1

Risk management: a general view

Ron S. Kenett, Richard Pike and Yossi Raanan

1.1 Introduction

Risk has always been with us. It has been considered and managed since the earliest civilizations began. The Old Testament describes how, on the sixth day of creation, the Creator completed his work and performed an *ex post* risk assessment to determine if further action was needed. At that point in time, no risks were anticipated since the 31st verse of Genesis reads 'And God saw every thing that he had made, and, behold, it was very good' (Genesis 1: 31).

Such evaluations are widely conducted these days to determine risk levels inherent in products and processes, in all industries and services. These assessments use terms such as 'probability or threat of a damage', 'exposure to a loss or failure', 'the possibility of incurring loss or misfortune'. In essence, risk is linked to uncertain events and their outcomes. Almost a century ago, Frank H. Knight proposed the following definition:

> Risk is present where future events occur with measureable probability.

Quoting more from Knight:

> Uncertainty must be taken in a sense radically distinct from the familiar notion of risk, from which it has never been properly separated . . . .

Operational Risk Management: A Practical Approach to Intelligent Data Analysis Edited by Ron S. Kenett and Yossi Raanan

> The essential fact is that 'risk' means in some cases a quantity susceptible of measurement, while at other times it is something distinctly not of this character; and there are far-reaching and crucial differences in the bearings of the phenomena depending on which of the two is really present and operating .... It will appear that a measurable uncertainty, or 'risk' proper, as we shall use the term, is so far different from an unmeasurable one, that it is not in effect an uncertainty at all'.
>
> (Knight, 1921)

According to Knight, the distinction between risk and uncertainty is thus a matter of knowledge. Risk describes situations in which probabilities are available, while uncertainty refers to situations in which the information is too imprecise to be summarized by probabilities. Knight also suggested that uncertainty can be grasped by an 'infinite intelligence' and that to analyse these situations theoreticians need a continuous increase in knowledge. From this perspective, uncertainty is viewed as a lack of knowledge about reality.

This separates 'risk' from 'uncertainty' where the probability of future events is not measured. Of course what are current uncertainties (e.g. long-range weather forecasts) may some day become risks as science and technology make progress.

The notion of risk management is also not new. In 1900, a hurricane and flood killed more than 5000 people in Texas and destroyed the city of Galveston in less than 12 hours, materially changing the nature and scope of weather prediction in North America and the world. On 19 October 1987, a shock wave hit the US stock market, reminding all investors of the inherent risk and volatility in the market. In 1993, the title of 'Chief Risk Officer' was first used by James Lam, at GE Capital, to describe a function to manage 'all aspects of risk' including risk management, back-office operations, and business and financial planning. In 2001, the terrorism of September 11 and the collapse of Enron reminded the world that nothing is too big to collapse.

To this list, one can add events related to 15 September 2008, when Lehman Brothers announced that it was filing for Chapter 11 bankruptcy protection. Within days, Merrill Lynch announced that it was being sold to rival Bank of America at a severely discounted price to avert its own bankruptcy. Insurance giant AIG, which had previously received an AAA bond rating (one of only six US companies to hold an AAA rating from both Moody's and S&P) stood on the brink of collapse. Only an $85 billion government bailout saved the company from experiencing the same fate as Lehman Brothers. Mortgage backers Fannie Mae and Freddie Mac had previously been put under federal 'governorship', to prevent the failure of two major pillars in the US mortgage system. Following these events, close to 1000 financial institutions have shut down, with losses up to $3600 billion.

The car industry has also experienced such events. After Toyota announced a recall of 2.3 million US vehicles on 21 January 2010, its shares dropped 21%,

wiping out $33 billion of the company's market capitalization. These widely publicized events keep reinvigorating risk management.

The Food and Drug Administration, National Aeronautics and Space Administration, Department of Defense, Environmental Protection Agency, Securities and Exchange Commission and Nuclear Regulatory Commission, among others, have all being implementing risk management for over a decade. Some basic references that form the basis for these initiatives include: Haimes (2009), Tapiero (2004), Chorafas (2004), Ayyub (2003), Davies (1996) and Finkel and Golding (1994).

