average cost of Risk B over a number of years will be 50% of €20,000 per year or	€10,000 per year
So the average cost of both risks together over a number of years will be	€17,500 per year

Source: own construction

Example 1b. Calculating the distribution of combined impacts

RISK A			**RISK B**			**Combined risks A & B**	
It occurs?	Probability (%)	Impact (€)	It occurs?	Probability (%)	Impact (€)	Probability (%)	Impact (€)
Yes	25	30,000	Yes	50	20,000	12.5	50,000
Yes	25	30,000	No	50	–	12.5	30,000
No	75	–	Yes	50	20,000	37.5	20,000
No	75	–	No	50	–	37.5	–

Source: own construction

7. Conclusions

Modern risk management builds upon a sound foundation of traditional risk management and gives organizations a number of tools to use when addressing enterprise risk. These practices continue to be essential in the areas of hazard risk, internal controls, and regulatory compliance but are finding increasing applications for dealing with the broader exposures confronting profit, non-profit, and governmental bodies.

ERM can work in organizations of all sizes. The mega corporation can use it in a structured hierarchical system with risk owners and sub-risk owners. A single business unit in such an entity can use it as part of the parent system or even in isolation. A smaller organization can seek an understanding of the challenges it faces as it seeks to grow and prosper.

This is the closing message of ERM. Managing risk is not about hundreds or thousands of unorganized exposures. It is about getting value from an effort to understand the impact of risks and interrelationships of risk and opportunity. With new technology and the impact of the 2008 financial crisis, we can expect a renewed interest in getting it right with enterprise risk management.

Enterprise risk management (ERM) is being adopted by an increasing number of firms and is viewed as a paramount topic for business enterprises desiring to survive and succeed in the future. As *Fraser*, *Schoening-Thiessen*, and *Simkins* (2008) state: "ERM is not a fad – it is here to stay and is the natural evolution of risk management to view risk at the enterprise-wide level. New external drivers are pushing risk executives to find out more about ERM and the level of interest in this topic is increasing with time."

Unfortunately, the pace of academic research does not seem to be keeping pace with corporate interest in the topic. A primary hindrance to research of ERM is a lack of well-defined variables that measure either company-level implementation of ERM or the degree of implementation.

This paper discusses the four alternative approaches of an organization's quantification of risk and presents a method for quantifying the total amount of risk in an organization's business plan. However, we believe that the choice depends on the organization's circumstances and capabilities. The members of the board need to feel that they have adequately assessed the risk and that the residual risk, after reduction measures and controls, is acceptable. It follows that a company's risk management strategy should be closely related to and consistent with its overall strategy. In particular, there is a great deal of agreement that the overall strategy should not conflict with the risk appetite of the organization. The risk appetite might be set in the risk management strategy statement as limiting the total amount of risk taken so that it does not exceed agreed-upon quantified limits.

References

Arnold, G. – Davies, M. 2000: *Value-Based Management: Context and Application*. John Wiley & Sons, Chichester.

Australia Standards 2004: AS/NZS 4360 Risk Management.

Bank for International Settlements (BIS) Joint Forum. 2003: *Trends in Risk Integration and Aggregation*. www.bis.org. [Accessed 10 January 2012]

Beasley, M. S. – Clune, R. – Hermanson, D. R. 2005a: ERM: A status report. *Internal Auditor*, 62, 1, pp. 67–72.

Beasley, M. S. – Clune, R. – Hermanson, D. R. 2005b: Enterprise risk management: An empirical analysis of factors associated with the extent of implementation. *Journal of Accounting and Public Policy*, 24, 6, 521–531.

Bell, T. – Marrs, F. – Solomon, I. – Thomas, H. 1997: *Auditing organizations through a strategic-systems lens: the KPMG business measurement process*. KPMG Peat Marwick, LLP.

Coles, S. 2001: *An introduction to statistical modelling of extreme values*. London, UK, Springer–Verlag.

Colquitt, L. – Hoyt, R. E. – Lee, R. B. 1999: Integrated risk management and the role of the risk manager. *Risk Management and Insurance Review*, 2, pp. 43–61.

Committee of Sponsoring Organizations of the Treadway Commission (COSO) 2004: Enterprise Risk Management Framework. September, Available on http://www.coso.org/ documents/COSO_ERM_ExecutiveSummary.pdf. [Accessed 10 January 2012]

Dorfmann, M. 1997: *Introduction to risk management and insurance.* 6th edition, Prentice Hall, New Jersey.

Drzik, J. – Nakada, P. – Schuermann, T. 2004: *Risk Capital Measurement in Financial Institutions*. Part One, www.erisk.com. [Accessed 10 January 2012]

Embrechts, P. – Kluppelberg, C. – Mikosch, T. 1997: *Modelling extreme values for insurance and finance*. Berlin, Germany, Springer–Verlag.

Fraser, J. R. S. – Schoening-Thiessen, K. – Simkins, B. J. 2008: Who reads what most often? A survey of enterprise risk management literature read by risk executives. *Journal of Applied Finance*, 18, 1, pp. 73–91.

Garside, T. – Nakada, P. 1999: Enhancing risk measurement capabilities. *Balance Sheet*, 8, 3, pp. 12–17.

Gumbel, B. 1935: Les valeurs extremes des distributions statistiques. *Annales de l'Institut Henri Poincare*, 5, pp. 115–158.

Gumbel, B. 1958: *Statistics of extremes*. New York, Columbia University Press.

Hampton, J. J. 2009: *Fundamentals of Enterprise Risk Management-How Top Companies Assess Risk, Manage Exposures, and Seize Opportunities*. ISBN–13: 978–0–8144–1492–7, American Management Association, New York.

Hargreaves, J. 2010: Quantitative Risk Assessment in ERM, In Fraser, J. – Simkins, B. J.: *Enterprise Risk Management: today's leading research and best practices for tomorrow's executives*. John Wiley & Sons, New Jersey, pp. 219–235.

Kleffner, A. E. – Lee, R. B. – McGannon, B. 2003b: The effect of corporate governance on the use of enterprise risk management: Evidence from Canada. *Risk Management and Insurance Review*, 6, 1, 53–73.

Knechel, R. 2002: The role of the independent accountant in effective risk management. *Journal of Economics and Management*, pp. 65–86.

Liebenberg, A. –Hoyt, R. 2003: The determinants of enterprise risk management: Evidence from the appointment of chief risk officers. *Risk Management and Insurance Review*, 6, 1, pp. 37–52.

Marrison, C. 2002: *The Fundamentals of Risk Measurement*. McGrawHill, New York.

Miccolis, J. – Hively, K. – Merkley, B. 2001: *Enterprise risk management: trends and emerging practices.* Institute of Internal Auditors Research Foundation, Altamonte Springs.

Pagach, D. – Warr, R. 2007: *An Empirical Investigation of the Characteristics of Firms Adopting Enterprise Risk Management*. North Carolina State University working paper.

Reiss, R-D. – Thomas, M. 2001: *Statistical analysis of extreme values*. 2nd edition, Basel, Switzerland, Birkhauser.

Risk Management Standards 2002: IRM, Airmic and Alarm.

Shortreed, J. 2010: ERM Frameworks. In Fraser, J. – Simkins, B. J.: *Enterprise Risk Management: today's leading research and best practices for tomorrow's executives*. John Wiley & Sons, New Jersey, pp. 97–123.

Van Gestel, T. – Baesens, B. 2009: *Credit Risk Management*. Oxford University Press, New York, ISBN 978–0–19-954511–7.