Risk management, then, has long been a topic worth pursuing, and indeed several industries are based on its successful applications, insurance companies and banks being the most notable. What gives this discipline enhanced attention and renewed prominence is the belief that nowadays we can do a better job of it. This perception is based on phenomenal developments in the area of data processing and data analysis. The challenge is to turn 'data' into information, knowledge and deep understanding (Kenett, 2008). This book is about meeting this challenge. Many of the chapters in the book are based on work conducted in the MUSING research project. MUSING stands for MUlti-industry, Semantic-based next generation business INtelliGence (MUSING, 2006). This book is an extended outgrowth of this project whose objectives were to deliver next generation knowledge management solutions and risk management services by integrating Semantic Web and human language technologies and to combine declarative rule-based methods and statistical approaches for enhancing knowledge acquisition and reasoning. By applying innovative technological solutions in research and development activities conducted from 2006 through 2010, MUSING focused on three application areas:

1. *Financial risk management.* Development and validation of next generation (Basel II and beyond) semantic-based business intelligence (BI) solutions, with particular reference to credit risk management and access to credit for enterprises, especially small and medium-sized enterprises (SMEs).
2. *Internationalization.* Development and validation of next generation semantic-based internationalization platforms supporting SME internationalization in the context of global competition by identifying, capturing, representing and localizing trusted knowledge.
3. *Operational risk management.* Semantic-driven knowledge systems for operational risk measurement and mitigation, in particular for IT-intensive organizations. Management of operational risks of large enterprises and SMEs impacting positively on the related user communities in terms of service levels and costs.

Kenett and Shmueli (2009) provide a detailed exposition of how data quality, analysis quality and information quality are all required for achieving knowledge

with added value to decision makers. They introduce the term InfoQ to assess the quality of information derived from data and its analysis and propose several practical ways to assess it. The eight InfoQ dimensions are:

1. *Data granularity.* Two aspects of data granularity are measurement scale and data aggregation. The measurement scale of the data must be adequate for the purpose of the study and. The level of aggregation of the data should match the task at hand. For example, consider data on daily purchases of over-the-counter medications at a large pharmacy. If the goal of the analysis is to forecast future inventory levels of different medications, when restocking is done on a weekly basis, then we would prefer weekly aggregate data to daily aggregate data.

2. *Data structure.* Data can combine structured quantitative data with unstructured, semantic-based data. For example, in assessing the reputation of an organization one might combine data derived from balance sheets with data mined from text such as newspaper archives or press reports.

3. *Data integration.* Knowledge is often spread out across multiple data sources. Hence, identifying the different relevant sources, collecting the relevant data and integrating the data directly affects information quality.

4. *Temporal relevance.* A data set contains information collected during a certain period of time. The degree of relevance of the data to the current goal at hand must be assessed. For instance, in order to learn about current online shopping behaviours, a data set that records online purchase behaviour (such as Comscore data, www.comscore.com) can be irrelevant if it is even one year old, because of the fast-changing online shopping environment.

5. *Sampling bias.* A clear definition of the population of interest and how a sample relates to that population is necessary in both primary and secondary analyses. Dealing with sampling bias can be proactive or reactive. In studies where there is control over the data acquisition design (e.g. surveys), sampling schemes are selected to reduce bias. Such methods do not apply to retrospective studies. However, retroactive measures such as post-stratification weighting, which are often used in survey analysis, can be useful in secondary studies as well.

6. *Chronology of data and goal.* Take, for example, a data set containing daily weather information for a particular city for a certain period as well as information on the air quality index (AQI) on those days. For the United States such data is publicly available from the National Oceanic and Atmospheric Administration website (www.noaa.gov). To assess the quality of the information contained in this data set, we must consider the purpose of the analysis. Although AQI is widely used (for instance, for issuing a ‘code red’ day), how it is computed is not easy to figure out. One analysis goal might therefore be to find out how AQI is computed

from weather data (by reverse engineering). For such a purpose, this data is likely to contain high-quality information. In contrast, if the goal is to predict future AQI levels, then the data on past temperatures contains low-quality information.

7. *Concept operationalization.* Observable data is an operationalization of underlying concepts. 'Anger' can be measured via a questionnaire or by measuring blood pressure; 'economic prosperity' can be measured via income or by unemployment rate; and 'length' can be measured in centimetres or in inches. The role of concept operationalization is different for explanatory, predictive and descriptive goals.

8. *Communication and data visualization.* If crucial information does not reach the right person at the right time, then the quality of information becomes poor. Data visualization is also directly related to the quality of information. Poor visualization can lead to degradation of the information contained in the data.

Effective risk management necessarily requires high InfoQ. For more on information quality see Guess (2000), Redman (2007) and Kenett (2008).

We are seeking knowledge and require data in order to start the chain of reasoning. The potential of data-driven knowledge generation is endless when we consider both the increase in computational power and the decrease in computing costs. When combined with essentially inexhaustible and fast electronic storage capacity, it seems that our ability to solve the intricate problems of risk management has stepped up several orders of magnitude higher.

As a result, the position of chief risk officer (CRO) in organizations is gaining popularity in today's business world. Particularly after the 2008 collapse of the financial markets, the idea that risk must be better managed than it had been in the past is now widely accepted (see Kenett, 2009). Still, this position is not easy to handle properly. In a sense it is a new version of the corporate quality manager position which was popular in the 1980s and 1990s. One of the problems inherent in risk management is its almost complete lack of glamour. Risk management done well is treated by most people like electric power or running water – they expect those resources to be ever present, available when needed, inexpensive and requiring very little management attention. It is only when they are suddenly unavailable that we notice them. Risks that were well managed did not materialize, and their managers got little attention. In general, risk management positions provide no avenues to corporate glory. Indeed, many managers distinguish themselves in times of crisis and would have gone almost completely unnoticed in its absence. Fire fighting is still a very prevalent management style. Kenett *et al*. (2008) formulated the Statistical Efficiency Conjecture that stipulates that organizations exercising fire fighting, as opposed to process improvement of quality by design, are less effective in their improvement initiatives. This was substantiated with 21 case studies which were collected and analysed to try to convince management that prevention is carrying significant rewards.

An example of this phenomenon is the sudden glory bestowed on Rudy Giuliani, the former Mayor of New York City, because of his exceptional crisis management in the aftermath of the September 11 terrorist attack on the twin towers. It was enough to launch his bid for the presidency (although not enough, apparently, to get him elected to that office or even to the post of Republican candidate). Had the attacks been avoided, by a good defence intelligence organization, he would have remained just the Mayor of New York City. The people who would have been responsible for the prevention would have got no glory at all, and we might even never have heard about them or about that potential terrible threat that had been thwarted. After all, they were just doing their job, so what is there to brag about? Another reason for not knowing about the thwarted threat, valid also for business risk mitigation strategies, is not exposing the methods, systems and techniques that enabled the thwarting.

Nonetheless, risk management is a critically important job for organizations, much like vaccination programmes. It must be funded properly and given enough resources, opportunities and management attention to achieve concrete results, since it can be critical to the organization's survival. One should not embrace this discipline only after disaster strikes. Organizations should endeavour to prevent the next one by taking calculated, evidence-based, measured steps to avoid the consequences of risk, and that means engaging in active risk management.

1.2 Definitions of risk

As a direct result of risk being a statistical distribution rather than a discrete point, there are two main concepts in risk measurement that must be understood in order to carry out effective risk management:

1. *Risk impact*. The impact (financial, reputational, regulatory, etc.) that will happen should the risk event occur.
2. *Risk likelihood*. The probability of the risk event occurring.

This likelihood usually has a time period associated with it. The likelihood of an event occurring during the coming week is quite different from the likelihood of the same event occurring during the coming year. The same holds true, to some extent, for the risk impact since the same risk event occurring in two different points in time may result in different impacts. These differences between the various levels of impact may even owe their existence to the fact that the organization, realizing that the event might happen, has engaged actively in risk management and, at the later of the two time periods, was better prepared for the event and, although it could not stop it from happening, it succeeded in reducing its impact.

Other base concepts in the risk arena include:

- *Risk event*. An actual instance of a risk that happened in the past.
- *Risk cause*. The preceding activity that triggers a risk event (e.g. fire was caused by faulty electrical equipment sparking).

Risk itself has risk, as measures of risk often are subject to possible change and so measures of risk will often come with a confidence level that tells the reader what the risk of the risk measure is. That is, there may be some uncertainty about the prediction of risk but of course this should never be a reason to avoid the sound practice of risk management, since its application has generated considerable benefits even with less than certain predictions.

1.3 Impact of risk

In her book *Oracles, Curses & Risk Among the Ancient Greeks*, Esther Eidinow shows how the Greeks managed risk by consulting oracles and placing curses on people that affected their lives (Eidinow, 2007). She also posits that risk management is not just a way of handling objective external dangers but is socially constructed and therefore, information about how a civilization perceives risk, provides insights into its social dynamics and view of the world. The type of risks we are concerned with, at a given point in time, also provides insights into our mindset. Specifically, the current preponderance on security, ecological and IT risks would make excellent research material for an anthropologist in 200 years.

This natural tendency to focus on specific types of risk at certain times causes risk issues, as it is exactly the risks you have not been focusing on that can jump up and bite you. In his book *The Black Swan*, Nassim Nicholas Taleb describes events that have a very low probability of occurrence but can have a very great impact (Taleb, 2007). Part of the reasons he gives for these unexpected events is that we have not been focusing on them or their possibilities because of the underlying assumptions we made about our environment (i.e. all swans are white).

It is also true that the impact of many risk events is difficult to estimate precisely, since often one risk event triggers another, sometimes even a chain reaction, and then the measurements tend to become difficult. This distribution of the total impact of a compound event among its components is not of great importance during an initial analysis of risks. We would be interested in the whole, and not in the parts, since our purpose is to prevent the impact. Subsequent, finer, analysis may indeed assign the impacts to the component parts if their happening separately is deemed possible, or if it is possible (and desirable) to manage them separately. A large literature exists on various aspects or risk assessment and risk management. See for example Alexander (1998), Chorafas (2004), Doherty (2000), Dowd (1998), Embrecht *et al*. (1997), Engelmann and Rauhmeier (2006), Jorion (1997), Kenett and Raphaeli (2008), Kenett and Salini (2008), Kenett and Tapiero (2009), Panjer (2006), Tapiero (2004) and Van den Brink (2002).

1.4 Types of risk

In order to mitigate risks the commercial world is developing holistic risk management programmes and approaches under the banner of enterprise risk management (ERM). This framework aims to ensure that all types of risk are

considered and attempts are made to compare different risk types within one overall risk measurement approach. There are many ERM frameworks available, but one of the most prevalent is the COSO ERM model created by the Committee of Sponsoring Organizations of the Treadway Commission. This framework categorizes risks within the following types: (1) financial, (2) operational, (3) legal/compliance and (4) strategic.

It is within this framework that this book approaches operational risks. This category is very broad and is present in, and relevant to, all industries and geographies. It covers such diverse topics as IT security, medical malpractice and aircraft maintenance. This diversity means that there are many approaches to measuring operational risk and all differ in terms of quantitative maturity and conceptual rigour. One important scope of the 'operational' category of risks deals with risks that are associated with the operations of information and communications technology (ICT). The reasons for this are that ICT is nowadays a critical component in all enterprises, forming a layer of the business infrastructure, that attracts over half the capital investments of business and thus deserves to be well managed. Moreover, ICT produces diagnostic data that makes tracking, analysing and understanding risk events easier. This encourages getting insights into the causes of risk events and improving their management. These aspects of risk were the focus of the MUSING European Sixth Framework Programme (MUSING, 2006).

1.5 Enterprise risk management

ERM is a holistic approach that views all the areas of risk as parts of an entity called risk. In addition to the fact that the division of risks across the various categories listed above requires tailored decisions, what one organization may call strategic, may be considered operational in another. The view is that the classification into such areas is an important tool to help decompose a very large problem into smaller pieces. However, all these pieces must be dealt with and then looked at by a senior manager in order to determine which risks are dealt with first, which later and which will currently be knowingly ignored or perhaps accepted without any action to manage them.

The basic creed of ERM is simple: 'A risk, once identified, is no longer a risk – it is a management problem.' Indeed, a telling phrase, putting the responsibility and the accountability for risk management and its consequences right where they belong – on the organization's management. It is based on the realization that the issue of what type a risk is – while relevant to the handling of that risk – is totally immaterial when it comes to damages resulting from that risk. Different types of risks may result in similar damages to the organization.

Therefore, the decomposition of risks into separate areas by their functional root causes is no more than a convenience and not an inherent feature of risk. As a result, all risk management efforts, regardless of their functional, organizational or geographical attributes, should be handled together. They should not be treated

differently just because of expediency or because some functional areas have 'discovered' risk – sometime disguised by other terms – sooner than other areas. For example, just because accounting deals with financial exposure does not mean that risk management should be subjugated to that functional area. For example the fact that IT departments have been dealing with disaster recovery planning (DRP) to their own installations and services does not mean that risk management belongs in those departments. Risk management should be a distinct activity of the organization, located organizationally where management and the board of directors deem best, and this activity should utilize the separate and important skills deployed in each department – be it accounting, IT or any other department – as needed.

1.6 State of the art in enterprise risk management

A well-established concept that has been deployed across different industries and situations is the concept of three lines of defence. It consists of:

- *The business*. The day-to-day running of the operation and the front office.
- *Risk and compliance*. The continual monitoring of the business.
- *Audit*. The periodic checking of risk and compliance.

This approach has offered thousands of organizations a solid foundation upon which to protect themselves against a range of potential risks, both internal and external. Some organizations adopted it proactively on their own, as part of managing risk, and others may have had it forced upon them through regulators' insistence on external audits.

Regardless of circumstance, the three lines of defence concept is reliable and well proven, but it needs to be periodically updated. Otherwise, its ability to meet the rigours of today's market, where there is an increasing number of risks and regulations, and an ever-increasing level of complexity, becomes outdated.

For the three lines of defence to succeed, the communication and relationship between them needs to be well defined and coordination across all three lines must be clearly established. This is not easy to accomplish. In the majority of organizations, management of the various forms of risk – operational risk, compliance risk, legal risk, IT risk, etc. – is carried out by different teams, creating a pattern of risk silos. Each form of risk, or risk silo, is managed in a different way. This situation leads to a number of negative consequences described below.

1.6.1 The negative impact of risk silos

1.6.1.1 Inefficiency multiplies across silos

Silos may be very efficient at one thing, but that may be at the expense of the overall organization's efficiency. In the case of risk silos, each gathers the information it needs by asking the business managers to provide various

information relating to their daily operations and any potential risks associated with them. Because of the silo structure, the business will find itself being asked for this same information on multiple occasions by a multiple of risk silos. These duplicative efforts are inefficient and counterproductive, and lead to frustrated front-office staff disinclined to engage with risk management in the future. The level of frustration is such today that when the recently appointed CEO of a large company asked his senior managers what single change would make their life easier, the reply was to do something to stop the endless questionnaires and check sheets that managers were required to fill out to satisfy risk managers and compliance officers. Frustration among business managers is never a positive development. But it can fully undermine a company's risk management programme as buy-in from the staff is essential.

1.6.1.2 Inconsistency adds to risks

Silos also tend to lead to inconsistency as the same information will be interpreted in different ways by different risk teams. This disparate relationship between risk teams can lead to the failure to recognize potential correlations between various risks. For example, the recent subprime mortgage crisis that has affected so many banks may have been partially avoided if there had been more coordination and communication between the banks' credit departments and those selling mortgages to people with bad credit. Or if the various regulators, whose function it is to reduce those risks, particularly catastrophic risks, were more forthcoming in sharing information with one another and preferred cooperation to turf protection. Similarly the €6.4 billion ($7 billion) loss at Société Générale was the result of several risk oversights, combining a lack of control on individual traders as well as a failure to implement various checks on the trading systems themselves. Also contributing was a negligence of market risk factors with risk management failing to highlight a number of transactions having no clear purpose or economic value.

1.6.1.3 Tearing down silos

Major risk events rarely result from one risk; rather they commonly involve the accumulation of a number of potential exposures. Consequently, companies need to coordinate better their risk management functions and establish consistent risk reporting mechanisms across their organizations. Applying this discipline to enterprise-wide risk management can be exceptionally difficult given that risk information is often delivered in inconsistent formats. For example, interest rate risk may be reported as a single value at risk (VaR) number, whereas regulatory compliance or operational risk may be expressed through a traffic-light format. This disparity can make it extremely difficult for a CRO, CEO or any senior executive accurately to rank risk exposures. As a result, organizations are now recognizing the need to establish a common framework for reporting risk. This is being undertaken through various initiatives across different industries – ICAS, Solvency II and the Basel II Accord. These initiatives have contributed to the

growth of risk and compliance teams. However, the intent of these regulations is not simply to require firms to fulfil their most basic regulatory requirement and to set aside a defined sum of money to cover a list of risk scenarios. Instead, regulators want firms to concentrate on the methodology used to arrive at their risk assessments and to ensure that the risk management process is thoroughly embedded throughout the organization. This requires sound scenario analyses that bring together risk information from all of the various risk silos. It is worthwhile to note that silos do not exist only in the area of risk management. They tend to show up everywhere in organizations where lack of cooperation, competition among units and tunnel vision are allowed to rein unchecked. A notable example of silos is that of the development of separate information systems for the different functional business divisions in an organization, a phenomenon that until the advent and relatively widespread adoption of enterprise-wide computer systems (like ERP, CRM, etc.) caused business untold billions of dollars in losses, wasted and duplicated efforts and lack of coordination within the business. It is high time that risk management adopted the same attitude.

1.6.1.4 Improving audit coordination

Scenario analysis is very much based on the ability to collate and correlate risk information from all over the organization. This includes close coordination not just across the various risk areas, but also with the internal audit teams. This ensures they are more effective and not simply repeating the work of the risk and compliance teams, but rather adding value by rigorously testing this work. Such a task requires using the same common framework as the risk and compliance teams so that information can be seen in the correct context. When this occurs, everyone benefits. Companies are seeing much greater independence and objectivity in the internal audit role. In an increasing number of organizations the internal audit function is no longer confined to existing within a corner of the finance department and has more direct communication with senior management.

1.6.2 Technology's critical role

The use of integrated technology to facilitate the evolution of the three lines of defence is a relatively new development, but will become essential in ensuring coordination across the three lines. Because it has been hard to clarify the different lines of defence and their relationships, it has been difficult to build a business case for a new system and to build the necessary workflow around these different roles. However, the current technology situation, where completely separate legacy systems are used in the business, risk and audit departments, is becoming intolerable and simply contributing to risk. Everyone is aware of the weaknesses in their own systems, but this knowledge does not always translate across the three lines of defence. This leaves most companies with two choices. The first is to design a new all-encompassing system from scratch. The second is to deploy a system that supports common processes and reporting while allowing

each function to continue using specialist solutions that suits its own needs. Successful firms will be those that recognize there are different functionalities in these different spaces, but they are all able to communicate with each other in a common language and through common systems. For example, observations can be shared and specific risk issues can then be discussed through an email exchange and summary reports can be automatically sent out to managers.

For internal auditors, a system that supports common processes and reporting improves efficiency and accuracy. The system can enable all lines of defence to establish risk and control libraries, so that where a risk is identified in one office or department, the library can then be reviewed to see if this risk has been recognized and if there are processes in place to manage this risk. Automating risk identification enables companies to take a smarter, more efficient and more global approach to the internal audit function. For business and risk managers, a system that supports common processes makes risk and compliance much simpler. Risk teams have a limited set of resources and must rely on the business to carry out much of the risk management process. This includes conducting risk and control self-assessments, and recording any losses and control breaches where these losses occur. Using a system that supports common processes means that business managers can accurately and efficiently contribute important information, while not being asked to duplicate efforts across risk silos. Risk managers also can then concentrate on the value-added side of their work and their role.

1.6.3 Bringing business into the fold

Beyond simply helping to get the work done, there are far wider benefits to the organization from using systems that support common processes and the principle behind them. For example, the more front-office staff are exposed to the mechanics of the risk management process (rather than being repeatedly petitioned for the same information from multiple parties), the more they are aware of its importance and their role in it.

A couple of decades ago, total quality management was a fashionable concept in many organizations. In some cases, a dedicated management team was assigned to this area, and the rest of the business could assume that quality was no longer their problem, but someone else's. This same misconception applies to risk and compliance, unless all management and employees are kept well informed of such processes and their own active role in them.

Today, it is indeed critically important that everyone realizes that risk is their responsibility. This requires a clear and open line of communication and coordination between three lines of defence: business, risk and compliance, and audit. In order to implement ERM within an organization, the key challenge facing organizations and the CROs is the myriad of risk approaches and systems implemented throughout the modern large institution. Not only is there a huge amount of disparate data to deal with, but the basis on which this data is created and calculated is often different throughout the organization. As a result, it becomes almost impossible to view risks across units, types, countries or business lines.

Another side of the challenge facing CROs is that there are many disparate customers for ERM reporting and analysis. Reports need to be provided to senior business line management, directors and board committees, regulators, auditors, investors, etc. Quite often these customers have different agendas, data requirements, security clearances and format requirements. Often armies of risk analysts are employed within the ERM team whose task is to take information from business and risks systems and manually sort, review and merge this to attempt an overall view of the risk position of the company. This process is very resource and time consuming and extremely prone to error.

In other cases, CROs tackle ERM in a piecemeal fashion. They choose certain risk types or business lines that they feel can be successfully corralled and develop an ERM system to load data concerning those risk types or business lines, normalize that data so that it can be collated and then implement an analytic system to review the enterprise risk within the corral. The aim is to generate a quick win and then expand the framework as methodologies and resources become available. While this approach is a pragmatic one, and derives benefit for the organization, it has one major flaw. If you do not consider the entire picture before designing the approach, it can often be impossible to graft on further types of risk or business line in the future. Even if you manage to make the new addition, the design can fall into the 'I wouldn't have started from here' problem and therefore compromise the entire framework.

What is needed is an approach that implements a general ERM framework from the start that can be utilized as needed by the organization. This framework should cover all risk types and provide support for any business line type or risk measurement type. It should enable an organization to collate data in a standard format without requiring changes to specific lines of business or risk management systems. The 14 chapters of this book provide answers and examples for such a framework using state-of-the-art semantic and analytical technologies.

1.7 Summary

The chapter introduces the concept of risk, defines it and classifies it. We also show the evolution of risk management from none at all to today's heightened awareness of the necessity to deploy enterprise risk management approaches. Risk is now at the core of many applications. For example, Bai and Kenett (2009) propose a risk-based approach to effective testing of web services. Without such testing, we would not be able to use web applications reliably for ordering books or planning a vacation. Kenett *et al*. (2009) present a web-log-based methodology for tracking the usability of web pages. Risks and reliability are closely related. The statistical literature includes many methods and tools in these areas (see Kenett and Zacks, 1998; Hahn and Doganaksoy, 2008). Two additional developments of risks are worth noting. The first one is the introduction of Taleb's concept of black swans. A black swan is a highly improbable event with three principal characteristics: (1) it is unpredictable; (2) it carries a massive impact;

and (3) after the fact, we concoct an explanation that makes it appear less random, and more predictable, than it was (Taleb, 2007). Addressing black swans is a huge challenge for organizations of all size, including governments and not-for-profit initiatives. Another development is the effort to integrate methodologies from quality engineering with risk economics (Kenett and Tapiero, 2009). The many tools used in managing risks seek, de facto, to define and maintain the quality performance of organizations, their products, services and processes. Both risks and quality are therefore relevant to a broad number of fields, each providing a different approach to their measurement, their valuation and their management which are motivated by psychological, operational, business and financial needs and the need to deal with problems that result from the uncertainty and their adverse consequences. Both uncertainty and consequences may be predictable or unpredictable, consequential or not, and express a like or a dislike for the events and consequences induced. Risk and quality are thus intimately related, while at the same time each has, in some specific contexts, its own particularities. When quality is measured by its value added and this value is uncertain or intangible (as is usually the case), uncertainty and risk have an appreciable effect on how we deal, measure and manage quality. In this sense, both risk and quality are measured by 'money'. For example, a consumer may not be able to observe directly and clearly the attributes of a product. And, if and when the consumer does so, this information might not be always fully known, nor be true. Misinformation through false advertising, unfortunate acquisition of faulty products, model defects, etc., have a 'money effect' which is sustained by the parties (consumers and firms) involved. By the same token, poor consumption experience in product and services can have important financial consequences for firms that can be subject to regulatory, political and social pressures, all of which have financial implications. Non-quality, in this sense, is a risk that firms assess, that firms seek to value and price, and that firms manage to profit and avoid loss. Quality and risk are thus consequential and intimately related. The level of delivered quality induces a risk while risk management embeds tools used to define and manage quality. Finally, both have a direct effect on value added and are a function of the presumed attitudes towards risk and the demands for quality by consumers or the parties involved in an exchange where it is quality or risk.

This introductory chapter lays the groundwork for the whole book that will move us from the general view of risk to specific areas of operational risk. In the following chapters the reader will be presented with the latest techniques for operational risk management coming out of active projects and research dedicated to the reduction of the consequences of operational risk in today's highly complex, fast-moving enterprises. Many examples in the book are derived from work carried out within the MUSING project (MUSING, 2006). The next chapter provides an introduction to operational risk management and the successive 12 chapters cover advanced methods for analysing semantic data, combining qualitative and quantitative information and putting integrated risk approaches at work, and benefiting from them. Details on operational risk ontologies and data mining

techniques for unstructured data and various applications are presented, including their implication to intelligent regulatory compliance and the analysis of near misses and incidents.

The overall objective of the book is to pave the way for next generation operational risk methodologies and tools.

References

Alexander, C.O. (1998) *The Handbook of Risk Management and Analysis*, John Wiley & Sons, Inc., New York.

Ayyub, B.M. (2003) *Risk Analysis in Engineering and Economics*, Chapman & Hall/CRC Press, Boca Raton, FL.

Bai, X. and Kenett, R.S. (2009) Risk-Based Adaptive Group Testing of Web Services, *Proceedings of the Computer Software and Applications Conference (COMPSAC'09)*, Seattle, USA.

Chorafas, D.N. (2004) *Operational Risk Control with Basel II: Basic Principles and Capital Requirements*, Elsevier, Amsterdam.

Davies, J.C. (Editor) (1996) *Comparing Environmental Risks: Tools for Setting Government Priorities*, Resources for the Future, Washington, DC.

Doherty, N.A. (2000) *Integrated Risk Management: Techniques and Strategies for Managing Corporate Risk*, McGraw-Hill, New York.

Dowd, K. (1998) *Beyond Value at Risk: The New Science of Risk Management*, John Wiley &, Ltd, Chichester.

Eidinow, E. (2007) *Oracles, Curses & Risk Among the Ancient Greeks*, Oxford University Press, Oxford.

Embrecht, P., Kluppelberg, C. and Mikosch, T. (1997) *Modelling External Events*, Springer-Verlag, Berlin.

Engelmann, B. and Rauhmeier, R. (2006) *The Basel II Risk Parameters*, Springer, Berlin–Heidelberg, Germany.

Finkel, A.M. and Golding, D. (1994) *Worst Things First? The Debate over Risk-Based National Environmental Priorities*, Resources for the Future, Washington, DC.

Guess, F. (2000) Improving Information Quality and Information Technology Systems in the 21st Century, *International Conference on Statistics in the 21st Century*, Orino, ME.

Hahn, G. and Doganaksoy, N. (2008) *The Role of Statistics in Business and Industry*, Wiley Series in Probability and Statistics, John Wiley & Sons,Inc., Hoboken, NJ.

Haimes, Y.Y. (2009) *Risk Modeling, Assessment and Management*, third edition, John Wiley & Sons, Inc., Hoboken, NJ.

Jorion, P. (1997) *Value at Risk: The New Benchmark for Controlling Market Risk*, McGraw-Hill, Chicago.

Kenett, R.S. (2008) From Data to Information to Knowledge, *Six Sigma Forum Magazine*, pp. 32–33.

Kenett, R.S. (2009) Discussion of Post-Financial Meltdown: What Do the Services Industries Need From Us Now?, *Applied Stochastic Models in Business and Industry*, 25, pp. 527–531.

Kenett, R.S. and Raphaeli, O. (2008) Multivariate Methods in Enterprise System Implementation, Risk Management and Change Management, *International Journal of Risk Assessment and Management*, 9, 3, pp. 258–276 (2008).

Kenett, R.S. and Salini, S. (2008) Relative Linkage Disequilibrium Applications to Aircraft Accidents and Operational Risks, *Transactions on Machine Learning and Data Mining*, 1, 2, pp. 83–96.

Kenett, R.S. and Shmueli, G. (2009) On Information Quality, University of Maryland, School of Business Working Paper RHS 06-100, http://ssrn.com/abstract=1464444 (accessed 21 May 2010).

Kenett, R.S. and Tapiero, C. (2009) Quality, Risk and the Taleb Quadrants, *Risk and Decision Analysis*, 4, 1, pp. 231–246.

Kenett, R.S. and Zacks, S. (1998) *Modern Industrial Statistics: Design and Control of Quality and Reliability*, Duxbury Press, San Francisco.

Kenett, R.S., de Frenne, A., Tort-Martorell, X. and McCollin, C. (2008) The Statistical Efficiency Conjecture, in *Statistical Practice in Business and Industry*, Coleman, S., Greenfield, T., Stewardson, D. and Montgomery, D. (Editors), John Wiley &Sons, Ltd, Chichester.

Kenett, R.S., Harel, A. and Ruggerri, F. (2009) Controlling the Usability of Web Services, *International Journal of Software Engineering and Knowledge Engineering*, 19, 5, pp. 627–651.

Knight, F.H. (1921) *Risk, Uncertainty and Profit*, Hart, Schaffner and Marx (Houghton Mifflin, Boston, 1964).

MUSING (2006) IST- FP6 27097, http://www.musing.eu (accessed 21 May 2010).

Panjer, H. (2006) *Operational Risks: Modelling Analytics*, John Wiley & Sons, Inc., Hoboken, NJ.

Redman, T. (2007) Statistics in Data and Information Quality, in *Encyclopedia of Statistics in Quality and Reliability*, Ruggeri, F., Kenett, R.S. and Faltin, F. (Editors in chief), John Wiley & Sons, Ltd, Chichester.

Taleb, N.N. (2007) *The Black Swan: The impact of the highly improbable*, Random House, New York.

Tapiero, C. (2004) *Risk and Financial Management: Mathematical and Computational Methods*, John Wiley & Sons, Inc., Hoboken, NJ.

Van den Brink, G. (2002) *Operational Risk: The New Challenge for Banks*, Palgrave, New York.